REDES

A. Transmisión y comunicación de datos

I. Concepto Básicos.

1. Teoría de la información.

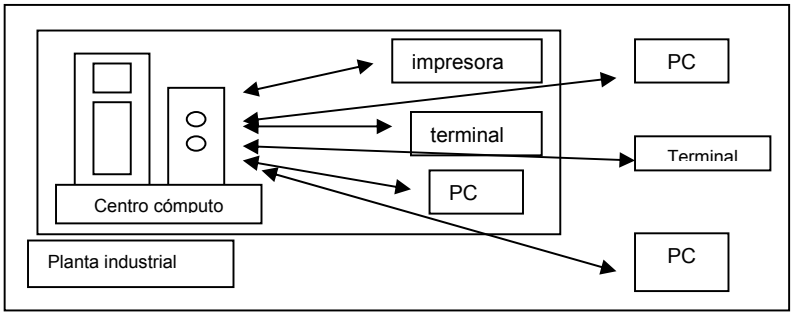
- ***Definición y conceptos de transmisión de datos***

Se entiende por transmisión de datos al movimiento de información codificada, de un punto a uno mas puntos, mediante señales eléctricas, ópticas, electromagnéticas o electro ópticas. El CCITT, en su recomendación X.25 define la transmisión de datos, como "la acción de cursar datos, atraves de un medio de telecomunicaciones, de un lugar en que son originados a otro que son recibidos ". Este punto puede estar dentro de la propia organización, próximo o alejado del computador central. La diferencia importante que es necesario efectuar, reside en la distancia y la geografía del problema a considerar, pues en función de estos parámetros, puede ser necesario o no el uso de redes de comunicación. Así, es que se puede hablar de dos tipos de transmisión de datos a saber:

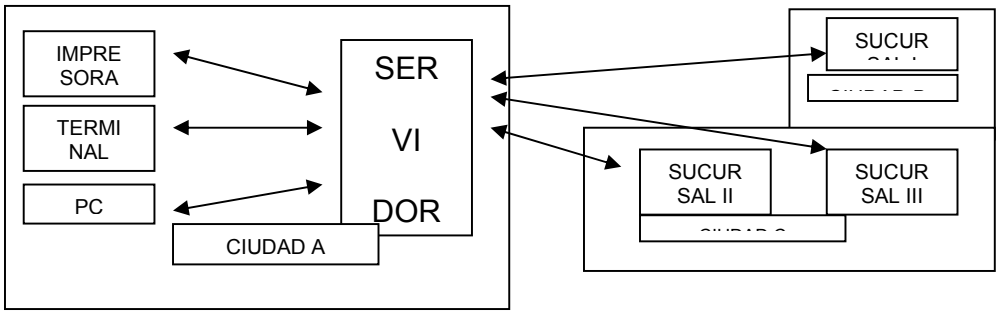
- **Local (en planta) ->** La propia organización generalmente construye las líneas de comunicaciones necesarias y los problemas técnicos cuando las distancias son pequeñas resultan mínimos y no requieren consideraciones especiales. Es el caso de computador central o un minicomputador, que tiene conectadas, dentro de un edificio o en una superficie geográfica reducida, una serie de terminales. Se trabaja con velocidades mayores y tanto las interfaces eléctricas como los protocolos de comunicación son provistos por los fabricantes del hardware.
- **Remota (fuera de planta) ->** se necesitará de líneas de telecomunicaciones para efectivarlas de allí surge la necesidad de tener en cuenta una serie de técnicas especiales que sé a denominado con el nombre de: teleinformática o telemática.

Se podría definir a la **teleinformática** como **la ciencia de que estudia al conjunto de técnicas que es necesario usar para poder transmitir datos dentro de un sistema informático o entre puntos de el situados en lugares remotos y usando redes de telecomunicaciones.** El problema que busca resolver, por lo tanto, la teleinformática, es el de "lograr que un computador pueda dialogar con equipos situados geográficamente distantes, reconociendo las características esenciales de la información como si la conexión fuera local, usando redes de telecomunicaciones ".

TRANSMISIÓN DE DATOS EN PLANTA.



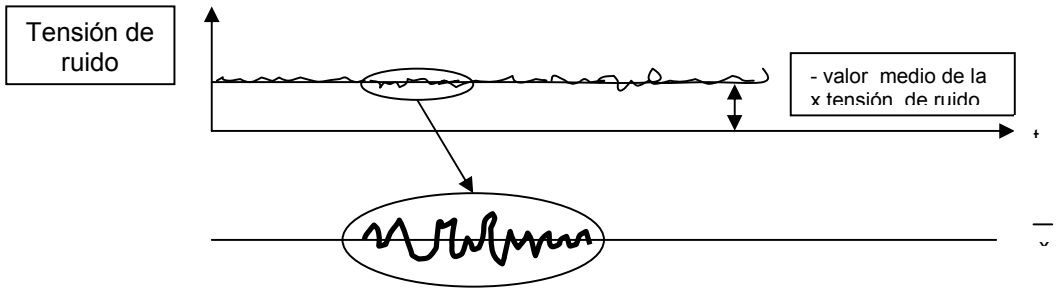
TRANSMISIÓN DE DATOS REMOTA



- ***Ruido (tipos y características)***

El ruido y la distorsión son fenómenos adversos para la propagación de señales en los sistemas de comunicaciones, ocasionando la disminución del rendimiento de dichos sistemas, los 2 parámetros que miden el comportamiento de los sistemas de comunicaciones frente al ruido y la distorsión son la tasa de error en los sistemas digitales y la relación señal ruido en los sistemas analógicos.
Ruido. **Es todo fenómeno que afecta la calidad de la señal recibida.** Tiene como caricaturistas principales que es variable en el tiempo en forma aleatoria y esta originado por la superposición de eventos externos e internos al sistema de comunicaciones. Aun suponiendo que un canal se puede blindar o proteger de alguna forma contra toda interferencia exterior, se mantendrá un ruido conocido como fluctuación o ruido térmico propio del sistema de telecomunicaciones.

FORMA DE ONDA DE RUIDO TIPICA



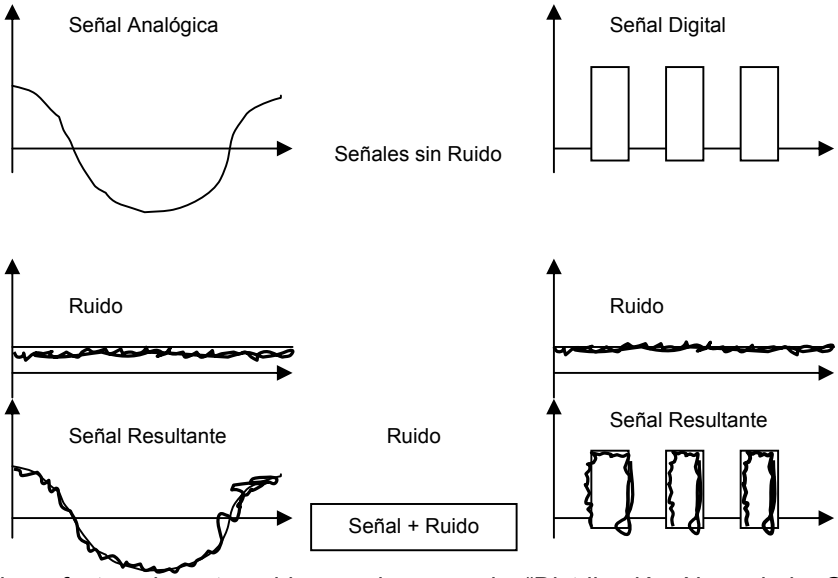
Clasificación del ruido respecto al sistema de comunicaciones.
El ruido se puede clasificar de acuerdo a sí proviene de elementos propios del sistema de comunicaciones o ajenos a este, en ruido endógeno o exógeno.

- **Ruido Endógeno:** Se denomina endógeno al ruido producido por variables propias incontrolables del sistema de comunicaciones.
- **Ruido Exógeno:** Se denomina exógeno al ruido producido por elementos externos al sistema de comunicaciones, pero que se acoplan al mismo.

Clasificación de los distintos tipos de ruido.
El ruido se puede clasificar en función de los agentes que lo producen y de los efectos nocivos que causa en el sistema de comunicaciones, en los sigs. Tipos:

- **Ruido Blanco o gaussiano (Ruido de johnson).** Se produce por el movimiento aleatorio de los electrones en los conductores y demás componentes electrónicos pertenecientes al sistema de comunicaciones. Estos movimientos aleatorios hacen que los cuerpos irradien energía en forma de ondas electromagnéticas, siendo la potencia radiada proporcional a la temperatura. En los cables o conductores de un canal, los movimientos aleatorios de los átomos y electrones, radian energía electromagnética, parte de la cual se canaliza por los conductores hasta llegar al receptor, donde aparecerá como un tensión de ruido superpuesta a la señal útil. Esta tensión tiene un valor cuadratico proporcional al ancho de banda empleado por lo que este ultimo de be de ser lo más pequeño posible, a efectos de disminuir el ruido. También se conoce como ruido blanco porque por que la densidad del ruido es constante sobre todas las frecuencias de interés en las redes, lo cual tiene analogía con el espectro de la luz blanca donde toma su nombre. Si se tiene señales analógicas o digitales se observa que el ruido blanco se suma a la señal a transmitir formando un fondo de bajo nivel que puede llegar a producir errores si los niveles de señal son bajos.
  EFECTO DEL RUIDO BLANCO S/ LAS SEÑALES TRANSMITIDAS.

Redes



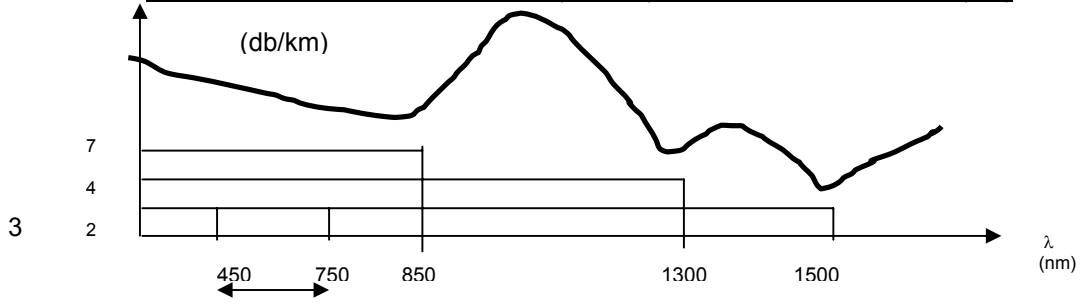
El estudio de los efectos de este ruido se basa en la "Distribución Normal de Gauss". Una propiedad de la distribución de Gauss es que siempre habrá un a probabilidad finita, aunque pequeña de que se pueda exceder cualquier nivel. El ruido blanco se extiende a todo el espectro de frecuencias.

- **Ruido impulsivo.->** es un ruido que no aparece en forma continua, sino a intervalos irregulares y con picos de corta duración, pero de gran amplitud. Es de difícil localización en cuanto a su origen. En particular este ruido puede ser de muy alto nivel. Los pulsos de ruido, también conocidos como "bursts", ocurren comúnmente en forma dispersa en el tiempo de, en ráfagas cortas con una duración aprox. De 20 mseg. Sobre circuitos telefónico típicos.
- **Ruido de intermodulacion:->** es la distorsión de que ocurre cuando se aplican varias señales senoidales a un dispositivo no lineal. En este caso, aparecen frecuencias adicionales que no están armónicamente relacionadas ala frecuencia de la señal.
- **Diafonia o "cross - talk": ->** es el acoplamiento indeseado entre dos señales(cross - talk) mediante la inducción electromagnética mutua generalmente producida entre conductores. Un ej., Dé ellos son los pares telefónicos, que ocurren paralelos muchos kms. O también por circuitos eléctricos de alta tensión, instalados próximos a la ruta telefónica. Para eliminar se suelen usar las transposiciones, para compensar las inducciones electromagnéticas mutuas que se producen en dichos conductores. La diafonia se presenta también cundo los filtros que forman parte de un canal de comunicación son de poca calidad o se encuentran mal diseñados en el caso de los sistemas con MULTIPLEXORES analógicos, cuando estos últimos presentan un comportamiento no lineal.
- **Ruido de línea o simple: ->**es el provocado por la presencia de líneas electrónicas de energía (220 volts/50 hertz o 110 volts/60 hertz) que se usan en instalaciones eléctricas para la iluminación y alimentación de equipos y/o sistemas eléctricos y electrónicos. Las líneas de alta tensión y los transformadores de potencia son las principales fuentes de este tipo de ruido. Se puede reducir y hasta eliminar este tipo de ruido mediante el uso de filtros especiales llamados: "filtros de línea", los cuales eliminan las frecuencias de 50 o 60 hertz correspondientes a las tensiones de alimentación.

- ***Atenuación***.

El término "atenuación", se usa para medir la perdida de la potencia óptica de un haz de luz que viaja por la fibra. La atenuación se mide en db/km y es función de la longitud de onda. Existen ciertas longitudes de onda llamadas ventanas, para las cuales la atenuación de la luz es mínima.

VARIACIÓN DE LA ATENUACIÓN (DB/KM) Vs LONGITUD DE ONDA(nm)



Luz visible 1ra ventana 2da ventana 3ra ventana

De las 3 ventanas la que corresponde a 1550 nm esla que representa menor atenuacion.

2. Códigos

Código (informática)
Término genérico para nombrar las instrucciones del programa, utilizadas en dos sentidos generales. El primero se refiere al código fuente, legible a simple vista, que son las instrucciones escritas por el programador en un lenguaje de programación. El segundo se refiere al código máquina ejecutable, que son las instrucciones convertidas de código fuente a instrucciones que el ordenador o computadora puede comprender.

- ***Códigos binarios.***

Códigos binarios Los computadores digitales utilizan el sistema de números binarios, que tiene dos dígitos O y 1. Un dígito binario se denomina un *bit.* La información está representada en los computadores digitales en grupos de bits. Utilizando diversas técnicas de codificación de los grupos de bits puede hacerse que representen no solamente números binarios si no también otros símbolos discretos cualesquiera, tales como dígitos decimales o letras del alfabeto. Por medio de un uso razonable de los arreglos binarios y utilizando diversas técnicas de codificación, los dígitos binarios o grupos de bits pueden utilizarse para desarrollar conjuntos completos de instrucciones para realizar diversos tipos de cálculos.

En contraste con los números decimales comunes que se emplean en el sistema de base 1o' los números binarios utilizan un sistema de base 2, por ejemplo el número binario 101101 representa una cantidad que puede convertirse a un número decimal multiplicando cada bit por la base 2 elevada a una potencia entera de la manera siguiente:

1 x 25 + O X 24 + 1 X 23 + 1 X 22 + O X 21 + 1 x 2° = 45

Los seis bits 101101 representan un número binario cuyo equivalente decimal es 45. Sin embargo, el grupo de seis bits podría también representar un código binario para una letra del alfabeto o un código de control para especificar alguna decisión lógica en un sistema digital particular. En otras palabras, los grupos de bits en un computador digital son utilizados para representar muchas cosas diferentes. Esto es similar al concepto que la misma letra de un alfabeto se utiliza para constituir lenguajes diferentes, tales como el inglés y el francés.

La información binaria se representa en un sistema digital por cantidades físicas denominadas *señales.* Las señales eléctricas tales como voltajes existen a través del sistema digital en cualquiera de dos valores reconocibles y representar una variable binaria igual a 1 o a O. Por ejemplo, un sistema digital particular puede emplear una señal de 3V para representar el binario 1 y 0,5 V para el binario 0. Como se muestra en la figura, cada valor binario tiene una desviación aceptable del valor nominal. La región intermedia entre las dos regiones permitidas se cruza solamente durante la transición de estado. Los terminales de entrada de un circuito digital aceptan señales binarias dentro de las tolerancias permitidas y los circuitos responden en los terminales de salida con señales binarias que caen dentro de las tolerancias especificadas.

Binario 1

La lógica binaria tiene que ver con variables y con operaciones que toman un sentido lógico. Es utilizada para describir, en forma algebraica o tabular, la manipulación y proceso de información binaria. La manipulación de información binaria se hace por circuitos lógicos que se denominan *compuertas.* Las compuertas son bloques del hardware que producen señales del binario 1 ó O cuando se satisfacen los requisitos de la entrada lógico. Las diversas compuertas lógicas comúnmente en sistemas de computador digital. Cada compuerta tiene un símbolo gráfico diferente y su operación puede describirse por medio de una función algebraica. Las relaciones entrada-salida de las variables binarias para cada compuerta pueden representante en forma tabular en una *tabla de verdad.*

Binario O

Tolerancia permitida para el binario 1

Redes

Los nombres, símbolos gráficos, funciones algebraicas, y tablas de verdad de verdad de ocho compuertas lógicas se enumeran en la siguiente figura. Cada compuerta tiene una o dos variables de entrada binarias designadas por A y B y una binaria designada por x. La compuerta AND produce la unión AND: esto es; la salida es 1 si la entrada A y la entrada *B* están en el binario 1; de otra manera, la salida es O. Estas condiciones también son especificadas en la tabla de verdad para la compuerta AND. La tabla muestra que la salida x es 1 solamente cuando ambas entradas *A* y *B* están en 1. El símbolo de la multiplicación de la aritmética ordinaria. Podemos utilizar o un punto entre las variables o concatenar las variables sin ningún símbolo de operación entre ellas. Las compuertas AND pueden tener más de dos entradas y por definición, la salida es 1 si y solamente si *todas* las entradas son 1.

Ejemplo de una señal binaria

Tolerancia permitida para el binario O

La compuerta OR produce la función OR inclusiva, esto es, la salida es 1 si la entrada A o la entrada *B* o ambas entradas son 1; de otra manera, la salida es O. El símbolo algebraico de la función OR es + , similar a la operación aritmética de suma. Las compuertas OR pueden tener más de dos entradas y por definición la salida es 1 si *cualquier* estrada es 1 .

El circuito inversor invierte el sentido lógico de una señal binaria. Produce el NOT, o función, *complemento.* El símbolo algebraico utilizado para el complemento es o una prima o una barra sobre el símbolo de la variable. Este libro utiliza una prima para el complemento lógico de una variable binaria, mientras que una barra sobre la letra se reserva para designar un complemento de una micro-operación.

El círculo pequeño en la salida de un símbolo gráfico de un inversor designa un complemento lógico. Un símbolo triángulo por si mismo designa un circuito separador. Un separador no produce ninguna función lógica particular puesto que el valor binario de la salida es el mismo de la entrada. Este circuito se utiliza simplemente para amplificación de la señal. Por ejemplo, un separador que utiliza 3V. Sin embargo, la corriente suministrada en la entrada es mucho más pequeña que la corriente producida en la salida. De esta manera, un separador puede excitar muchas otras compuertas que requieren una cantidad mayor de corriente que de otra manera no se encontraría en la pequeña cantidad de corriente aplicada a la entrada del separador.

La compuerta OR exclusiva tiene un símbolo gráfico similar a la compuerta OR excepto por una línea adicional en el lado de entrada. La salida de esta compuerta es 1 si cada entrada es 1 pero excluye la combinación cuando las dos entradas son 1. La función OR exclusiva tiene su propio símbolo algebraico o puede expresarse en términos de operaciones complementarias AND, OR como se muestra en la figura anterior. El NOR exclusivo es el complemento del OR exclusivo como se indica en el círculo pequeño en el símbolo gráfico. La salida de esta compuerta es 1 solamente si ambas entradas tienen el mismo valor binario. Nosotros nos referimos a la Función NOR exclusivo como la función de *equivalencia.* Puesto que las funciones OR exclusivo y funciones de equivalencia no son siempre complemento la una de la otra. Un nombre más adecuado para la operación OR exclusivo sería la función *impar;* esto es, la salida es 1 si un número impar de las entradas es 1. Así en una función OR (impar) exclusiva de tres entradas la salida es 1 si solamente la entrada es 1 o si todas las tres entradas son 1. La función de equivalencia es una función *par;* esto es, su salida es 1 si un número par de entradas es O. Para una función de equivalencia de tres entradas la salida es 1 si ninguna de las entradas son 0 (todas las entradas son 1) o si dos de las entradas son 0 (una entrada es 1). Una investigación cuidadosa revelará que el OR exclusivo y las funciones de equivalencia son el complemento la una de la otra cuando las compuertas tienen un número par de entradas pero si las funciones son iguales cuando el número de entradas es impar. Estas dos compuertas comúnmente disponibles con dos entradas y solamente en forma rara se encuentran con tres o más entradas.

- ***Caracteres alfanuméricos y de control en ASCII y EBCDIC.***

ASCII, acrónimo de American Standard Code for Information Interchange
(Código Normalizado Americano para el Intercambio de Información). En computación, un esquema de codificación que asigna valores numéricos a las letras, números, signos de puntuación y algunos otros caracteres. Al normalizar los valores utilizados para dichos caracteres, ASCII permite que los ordenadores o computadoras y programas informáticos intercambien información. ASCII incluye 256 códigos divididos en dos conjuntos, estándar y extendido, de 128 cada uno. Estos conjuntos representan todas las combinaciones posibles de 7 u 8 bits, siendo esta última el

número de bits en un byte. El conjunto ASCII básico, o estándar, utiliza 7 bits para cada código, lo que da como resultado 128 códigos de caracteres desde 0 hasta 127 (00H hasta 7FH hexadecimal). El conjunto ASCII extendido utiliza 8 bits para cada código, dando como resultado 128 códigos adicionales, numerados desde el 128 hasta el 255 (80H hasta FFH extendido). En el conjunto de caracteres ASCII básico, los primeros 32 valores están asignados a los códigos de control de comunicaciones y de impresora -caracteres no imprimibles, como retroceso, retorno de carro y tabulación- empleados para controlar la forma en que la información es transferida desde una computadora a otra o desde una computadora a una impresora. Los 96 códigos restantes se asignan a los signos de puntuación corrientes, a los dígitos del 0 al 9 y a las letras mayúsculas y minúsculas del alfabeto latino. Los códigos de ASCII extendido, del 128 al 255, se asignan a conjuntos de caracteres que varían según los fabricantes de computadoras y programadores de software. Estos códigos no son intercambiables entre los diferentes programas y computadoras como los caracteres ASCII estándar. Por ejemplo, IBM utiliza un grupo de caracteres ASCII extendido que suele denominarse conjunto de caracteres IBM extendido para sus computadoras personales. Apple Computer utiliza un grupo similar, aunque diferente, de caracteres ASCII extendido para su línea de computadoras Macintosh. Por ello, mientras que el conjunto de caracteres ASCII estándar es universal en el hardware y el software de los microordenadores, los caracteres ASCII extendido pueden interpretarse correctamente sólo si un programa, computadora o impresora han sido diseñados para ello.
Conjunto de caracteres ASCII, en informática, un código estándar de 7 bits para la representación de caracteres -letras, dígitos, signos de puntuación e instrucciones de control- con valores binarios. El intervalo de los valores del código es de 0 a 127. Aunque ASCII carece tanto de los acentos como de los caracteres especiales utilizados en diversos idiomas europeos, y no es capaz de representar caracteres en los alfabetos no latinos, reviste importancia por ser el sistema de codificación de caracteres más internacional. Muchos conjuntos de caracteres latinos no ingleses son extensiones o modificaciones del sistema de codificación ASCII. La mayoría de los sistemas de ordenadores o computadoras personales utilizan un código ASCII extendido o modificado de 8 bits, con 128 caracteres adicionales para símbolos especiales, letras y signos de puntuación de diversos idiomas, y símbolos gráficos.
ASCII extendido, en informática, cualquier conjunto de caracteres asignado a los valores de ASCII entre 128 y 255 decimal (hexadecimal 80 a FF). El ASCII extendido se diferencia del ASCII estándar en que no es un único grupo definido de caracteres que se pueda considerar como el conjunto extendido de caracteres ASCII. Los caracteres específicos asignados a los códigos de ASCII extendido pueden variar mucho entre distintos equipos (por ejemplo entre un PC de IBM y un equipo Apple Macintosh) y entre programas, fuentes, o conjuntos de caracteres gráficos. El ASCII estándar cubre fundamentalmente lo básico, proporcionando códigos de caracteres, como letras y números, con los que todas las computadoras deben trabajar. El ASCII extendido proporciona una capacidad añadida de 128 caracteres adicionales, tales como letras acentuadas, caracteres gráficos y símbolos especiales. Los códigos utilizados en ASCII extendido representan los valores adicionales posibles mediante el uso de los 8 bits de un byte para la codificación (en ASCII estándar se usan sólo 7).
EBCDIC, acrónimo de Extended Binary Coded Decimal Interchange Code
(Código Ampliado de Caracteres Decimales Codificados en Binario para el Intercambio de la Información). Un esquema de codificación desarrollado por IBM para utilizarlo en sus ordenadores o computadoras como método normalizado de asignación de valores binarios (numéricos) a los caracteres alfabéticos, numéricos, de puntuación y de control de transmisión. EBCDIC es análogo al esquema de codificación ASCII aceptado más o menos en todo el mundo de los microordenadores o las microcomputadoras. Se diferencia por utilizar 8 bits para la codificación, lo que permite 256 caracteres posibles (en contraste con los 7 bits y 128 caracteres del conjunto ASCII estándar). Aunque EBCDIC no se utiliza mucho en las microcomputadoras, es conocido y aceptado internacionalmente, sobre todo como código de IBM para los mainframes y minicomputadoras de la compañía.

3. Errores.

- ***Naturaleza de los errores.***

Los errores en la transmision en las lineas telefonicas son provicados por varios fenomenos fisicos. Un fenomeno que siempre esta presente es el ruido termico. Los electrones, en los hilos de cobre, estan moviendose a muy alta velocidad y en todas las direcciones, produciendo un amplio espectro de nivel de ruido de fondo. Esta es la relacion señal a ruido. Tambien contribuyen los relampagos , los separadores detelefonos toscos, petardos de los tubos de escape de los coches, sobretenciones de las lineas de energia y los tonos de señalizacion del sistema telefonico. Otras fuentes de errores de suma importancia es el hecho de que la amplitud, velocidad de porpagacion y fase de las señales, dependen todos de la frecuencia. El cruce de señales de entre lineas. Como resultado de los procesos fisicos que ocasionan el ruido, los errores tienden a presentarse como rafagas, mas que aisladamente. Este hecho tiene ciertas ventajas y desventajas con respectos a los errores aislados, de un solo bit. Las ventajas son: los datos

de la pc siempre se envian en bloques de bits. Suponga que eltamaño del bloque es de 1000 bits, y que la tasa de error es de 0.001 por bit. Si los errores fueran independientes, la mayorai de los bloques tendira un error. Sin embargo los errores vienen en rafagas de 100, solo uno de los dos bloques de cda cien son afectados.
La desventaja es que son mucho mas dificiles de detectar y corregir que los errores aislados y, tambien, son mas dificiles de modelar analiticamente.

- ***Algoritmos de detecciòn de error.***

Comprobación De Paridad

Se añade un bit de paridad al bloque de datos por ejemplo si hay número de bits 1 se añade un bits 0 de paridad y si son impares se añade un bits 1 de paridad, pero pude ocurrir que propio bits de paridad sea cambiado por el ruido o incluso que más de un bits de datos sea cambiado par evitar esta situación el tramo me trae otro bits de controles que detectaran si existe falla en la transmisión.

Por ejemplo, asume que tenemos un canal con una taza de errores de 10^{-6} por bit (es decir, un bit en cada 10^6). Usamos mensajes de 1000 bits de dato.

- Para la corrección debemos añadir 10 bits por mensaje. En la transmisión de 10^6 bits de dato mandamos 10.000 bits de chequeo para detectar y corregir el un bit de error que esperamos.
- Para la detección usamos solamente un bit de paridad por mensaje. Para 10^6 bits de dato usamos solamente 1000 bits. Pero uno de los mensajes tiene un error, así que tenemos que retransmitirlo con su bit de paridad (1001 bits). En total usamos 2001 bits para este esquema.

Si usamos un solo bit de paridad y tenemos un grupo de errores, la probabilidad de detección es solamente 1/2. Podemos aumentar la capacidad a detectar un grupo de errores usando el truco de la transmisión de un matriz de k×n: Se transmiten los datos por columna, y cada fila tiene un bit de paridad. Podemos detectar los errores en grupo hasta n, el número de filas. No podemos detectar n+1 si el primer bit y el último bit son invertidos y todos los otros son correctos. Si tenemos muchos errores en el bloque la probabilidad de aceptarlo es solamente $(1/2)^n$.

El algoritmo de *checksum*

La idea en la que se basa la suma de chequeo de Internet es muy sencilla: se suman todas las palabras de 16 bits que conforman el mensaje y se transmite, junto con el mensaje, el resultado de dicha suma (este resultado recibe el nombre de *checksum*). Al llegar el mensaje a su destino, el receptor realiza el mismo cálculo sobre los datos recibidos y compara el resultado con el checksum recibido. Si cualquiera de los datos transmitidos, incluyendo el mismo *checksum*, esta corrupto, el resultado no concordará y el receptor sabrá que ha ocurrido un error.

El *checksum* se realiza de la siguiente manera: los datos que serán procesados (el mensaje) son acomodados como una secuencias de enteros de 16 bits. Estos enteros se suman utilizando aritmética complemento a uno para 16 bits y, para generar el *checksum*, se toma el complemento a uno para 16 bits del resultado.

En aritmética complemento a uno, un entero negativo -*x* se representa como el complemento de *x*; es decir, cada bit de *x* es invertido. Cuando los números se adicionan, si se obtiene un acarreo (*carry*) en el bit más significativo, se debe incrementar el resultado. Por ejemplo, sumemos -5 y -3 en aritmética complemento a uno con enteros de 4 bits. En este caso +5 se representaría con 0101 y -5 con 1010; +3 se representaría con 0011 y -3 con 1100. Al sumar 1010 y 1100, ignorando el acarreo (*carry*) que queda en el bit más significativo, tendremos como resultado 0110. En la aritmética complemento a uno, cuando una operación genera un acarreo (*carry*) en el bit más significativo, se debe incrementar el resultado; es decir que 0110 se convierte en 0111, que es la representación complemento a uno de -8 (obtenido de invertir los bits 1000).

El uso del algoritmo de *checksum* de Internet en los headers de los protocolos se puede resumir en tres pasos simples.

1. Los octetos adyacentes que se deben verificar con al suma de chequeo deben ser acomodados para formar enteros de 16 bits, luego se calcula la suma complemento a uno de estos enteros (de 16 bits)

2. Para generar el *checksum*, el campo de *checksum* del header del PDU que será transmitido es puesto en cero, luego la suma complemento a uno es calculada sobre los octetos correspondientes y el complemento a uno de esta suma se coloca en el campo de *checksum*.

3. Para revisar el checksum, la suma es calculada sobre los mismo octetos, incluyendo el campo de checsum. Si el resultado es 16 bits con valor 1 (-0 en aritmética complemento a uno), el chequeo es correcto.

Como un ejemplo sencillo del cálculo del *checksum* supongamos que tenemos tres "palabras" de 16 bits

0110011001100110
0101010101010101
0000111100001111

La suma de las dos primeras palabras sería:

0110011001100110
0101010101010101
1011101110111011

Adicionando ahora la tercera "palabra" al resultado anterior tenemos

1011101110111011
0000111100001111
1100101011001010

La suma complemento a uno se obtiene convirtiendo todos los ceros en unos y todos los unos en ceros. De esta forma la suma complemento a uno de 1100101011001010 sería 0011010100110101. Que vendría a ser el *checksum*. Al llegar al receptor las cuatro palabra de 16 bits, incluyendo el *checksum* son sumados y el resultado debe ser 1111111111111111. Si uno de los bits es cero, un error ha sido detectado.

Chequeo de Redundancia Cíclica

Probablemente el esquema más confiable para la detección de errores es el chequeo de redundancia cíclica (CRC). Con CRC aproximadamente el 99.95% de todos los errores de transmisión se detectan. El CRC se usa generalmente con códigos de 8 bits, tales como EBCDIC o códigos de 7 bits, cuando no se usa paridad.

En Estados Unidos, el código CRC más común es el CRC-16, el cual es idéntico al estándar internacional CCITT V.41. Con el CRC-16 se utilizan 16 bits para el BCS. Esencialmente el carácter CRC es el sobrante de un proceso de división. Un mensaje de datos polimórfico *G(x)* se divide por una función de polinómico del generador *P(x)* el cociente se descarta, y el residuo se trunca en 16 bits y se agrega al mensaje como el BCS. Con la generación de CRC, la división no se logra con un proceso de división aritmética estándar. En vez de usar una resta común, el residuo se deriva de una operación XOR. En el receptor, el flujo de datos y el BCS se dividen por la misma función de generación *P(x).* Si ningún error de transmisión ha ocurrido, el residuo será cero.

El polinomio generado para CRC-16 es

P(x)= X16 + X12 + x S + XO

en donde XO = 1

el número de bits en el código CRC es igual al exponente más alto del polinomio generado. Los exponentes identifican las posiciones del bit que contiene un 1. Por lo tanto b_{16}, b_{12}, y b_o son todos unos y todas las demás posiciones son ceros.

Ahora determinaremos el BSC para los siguientes polinomios generadores de datos y CRC.
Datos = *G(x)*= $x^7 + x^5 + x^4 + x^2 + x^1 + X^O$ o 1011011

CRC $P(x)= x^{s} + X^{4} + X^{1} + X^{O}$ o 110011

Primero *G(x)* es multiplicado por el número de bits en el código CRC, 5.

$X^{5}(X^{7}+ X^{5}+ X^{4} + X^{2} + X^{1} + X^{O}) = X^{12}+ X^{1O} + X^{9} + X^{7} + X^{6} + X^{5} = 1011011100000$

Después divida el resultado por *P(x)*

```
            11001111
          ┌──────────
11010111  │ 1011011100000
            11011
             111101
             110011
                111010
                110011
                 100100
                 110011
                  101110
                    110011
                     111010
                     110011
      1001 = CRC
```

II Señales

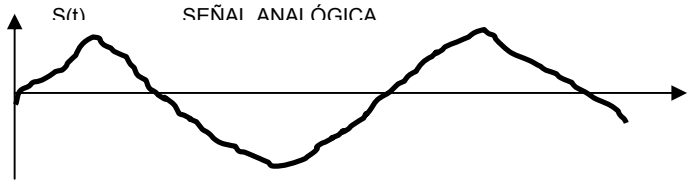
1. Tipos y modulacion.

- ***Introducción.***

Las señales que se pueden transmitir por las redes de comunicaciones, puden ser de dos tipos:señales analogicas y digitales. El comportamiento de estos dos tipos de señales, repectos a los elementos tecnicos que pueden ser parte del hardware de comunicaciones para la construcccion de redes, es tan diferente que da lugar a que estas se puedan clasificar tambien en redes analogicas y redes digitales. De alli la importancia de diferenciar unas de otras.

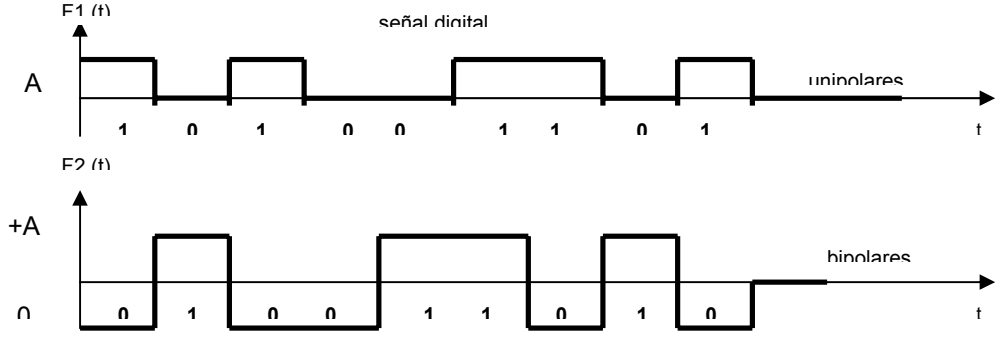
- ***Señales analogicas.***

Son aquellas que están representadas por fuciones que pueden tomar un número **infinito** de valores en cualquier intervalo de tiempo.



- ***Señales digitales*.**

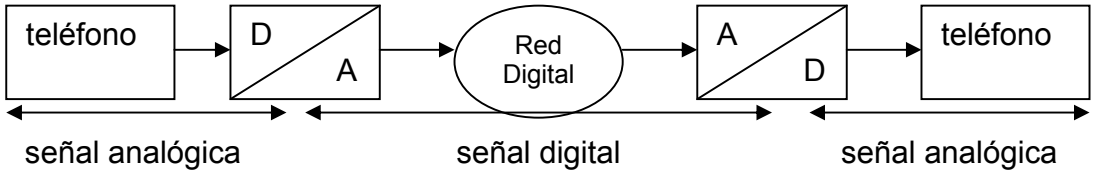
Son aquellas que están representadas por funciones que pueden tomar un numero **finito** de valores en cualquier intervalo de tiempo.



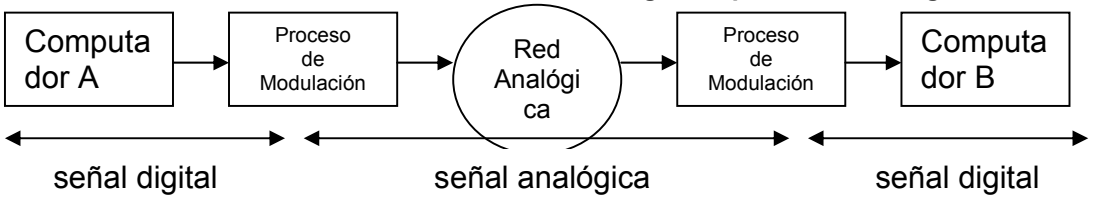
Características de los sistemas de transmisión analógicos y de los sistemas de transmisión digitales:

- Tanto un sistema de transmisión analógico, como uno digital, están capacitados para transportar señales inteligentes que contengan servicios de voz, textos, imágenes y datos.
- Cuando el sistema es analógico, las señales transmitidas contienen la información, en la propia forma de la onda que se transmite.
- Cuando el sistema es digital, las señales transmitidas contienen la información, en la codificación de los pulsos que se transmiten por el medio.
- Existen servicios que son desde el mismo momento que se originan, típicamente analógicos, como lo es la transmisión de voz; y otros típicamente digitales como es la transmisión de datos producida por equipos informáticos en general. Sin embargo, en ambos casos, las señales originales mediante procedimientos especiales, pueden ser transportadas por cualquiera de los 2 tipos de redes.
- En un caso si la red es digital, las señales típicamente analógicas, como la voz deben de ser previamente digitalizadas, para ser transmitidas por estas redes el equipo usado para efectuar esta transmisión se denomina genéricamente "digitalizador"; en cambio las señales digitales para ser transportadas por redes analógicas, deben sufrir previamente un proceso denominado de demodulacion y el equipo usado para efectuar este proceso, de llama "MODEMS".

Transmisión de señales analógicas por redes digitales.

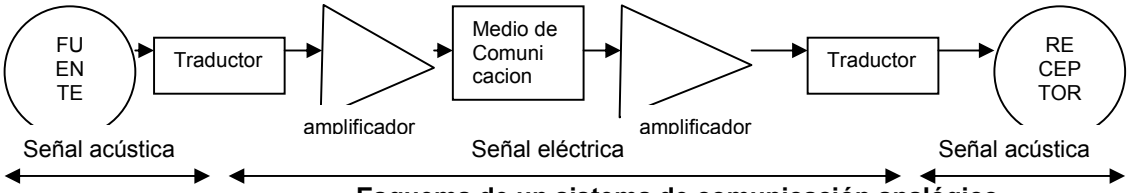


Transmisión de señales digitales por redes analógicas.



Medios que transportan señales analógicas.

Debido a la atenuación propia que se produce en un medio analógico, la señal debe de ser amplificada. Debe tenerse en cuenta que el ruido que acompaña a la señal analógica, también es amplificado conjuntamente con la señal útil, de ahí la tendencia a que los medios de transmisión futuros, sean digitales.

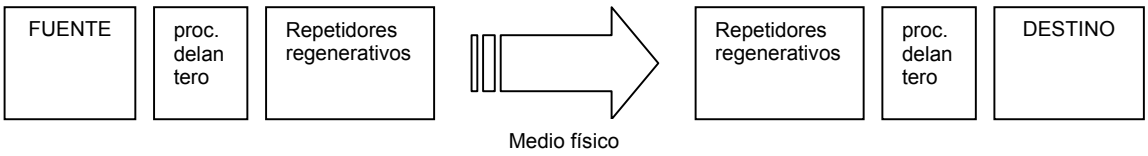


Esquema de un sistema de comunicación analógico.

Medios que transportan señales digitales.

Cuando el medio es digital, la señal debe de ser regenerada debido a la distorsión que este produce en los pulsos transmitidos. Mediante esta acción por medio de un repetidor degenerativo, la señal transmitida mantiene su forma hasta llegar a su destino.

Esquema de un sistema de comunicación digital.



III. Transmisión de datos.

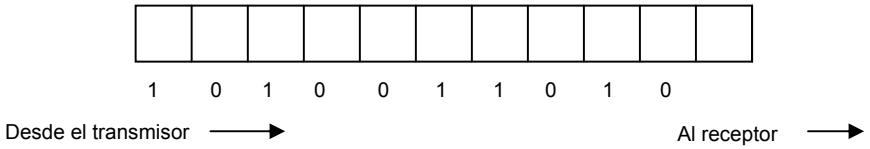
1. Conceptos básicos.

- **Métodos de transmisión (serie y paralelo).**

La transmisión en modo serie es aquella en que los bits que componen cada carácter se transmiten en n ciclos de 1 bit cada uno. Características de la transmisión en modo serie:

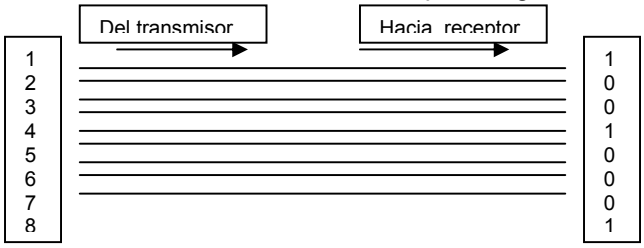
- Se envía un bit después de otro, hasta completar cada carácter.
- Es el típico de los sistemas teleinformáticos.
- Las señales que son transmitidas por los vínculos de telecomunicaciones, al llegar a los equipos informáticos deben pasar al modo paralelo, este proceso se llama deserializacion.
- La secuencia de los bits transmitidos se efectúan siempre, por orden pesos crecientes, n1, n2,.., n8; es decir al revés de cómo se escriben las cifras en el sistema de numeración binaria.

La transmisión en modo serie



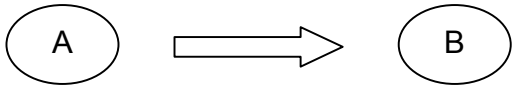
La transmisión en modo paralelo es aquella en que los n bits que componen cada carácter se transmiten en un solo ciclo de n bits. Características de la transmisión en modo paralelo:

- Este es el modo que se usa en las computadoras para realizar la transferencia interna de los datos.
- Se transmite cada conjunto de n bits, seguido por un espacio de tiempo y luego nuevamente otro conjunto de n bits, y así sucesivamente.
- Se pueden usar dos tipos de transmisión distintas: una es de disponer de n líneas diferentes a razón de una por bit a transmitir; la otra, es usar una línea, pero enviando cada bit mediante un procedimiento técnico llamado "multiplexación".
- Se emplean altas velocidades, enviar mas bits en el menor tiempo posible. En este caso las velocidades se miden en bytes por segundo.
- En general no se usa este tipo, cuando las distancias superan las docenas de metros debido a que el tiempo de arribo de los bits difiere de una línea a otra, situación esta que se agrava con el aumento de la distancia.

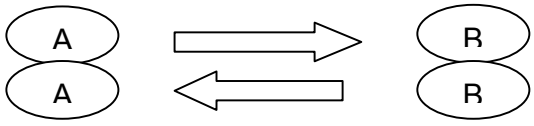


- **Conexiones half duplex y full duplex**

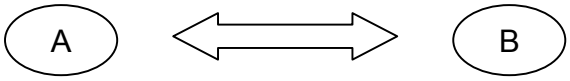
El método simplex es el método de transmisión en que una estación siempre actúa como fuente de y la otra siempre como colector. Permite la transmisión de información en un único sentido. Un Ej. Es el que brindan las agencias de noticias a sus asociados (diarios, estaciones de radio y TV, etc.) los asociados pueden recibir libremente, pero no pueden repreguntar o pedir ampliaciones de las mismas.



El método Half duplex es el método en el que una estación A en un momento determinado tiempo, actúa como fuente y otra estación B actúa como colector y en el siguiente momento, la estación B actuara como fuente y la A como colector. Este método permite la transmisión en dos direcciones, aunque en tiempos diferentes.



El método Full duplex es el método de transmisión en que 2 estaciones A y B, actúan como fuente y receptor, transmitiendo y recibiendo información simultáneamente. Un Ej. Es el de 2 personas conversando telefónicamente en que se habla y se escucha simultáneamente en forma permanente.



- ***Transmisión sincrónica y asincrónica***

En el procedimiento asincronico, cada carácter (byte) a ser transmitido es delimitado por un bit denominado de cabecera o arranque, un o dos bits denominados de terminación o parada. El bit de arranque tiene las funciones de sincronización de los relojes del transmisor y del receptor. El bit de parada, se usa para separar un carácter del siguiente.

2. Medios físicos de transmisión de datos.

Se pueden diferenciar dos grupos:

- Los medios alámbricos (cables).
- Los medios inalámbricos.

Cables

El cable utilizado para formar una red se denomina a veces *medio*. Los tres factores que se deben tener en cuenta a la hora de elegir un cable para una red son:

- Velocidad de transmisión que se quiere conseguir.
- Distancia máxima entre ordenadores que se van a conectar.
- Nivel de ruido e interferencias habituales en la zona que se va a instalar la red.

Los cables más utilizados son el par trenzado, el cable coaxial y la fibra óptica.

- ***Alámbricos (coaxial, par trenzado, fibra óptica)***

Cable coaxial

Consiste en un núcleo de cobre rodeado por una capa aislante. A su vez, esta capa está rodeada por una malla metálica que ayuda a bloquear las interferencias; este conjunto de cables está envuelto en una capa protectora. Le pueden afectar las interferencias externas, por lo que ha de estar apantallado para reducirlas. Emite señales que pueden detectarse fuera de la red. Es utilizado generalmente para señales de televisión y para transmisiones de datos a alta velocidad a distancias de varios kilómetros. La velocidad de transmisión suele ser alta, de hasta 100 Mbits/seg; pero hay que tener en cuenta que a mayor velocidad de transmisión, menor distancia podemos cubrir, ya que el periodo de la señal es menor, y por tanto se atenúa antes. La nomenclatura de los cables Ethernet tiene 3 partes:

- La primera indica la velocidad en Mbits/seg.
- La segunda indica si la transmisión es en Banda Base (BASE) o en Banda Ancha (BROAD).
- La tercera los metros de segmento multiplicados por 100.

CABLE	CARACTERÍSTICAS
10-BASE-5	Cable coaxial grueso (Ethernet grueso). Velocidad de transmisión: 10 Mb/seg. Segmentos : máximo de 500 metros.
10-BASE-2	Cable coaxial fino (Ethernet fino). Velocidad de transmisión: 10 Mb/seg. Segmentos : máximo de 185 metros.
10-BROAD-36	Cable coaxial Segmentos : máximo de 3600 metros. Velocidad de transmisión: 10 Mb/seg.
100-BASE-X	Fast Ethernet. Velocidad de transmisión : 100 Mb/seg.

Par trenzado

Se trata de dos hilos de cobre aislados y trenzados entre sí, y en la mayoría de los casos cubiertos por una malla protectora. Los hilos están trenzados para reducir las interferencias electromagnéticas con respecto a los pares cercanos que se encuentran a su alrededor (dos pares paralelos constituyen una antena simple, en tanto que un par trenzado no). Se pueden utilizar tanto para transmisión analógica como digital, y su ancho de banda depende de la sección de cobre utilizado y de la distancia que tenga que recorrer. Se trata del cableado más económico y la mayoría del cableado telefónico es de este tipo. Presenta una velocidad de transmisión que depende del tipo de cable de par trenzado que se esté utilizando. Está dividido en categorías por el EIA/TIA:

- **Categoría 1**: Hilo telefónico trenzado de calidad de voz no adecuado para las transmisiones de datos. Velocidad de transmisión inferior a 1 Mbits/seg
- **Categoría 2** : Cable de par trenzado sin apantallar. Su velocidad de transmisión es de hasta 4 Mbits/seg.
- **Categoría 3** : Velocidad de transmisión de 10 Mbits/seg. Con este tipo de cables se implementa las redes Ethernet 10-Base-T
- **Categoría 4** : La velocidad de transmisión llega a 16 bits/seg.
- **Categoría 5** : Puede transmitir datos hasta 100 Mbits/seg.

Ventajas

Se trata del cableado más económico y la mayoría del cableado telefónico es de este tipo. Presenta una velocidad de transmisión que depende del tipo de cable de par trenzado que se esté utilizando

Tiene una longitud máxima limitada y, a pesar de los aspectos negativos, es una opción a tener en cuenta debido a que ya se encuentra instalado en muchos edificios como cable telefónico y esto permite utilizarlo sin necesidad de obra. La mayoría de las mangueras de cable de par trenzado contiene más de un par de hilos por lo que es posible encontrar mangueras ya instaladas con algún par de hilos sin utilizarse. Además resulta fácil de combinar con otros tipos de cables para la extensión de redes.

Cable de fibra óptica

Una fibra óptica es un medio de transmisión de la luz que consiste básicamente en dos cilindros coaxiales de vidrios transparentes y de diámetros muy pequeños. El cilindro interior se denomina núcleo y el exterior se denomina envoltura, siendo el índice de refracción del núcleo algo mayor que el de la envoltura. En la superficie de separación entre el núcleo y la envoltura se produce el fenómeno de reflexión total de la luz, al pasar éste de un medio a otro que tiene un índice de refracción más pequeño. Como consecuencia de esta estructura óptica todos los rayos de luz que se reflejan totalmente en dicha superficie se transmiten guiados a lo largo del núcleo de la fibra. Este conjunto está envuelto por una capa protectora. La velocidad de transmisión es muy alta, 10 Mb/seg siendo en algunas instalaciones especiales de hasta 500 Mb/seg, y no resulta afectado por interferencias. Los cables de fibra óptica tienen muchas aplicaciones en el campo de las comunicaciones de datos:

- Conexiones locales entre ordenadores y periféricos o equipos de control y medición.
- Interconexión de ordenadores y terminales mediante enlaces dedicados de fibra óptica.
- Enlaces de fibra óptica de larga distancia y gran capacidad.

Los cables de fibra óptica ofrecen muchas ventajas respecto de los cables eléctricos para transmitir datos:

- Mayor velocidad de transmisión. Las señales recorren los cables de fibra óptica a la velocidad de la luz (c = 3 X 10^9 m/s), mientras que las señales eléctricas recorren los cables a una velocidad entre el 50 y el 80 por cien de ésta, según el tipo de cable.
- Mayor capacidad de transmisión. Pueden lograrse velocidades por encima de 1 Gbit/s.
- Inmunidad total ante interferencias electromagnéticas. La fibra óptica no produce ningún tipo de interferencia electromagnética y no se ve afectada por rayos o por pulsos electromagnéticos nucleares (NEMP) que acompañan a las explosiones nucleares.
- No existen problemas de retorno de tierra, crosstalk o reflexiones como ocurre en las líneas de transmisión eléctricas.
- La atenuación aumenta con la distancia más lentamente que en el caso de los cables eléctricos, lo que permite mayores distancias entre repetidores.
- Se consiguen tasas de error típicas del orden de 1 en 10^9 frente a las tasas del orden de 1 en 10^6 que alcanzan los cables coaxiales. Esto permite aumentar la velocidad eficaz de transmisión de datos, reduciendo el número de retransmisiones o la cantidad de información redundante necesaria para detectar y corregir lo errores de transmisión.
- No existe riesgo de cortocircuito o daños de origen eléctrico.
- Los cables de fibra óptica pesa la décima parte que los cables de corte apuntalados. Esta es una consideración de importancia en barcos y aviones.

- Los cables de fibra óptica son generalmente de menor diámetro, más flexibles y más fáciles de instalar que los cables eléctricos.
- Los cables de fibra óptica son apropiados para utilizar en una amplia gama de temperaturas.
- Es más difícil realizar escuchas sobre cables de fibra óptica que sobre cables eléctricos. Es necesario cortar la fibra para detectar los datos transmitidos. Las escuchas sobre fibra óptica pueden detectarse fácilmente utilizando un reflectómetro en el dominio del tiempo o midiendo las pérdidas de señal.
- Se puede incrementar la capacidad de transmisión de datos añadiendo nuevos canales que utilicen longitudes de onda distintas de las ya empleadas.
- La fibra óptica presenta una mayor resistencia a los ambientes y líquidos corrosivos que los cables eléctricos.
- Las materias primas para fabricar vidrio son abundantes y se espera que los costos se reduzcan a un nivel similar al de los cables metálicos.
- La vida media operacional y el tiempo medio entre fallos de un cable de fibra óptica son superiores a los de un cable eléctrico.
- Los costos de instalación y mantenimiento para grandes y medias distancias son menores que los que se derivan de las instalaciones de cables eléctricos.

La mayor desventaja es que no se puede "pinchar" fácilmente este cable para conectar un nuevo nodo a la red. Las transmisiones de la señal a grandes distancias se encuentran sujetas a atenuación, que consiste en una pérdida de amplitud o intensidad de la señal, lo que limita la longitud del cable. Los segmentos pueden ser de hasta 2000 metros.

- ***Inalámbricos (microondas, infrarrojos, satelital)***

Microondas.

Los enlaces de microondas se utilizan mucho como enlaces allí donde los cables coaxiales o de fibra óptica no son prácticos. Se necesita una línea de visión directa para transmitir en la banda de SHF, de modo que es necesario dispones de antenas de microondas en torres elevadas en las cimas de las colinas o accidentes del terreno para asegurar un camino directo con la intervención de pocos repetidores. Las bandas de frecuencias más comunes para comunicaciones mediante microondas son las de 2,4, 6 y 6.8 GHz. Un enlace de microondas a 140 Mbits/s puede proporcionara hasta 1920 canales de voz o bien varias comunicaciones de canales de 2 Mbits/s multiplexados en el tiempo. Los enlaces de microondas presentan unas tasas de error en el rango de 1 en 10^5 a 1 en 10^{11} dependiendo de la relación señal/ruido en los receptores. Pueden presentarse problemas de propagación en los enlaces de microondas, incluyendo los debidos a lluvias intensas que provocan atenuaciones que incrementan la tasa de errores. Pueden producirse pequeños cortes en la señal recibida cuando una bandada de pájaros atraviesa el haz de microondas, pero es poco frecuente que ocurra.

Infrarrojos.

La luz infrarroja permite la transmisión de información a velocidades muy altas: 10 Mbits/seg. 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.

Satelital.

Señales de radio

Consiste en la emisión/recepción de una señal de radio, por lo tanto el emisor y el receptor deben sintonizar la misma frecuencia. La emisión puede traspasar muros y no es necesario la visión directa de emisor y receptor. La velocidad de transmisión suele ser baja : 4800 Kbits/seg. Se debe tener cuidado con las interferencias de otras señales.

Comunicaciones via satélite

Los satélites artificiales han revolucionado las comunicaciones desde los últimos 20 años. Actualmente son muchos los satélites de comunicaciones que están alrededor de la tierra dando servicio a numerosas empresas, gobiernos, entidades. Un satélite de comunicaciones hace la labor de repetidor electrónico. Una estación terrena A transmite al satélite señales de una frecuencia determinada (canal de subida). Por su parte, el satélite recibe estas señales y las retransmite a otra estación terrena B mediante una frecuencia distinta (canal de bajada). La señal de bajada puede ser recibida por cualquier estación situada dentro del cono de radiación del satélite, y puede transportar voz, datos o imágenes de televisión. De esta manera se impide que los canales de subida y de bajada se interfieran, ya que trabajan en bandas de frecuencia diferentes. La capacidad que posee una satélite de recibir y retransmitir se debe a un dispositivo conocido como transpondedor. Los transpondedores de satélite trabajan a frecuencias muy elevadas, generalmente en la banda de los gigahertzios. La mayoría de los satélites de comunicaciones están situados en una órbita denominada geoestacionaria, que se encuentra a 36000 Km sobre el ecuador. Esto permite que el satélite gire alrededor de la tierra a la misma velocidad que ésta, de modo que parece casi estacionario. Así, las antenas

terrestres pueden permanecer orientadas hacia una posición relativamente estable (lo que se conoce como "sector orbital") ya que el satélite mantiene la misma posición relativa con respecto a la superficie de la tierra.

- Existe un retardo de unos 0.5 segundos en las comunicaciones debido a la distancia que han de recorrer las señales. Los cambios en los retrasos de propagación provocados por el movimiento en ocho de un satélite geoestacionario necesitan transmisiones frecuentes de tramas de sincronización.
- Los satélites tienen una vida media de siete a 10 años, pero pueden sufrir fallos que provocan su salida de servicio. Es, por tanto, necesario dispones de un medio alternativo de servicio en caso de cualquier eventualidad.
- Las estaciones terrenas suelen estar lejos de los usuarios y a menudo se necesitan caros enlaces de alta velocidad. Las estaciones situadas en la banda de bajas frecuencias (la banda C) están dotadas de grandes antenas (de unos 30 metros de diámetro) y son extremadamente sensibles a las interferencias. Por este motivo suelen estar situadas lejos de áreas habitadas. Las estaciones que trabajan en la banda Ku disponen de una antena menor y son menos sensibles a las interferencias. Utilizar un enlace de microondas de alta capacidad sólo ayudaría a complicar los problemas de ruido que presente el enlace con el satélite.
- Las comunicaciones con el satélite pueden ser interceptadas por cualquiera que disponga de un receptor en las proximidades de la estación. Es necesario utilizar técnicas de encriptación para garantizar la privacidad de los datos.
- Los satélites geoestacionarios pasan por periodos en los que no pueden funcionar. En el caso de un eclipse de Sol en el que la tierra se sitúa entre el Sol y el satélite, se corta el suministro de energía a las células solares que alimentan el satélite, lo que provoca el paso del suministro de energía a las baterías de emergencia, operación que a menudo se traduce en una reducción de las prestaciones o en una pérdida de servicio.
- En el caso de tránsitos solares, el satélite pasa directamente entre el Sol y la Tierra provocando un aumento del ruido térmico en la estación terrena, y una pérdida probable de la señal enviada por el satélite.
- Los satélites geoestacionarios no son totalmente estacionarios con respecto a la órbita de la tierra. Las desviaciones de la órbita ecuatorial hace que el satélite describa una figura parecida a un ocho, de dimensiones proporcionales a la inclinación de la órbita con respecto al ecuador. Estas variaciones en la órbita son corregidas desde una estación de control.

Actualmente hay un problema de ocupación de la órbita geoestacionaria. Cuando un satélite deja de ser operativo, debe irse a otra órbita, para dejar un puesto libre. La separación angular entre satélites debe ser de 2 grados (anteriormente era de 4). Esta medida implicó la necesidad de mejorar la capacidad de resolución de las estaciones terrenas para evitar detectar las señales de satélites próximos en la misma banda en forma de ruido.

B. Modelos

I. Arquitecturas.

1. El modelo OSI.

- ***Conceptos básicos (origen, stacks, servicios, protocolos, interfaces, puntos de acceso a los servicios).***

OSI : Open System Interconnections: fue creado a partir del año 1978, con el fin de conseguir la definición de un conjunto de normas que permitieran interconectar diferentes equipos, posibilitando de esta forma la comunicación entre ellos. El modelo OSI fue aprobado en 1983. Un sistema abierto debe cumplir las normas que facilitan la interconexión tanto a nivel hardware como software con otros sistemas (arquitecturas distintas). Un modelo basado en una propuesta desarrollada por la organización internacional de normas(OSI), como un primer paso hacia la normalización internacional de varios protocolos. A este modelo se le conoce como **Modelo de referencia OSI (interconexión de sistemas abiertos) de la ISO, porque se refiere a la conexión de sistemas heterogéneos – es decir, a sistemas dispuestos a establecer comunicación con otros distintos.** El modelo OSI tiene 7 capas. Los principios aplicados para el establecimiento de estas fueron las siguientes:

1. Una capa se creara en situaciones en donde se necesita un nivel diferente de abstracción.
2. Cada capa deberá efectuar una función bien definida.
3. La función que realizara cada capa deberá seleccionarse con la intención de definir protocolos normalizados internacionalmente.

4. Los limites de las capas deberán seleccionarse tomando en cuenta la minimización del flujo de información a través de las interfaces.
5. El numero de capas deberá ser lo suficientemente grande para que las funciones diferentes no tengan que ponerse juntas en la misma capa y, por otra parte, también deberá ser lo suficientemente pequeño para que su arquitectura no llegue a ser difícil de manejar.

Este modelo define los servicios y los protocolos que posibilita la comunicación, dividiéndolos en 7 niveles diferentes, en el que cada nivel se encarga de problemas de distinta naturaleza interrelacionándose con los niveles contiguos, de forma que cada nivel se abstrae de los problemas que los niveles inferiores solucionan para dar solución a un nuevo problema, del que se abstraerán a su vez los niveles superiores.

NIVELES	FUNCIÓN
Aplicación	Semántica de los datos
Presentación	Representación de los datos
Sesión	Diálogo ordenado
Transporte	Extremo a extremo
Red	Encaminamiento
Enlace	Punto a punto
Físico	Eléctrico/Mecánico

Tenga en cuenta que el modelo OSI. Por si mismo, no es una arquitectura de red, dado que no especifica, en forma exacta, los servicios y protocolos que usaran en cada una de las capas. Solo indica lo que cada capa deberá hacer. Sin embargo la ISO también a generado normas para todas las capas, aunque estas, no formen parte del modelo. Cada una de ellas se ha publicado como normas internacionales independientes. Se puede decir que la filosofía de este modelo se basa en la idea de dividir un problema grande (la comunicación en sí), en varios problemas pequeños, independizando cada problema del resto. Es un método parecido a las cadenas de montaje de las fábricas.; los niveles implementan a un grupo de operarios de una cadena, y cada nivel, al igual que en la cadena de montaje, supone que los niveles anteriores han solucionado unos problemas de los que él se abstraerá para dar solución a unos nuevos problemas, de los que se abstraerán los niveles superiores.

SERVICIOS

La verdadera función de las capas OSI consiste en proporcionar servicios a las capas superiores. Las capas pueden ofrecer dos tipos diferentes de servicios a las capas que se encuentras sobre ellas:

1. Orientados a conexión se modelo tomando en cuenta el sistema telefónico. Para poder hablarle a alguien se debe tomar el teléfono, marcar el numero, hablar y colgar. Similarmente, para utilizar una red de servicio orientado a conexión, el usuario del servicio establece primero una conexión, la utiliza y después termina la conexión. El aspecto fundamental de la conexiones que actúa en forma parecida a la de un tubo: el que envía, introduce objetos por un extremo, y el receptor los recoge, en el mismo orden, por le otro extremo.
2. Sin conexión se modela con base en el sistema postal. Cada mensaje (carta) lleva consigo la dirección completa de destino y cada uno de ellos se encamina, en forma independiente, atreves del sistema.

Tipos de servicios:

Orientados a conexión

Servicio	Ejemplo
Flujo de mensaje fiable	Secuencia de paginas
Flujo de octetos fiable	Conexión remota
Conexión no fiable	Voz digitalizada

Sin conexión

Servicio	Ejemplo
Datagrama no fiable	Correo electrónico basura
Datagrama con asentimiento	Correo certificado
Pregunta-respuesta	Interrogación de base de datos

SERVICIO(Def.) Esta formalmente especificado por un conjunto de primitivas (operaciones), a disposición de todos los usuarios o de otras entidades para acceder al servicio. Estas primitivas le indican al servicio que debe efectuar una acción o notifican la acción tomada por una entidad par. Las primitivas de servicio en el modelo OSI pueden dividirse en 4 clases:

Primitiva	Significado
Solicitud	Una entidad desea que el servicio realice un trabajo
Indicación	Una entidad es informada acerca de un evento

Respuesta	Una entidad desea responder a un evento
Confirmación	Una entidad va a ser informada acerca de su solicitud

Los servicios pueden ser confirmados o no confirmados. En un servicio confirmado hay una petición, una indicación, una respuesta y una confirmación. En un servicio sin confirmar, solamente hay una petición y una indicación.

Diferencia entre servicios y protocolos.

Los conceptos de servicio y protocolo tienen un significado diferente. Un servicio es un conjunto de primitivas (operaciones), que una capa proporciona a la superior. El servicio define las operaciones que la capa efectuara en beneficio de sus usuarios, pero no dice nada con respecto a como se realizan dichas operaciones. Un servicio se refiere a una interface entre dos capas, siendo la capa inferior la que provee el servicio y la capa superior la que utiliza el servicio. Un protocolo, es un conjunto de reglas que gobiernan el formato y el significado de las tramas, paquetes o mensajes que son intercambiados por las entidades corres ponsales dentro de una capa. las entidades utilizan protocolos para realizar sus definiciones de servicio, teniendo libertad para cambiar el protocolo, pero asegurándose de no modificar el servicio visible a los usuarios. De esta manera se observa con claridad como los conceptos de servicio y protocolo están completamente desacoplados. Seria conveniente hacer una analogía con los lenguajes de programación. Un servicio es como un tipo de dato abstracto que define las operaciones que pueden efectuarse sobre un objeto, pero no especifica la manera como se realizan estas operaciones. Un protocolo se relaciona con la realización de un servicio y, como tal, no es visible para el usuario del servicio.

Nivel 1: capa física.

La capa física se ocupa de la transmisión de bits a lo largo de un canal de comunicación. Su diseño debe de asegurar que cuando u extremo de envía un bit con valor 1, este se reciba exactamente como un bit con ese valor en el extremo, y no como un bit de valor 0. Preguntas comunes aquí son cuantos voltios deberán utilizarse para representar un bit de valor 1 o 0; cuantos microsegundos deberán durar un bit; la posibilidad de realizar transmisiones bidireccionales en forma simultanea la forma de establecer la conexión inicial y cuando interrumpirla cuando ambos extremos terminan su comunicación; o bien, cuantas puntas terminales tiene el conector de la red y cual es el uso de cada una de ellas. Los problemas de diseño a considerar aquí son los aspectos mecánicos, eléctricos, de procedimiento de interfase y el medio de transmisión física, que se encuentra bajo la capa física, este diseño cae en el dominio del ingeniero eléctrico.

Nivel 2: capa de enlace.

La tarea primordial de la capa de enlace consiste en, a partir de la transmisión común y corriente, trasnformarlo en una línea sin errores de transmisión para la capa de red. Esta tarea se realiza al hacer que el emisor trocee la entrada de datos en tramas de datos(típicamente constituidas por algunos cientos de octetos), y las transmita en forma secuencial y procese las tramas de asentimiento, devueltas por el receptor. Como la capa física básicamente acepta y transmite un flujo de bits sin tener en cuenta su significado o estructura, recae sobre la capa de enlace la creación o reconocimiento de los limites de la trama. Esto puede llevarse a cabo mediante la inclusión de un patrón de bit especial al inicio y al termino de la trama. Otro de los problemas que aparecen en la capa de enlace(y también en la mayoría de las capas superiores) es él referente a como evitar que un transmisor muy rápido sature con datos a un receptor lento. se usaran procedimientos de regulación de flujo y control de errores. Otra dificultad aparece cuando la línea tiene la capacidad de utilizarse para la transmisión de datos bidireccionalmente.

Nivel 3: capa de red.

La capa de red se ocupa del control de la operación de la subred. Un punto de suma importancia en su diseño, es la determinación sobre como encaminar los paquetes del origen al destino.

Nivel 4: capa de transporte.

La función principal de la capa de transporte consiste en aceptar los datos de la capa de sesión, dividirlos, siempre que sea necesario, en unidades más pequeñas, pasarlos a la capa de la red asegurar que todos ellos lleguen correctamente al otro extremo. Bajo condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de la transporte solicitada por la capa de sesión. La capa de transporte determina que tipo de transporte determina que tipo de servicio debe de dar a la capa de sesión y en ultimo termino a los usuarios de la red. La capa de transporte es una capa de tipo origen-destino o extremo a extremo. Es decir, un programa en la maquina origen lleva una conversación con un programa parecido que esta en la maquina destino, utilizando las cabeceras de los mensajes y los mensajes de control.

Nivel 5: capa de sesión.

Esta capa permite que los usuarios de diferentes maquinas puedan establecer sesiones entre ellos. Atreves de una sesión se puede llevar acabo un transporte de datos ordinario, tal y como lo hace la capa de transporte, pero mejorando los servicios que esta proporciona y que se utiliza en algunas aplicaciones. Una sesión podría permitir al usuario acceder a un sistema de tiempo compartido a distancia, o transferir un archivo entre dos maquinas. Uno de los servicios de la capa de sesión consiste en gestionar el control de dialogo. Las sesiones permiten que el trafico

vaya en ambas direcciones al mismo tiempo, o bien, en una sola dirección en un instante dado. Si el trafico puede ir en una dirección en un momento dado(en forma análoga aun solo sentido en una vía de ferrocarril), la capa de sesión ayudara en el seguimiento de quien tiene el turno. La administración del testigo es otro de los servicios relacionados con la capa de sesión. Para el caso de algunos protocolos resulta esencial que ambos lados no traten de realizar la misma operación en el mismo instante. Solamente el extremo con el testigo puede realizar la operación critica.
Otro de los servicios que ofrece la capa de sesión es la sincronización.

Nivel 6: capa de presentación.

Realiza ciertas funciones que se necesitan bastante a menudo como para buscar una solución general para ellas, mas que dejar que cada uno de los usuarios resuelva los problemas. Esta capa se ocupa de los aspectos de sintaxis y semántica de la información que se transmite. Un ejemplo típico de servicio de la capa de presentación es el relacionado con la codificación de datos conforme lo acordado previamente. Para posibilitar la comunicación entre ordenadores con diferentes representaciones, la estructura de los datos que se va a intercambiar puede definirse en forma abstracta, junto con una norma de codificación que se utilice en el cable, este trabajo se lleva a cabo atreves de la capa de presentación. Otros aspectos que se manejan en esta capa es la compresión de datos que se puede usar aquí para reducir él numero de bits que tienen que transmitirse, y el concepto de criptografía se necesita utilizar por razones de privacidad y de autentificación.

Nivel 7: capa de aplicación.

Contiene una variedad de protocolos que se necesitan frecuentemente. Una forma de resolver este problema consiste de definir un terminal virtual de red abstracto, con el que los editores y otros programas pueden ser escritos para tratar con el. Con el objeto de transferir funciones de terminal virtual de una red a una terminal real. El software completo de terminal virtual se encuentra en la capa de aplicación. Otra función de esta capa es la transferencia de archivos, el correo electrónico, la entrada de trabajo a distancia, el servicio de directorio y otros servicios.

2. Evolución de las redes.

- ***Clasificación de las redes por cobertura*.**
- ***Sistemas propietarios (SNA,DNA).***

SNA (ARQUITECTURAS DE REDES DE SISTEMAS). Es una arquitectura de red que permite que los clientes de IBM construyan sus propias redes privadas, tomando en cuenta a los hostales y la subred. Por Ej.: un banco puede tener un a o más cpus en su depto de proceso de datos, y numerosos terminales en cada una de sus terminales en cada una de sus sucursales. Con el uso de SNA todos estos componentes aislados pueden transformarse en un sistema coherente. Una red **SNA** esta constituida por una colección de maquinas denominadas **nodos**, de los cuales hay 4 tipos, que se caracterizan aproximadamente de la siguiente manera:

Tipo 1	Son los terminales
Tipo 2	Son los controladores, es decir, son las maquinas que supervisan el funcionamiento de las terminales y los periféricos.
Tipo 4	Son los procesadores frontales, es decir aquellos dispositivos cuya función consiste en reducir la carga del CPU principal y realizar el manejo de interrupciones asociadas con la comunicación de datos.
Tipo 5	Son los hostales principales, aunque, con la aparición de los microprocesadores de bajo costo, algunos controladores han adquirido algunas propiedades de hostales.

*****no hay nodos de tipo 3.

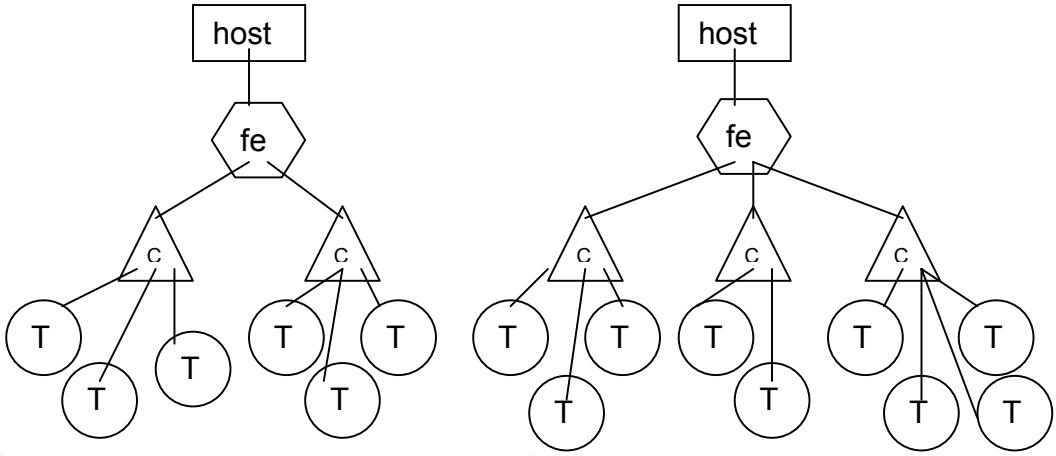
Cada uno de los nodos contiene uno o mas NAU(unidad direccionable de red, **UDR**), que son una pieza de software a través de la cual se permite que un proceso utilice la red; Puede considerarse como un SAP(punto de acceso a servicio), mas las entidades que proporcionan los servicios de las capas superiores. Para usar la red, el proceso debe conectarse directamente a una NAU y a partir de ese momento puede direccionarse y direccionar otras NAU. Las NAU son los puntos de entrada ala red para los procesos del usuario.

Hay 3 tipos diferentes de NAU:

Unidad Lógica(UL)	Es la variedad mas usual a la que se unen los proc de usuario
Unidad física (UF)	Se proporciona una forma de direccionar en la red un dispositivo físico, sin tener en cuenta los procesos que la están utilizando. La red la utiliza para poner al nodo en línea, dejarlo fuera de línea, probarlo y ejecutar funciones parecidas al administrador de redes.
Punto de control en los servicios de sistemas (SSCP)	Tiene un conocimiento completo de, y a su vez control sobre, todos los procesadores frontales, controladores y terminales unidos o ligados al host. Normalmente hay uno por cada tipo de nodo 5 y ninguno de los

	otros.

Se conoce como dominio al conjunto de hardware y software manejados por un SSCP. Ejemplo de una red SNA simple de 2 dominios:



Una red SNAde dos dominios. Fe=procesador central, C=controlador,T=terminal.

- ***Sistemas abiertos (DOD,IEEE).***

IEEE(Instituto de Ingenieros Eléctricos y Electrónicos).

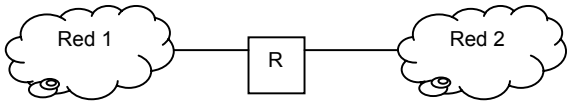
Es un participante importante en el uso de las normas, es la organización profesional mas grande del mundo. Esta institución, además de publicar numerosas revistas y programar un numero importante de conferencias anuales, ha establecido un grupo dedicado al desarrollo de normas en el área de ingeniería eléctrica y computación. La norma 802 del IEEE, para una red de área Local, es la norma clavé para el desarrollo de las Lan. Posteriormente fue adoptada por la ISO como base para la norma ISO 8802.

- ***Red de redes.***

La meta es construir una interconexión de redes, unificada y cooperativa, que incorpore un servicio universal de comunicación. Dentro de cada red las computaras utilizan funciones de comunicación sin importar la tecnología. El nuevo software, incorporado entre los servicios de comunicación de tecnología independiente y los programas de aplicación, ocultara los detalles de bajo nivel y hará que el grupo de redes parezca ser una sola y gran red. Un esquema de interconexión como este se conoce como RED DE REDES o INTERNET.

ARQUITECTURA DE INTERNET.

Las computadoras que interconectan dos redes y transfieren paquetes de una a otra se conocen como pasarelas o compuertas IP o ruteadores IP. En la figura el ruteador R conecta las redes1 y 2. para que R actúe como ruteador, debe capturar y transferir los paquetes de la red1 a la red 2 y viceversa.



Cada red puede ser una LAN o una WAN y cada una puede tener pocos o muchos anfitriones conectados. En una red de redes TCP/IP, las computadoras llamadas ruteadores o pasarelas proporcionan todas las interconexiones entre las redes físicas. Los ruteadores utilizan la red de destino, no el anfitrión de destino, cundo rutean un paquete. Los protocolos TCP/IP para Internet tratan de manera igual a todas las redes. Una LAN como ethernet, una WAN como la columna vertebral de ANSNET o un enlace punto a punto entre os maquinas se cuentan como redes individuales.

3. REDES LOCALES (LAN).

- ***Introducción a las redes locales***

Lo primero que se puede preguntar un usuario cuando se plantea la posibilidad de instalación o utilización de una red local, es saber cómo va a mejorar su trabajo en el ordenador al utilizar dicho entorno. La respuesta va a ser diferente

según el tipo de trabajo que desempeñe. En resumen, una red local proporciona la facilidad de compartir recursos entre sus usuarios. Esto es:

- Supone compartir ficheros.
- Supone compartir impresoras.
- Se pueden utilizar aplicaciones específicas de red.
- Se pueden aprovechar las prestaciones cliente/servidor.
- Se puede acceder a sistemas de comunicación global.

Compartir ficheros

La posibilidad de compartir ficheros es la prestación principal de las redes locales. La aplicación básica consiste en utilizar ficheros de otros usuarios, sin necesidad de utilizar el disquete. La ventaja fundamental es la de poder disponer de directorios en la red a los que tengan acceso un grupo de usuarios, y en los que se puede guardar la información que compartan dichos grupos. Ejemplo: se crea una carpeta para el departamento de contabilidad, otra para el departamento comercial y otra para el departamento de diseño, facilita que estos usuarios tengan acceso a la información que les interesa de forma instantánea. Si a esto se añaden aplicaciones concretas, entonces el trabajo en grupo mejora bastante con la instalación de la Intranet. Esto se aprecia en las aplicaciones de bases de datos preparadas para el trabajo en redes locales (la mayoría de las actuales), lo que permite que varios usuarios puedan acceder de forma simultánea a los registros de la base de datos, y que las actualizaciones que realice un operador queden inmediatamente disponibles para el resto de los usuarios.

Impresión en red

Las redes locales permiten que sus usuarios puedan acceder a impresoras de calidad y alto precio sin que suponga un desembolso prohibitivo. Por ejemplo, si tenemos una oficina en la que trabajan siete personas, y sus respectivos ordenadores no están conectados mediante una red local, o compramos una impresora para cada usuario (en total siete), o que cada usuario grabe en un disquete su documento a imprimir y lo lleve donde se encuentra la impresora. Si hay instalada una red local, lo que se puede hacer es comprar una o dos impresoras de calidad, instalarlas y que los usuarios las compartan a través de la red. Cuando se comparte una impresora en la red, se suele conectar a un ordenador que actúa como servidor de impresión, y que perfectamente puede ser el equipo de un usuario.

Aplicaciones de red

Existe un gran número de aplicaciones que aprovechan las redes locales para que el trabajo sea más provechoso. El tipo de aplicaciones más importante son los programas de correo electrónico. Un programa de correo electrónico permite el intercambio de mensajes entre los usuarios. Los mensajes pueden consistir en texto, sonido, imágenes, etc. y llevar asociados cualquier tipo de ficheros binarios. En cierto modo el correo electrónico llega a sustituir a ciertas reuniones y además.

Sistema distribuido y red local

No se debe confundir una red local con un sistema distribuido. Aunque parezca que son conceptos similares difieren en algunas cosas. Un sistema distribuido es multiusuario y multitarea. Todos los programas que se ejecuten en un sistema distribuido lo van a hacer sobre la CPU del servidor en lo que en términos informáticos se denomina "tiempo compartido". Un sistema distribuido comparte la CPU. Sin embargo, en una Intranet, lo que en realidad se denomina servidor, lo es, pero de ficheros o de bases de datos. Cada usuario tendrá un ordenador autónomo con su propia CPU dónde se ejecutarán las aplicaciones que correspondan. Además, con la aparición de la arquitectura cliente/servidor, la CPU del servidor puede ejecutar algún programa que el usuario solicite. Una red local puede tener distintas configuraciones que se verán más adelante, pero básicamente se pueden hablar de dos tipos:

- **Red con un servidor**: existe un servidor central que es el “motor” de la red. El servidor puede ser activo o pasivo dependiendo del uso que se le dé.
- **Peer to peer**: Una red de igual a igual. Todos los puestos de la red pueden hacer la función de servidor y de cliente.

En una Intranet, interesa tener un servidor Web, que será la parte más importante de la red.

- ***Topologías***

La topología de una red define únicamente la distribución del cable que interconecta los diferentes ordenadores, es decir, es el mapa de distribución del cable que forma la Intranet. Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta y son:

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones que se van a ejecutar.

- La inversión que se quiere hacer.
- El coste que se quiere dedicar al mantenimiento y actualización de la red local.
- El tráfico que va a soportar la red local.
- La capacidad de expansión. Se debe diseñar una Intranet teniendo en cuenta la escalabilidad.

No se debe confundir el término topología con el de arquitectura. La arquitectura de una red engloba:

- La topología.
- El método de acceso al cable.
- Protocolos de comunicaciones.

Actualmente la topología está directamente relacionada con el método de acceso al cable, puesto que éste depende casi directamente de la tarjeta de red y ésta depende de la topología elegida.

Topología física

Es lo que hasta ahora se ha venido definiendo; la forma en la que el cableado se realiza en una red. Existen tres topología físicas puras:

- Topología en anillo.
- Topología en bus.
- Topología en estrella.

Existen mezclas de topologías físicas, dando lugar a redes que están compuestas por mas de una topología física.

Topología lógica

Es la forma de conseguir el funcionamiento de una topología física cableando la red de una forma más eficiente. Existen topologías lógicas definidas:

- Topología anillo-estrella: implementa un anillo a través de una estrella física.
- Topología bus-estrella: implementa una topología en bus a través de una estrella física.

TOPOLOGÍA EN BUS

Consta de un único cable que se extiende de un ordenador al siguiente de un modo serie. Los extremos del cable se terminan con una resistencia denominada **terminador,** que además de indicar que no existen más ordenadores en el extremo, permiten cerrar el bus.

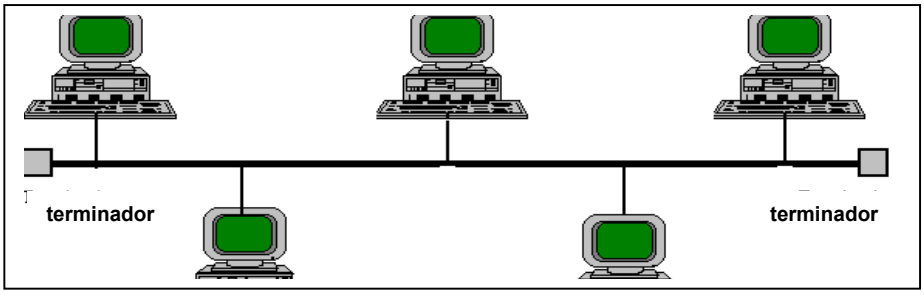
Sus principales ventajas son :

- Fácil de instalar y mantener.
- No existen elementos centrales del que dependa toda la red, cuyo fallo dejaría inoperativas a todas las estaciones.

Sus principales inconvenientes son:

- Si se rompe el cable en algún punto, la red queda inoperativa por completo.

Cuando se decide instalar una red de este tipo en un edificio con varias plantas, lo que se hace es instalar una red por planta y después unirlas todas a través de un bus troncal.



TOPOLOGÍA EN ANILLO

Sus principales características son:

- El cable forma un bucle cerrado formando un anillo.
- Todos los ordenadores que forman parte de la red se conectan a ese anillo.
- Habitualmente las redes en anillo utilizan como método de acceso al medio el modelo “paso de testigo”.

Los principales inconvenientes serían:

- Si se rompe el cable que forma el anillo se paraliza toda la red.
- Es difícil de instalar.
- Requiere mantenimiento.

TOPOLOGÍA EN ESTRELLA

Sus principales características son :

- Todas las estaciones de trabajo están conectadas a un punto central (concentrador), formando una estrella física.
- Habitualmente sobre este tipo de topología se utiliza como método de acceso al medio poolling, siendo el nodo central el que se encarga de implementarlo.
- Cada vez que se quiere establecer comunicación entre dos ordenadores, la información transferida de uno hacia el otro debe pasar por el punto central.
- existen algunas redes con esta topología que utilizan como punto central una estación de trabajo que gobierna la red.
- La velocidad suele ser alta para comunicaciones entre el nodo central y los nodos extremos, pero es baja cuando se establece entre nodos extremos.
- Este tipo de topología se utiliza cuando el trasiego de información se va a realizar preferentemente entre el nodo central y el resto de los nodos, y no cuando la comunicación se hace entre nodos extremos.
- Si se rompe un cable sólo se pierde la conexión del nodo que interconectaba.
- es fácil de detectar y de localizar un problema en la red.
- Si se rompe el cable que forma el anillo se paraliza toda la red.
- Es difícil de instalar.
- Requiere mantenimiento.

- ***Características y servicios de los sistemas operativos para LAN's***

4. Redes metropolitanas (MAN).

- ***Características y servicios de las MAN's***

(METROPOLITAN AREA NETWORK)Cualquiera de las nuevas tecnologías de red que operan a altas velocidades (Por lo general, de cientos de megabits a varios gigabits por segundo) en distancias que abarcan un área metropolitana.

5. Redes amplias(WAN).

- ***Características y servicios de las WAN's***

(WIDE AREA NETWORK) cualquier tecnología de red que abarca distancias geográficas extensas. También llamadas redes de largo alcance. Las WAN actualmente operan a bajas velocidades y tienen retardos significativamente mayores que las redes que operan sobre distancias cortas.

Características y servicios Redes de Area Extensa (WAN)

Cuando se llega a un cierto punto deja de ser poco práctico seguir ampliando una LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Dos de los componentes importantes de cualquier red son la red de teléfono y la de datos. Son enlaces para grandes distancias que amplían la LAN hasta convertirla en una red de área extensa (WAN).

El método más común para conectar las LAN y formar una WAN es usar los servicios de conexión, que proporciona la compañía telefónica. La compañía telefónica proporciona diversos servicios para conectar las LAN, y cada uno de ellos soporta varias velocidades de comunicación. Un puente o un ruteador conectado a una unidad de servicio de canal/unidad de servicio digital (CSU/DSU) conecta la LAN a la WAN, como se muestra en la figura siguiente.

Un CSU/DSU es un módem muy avanzado de alta velocidad que conecta a la red con las líneas telefónicas. Los servicios de la compañía telefónica incluyen conexiones conmutadas, líneas alquiladas y conmutación de paquetes. Una conexión conmutada es una conexión temporal a la WAN que se establece cada vez que se necesita. Una línea alquilada (privada) es una conexión permanente a la LAN. La conmutación de paquetes es un servicio que permite conexiones entre varias LAN.

Una Red Wan: es una red de gran cobertura en la cual pueden transmitirse datos a larga distancia, nterconectando facilidades de comunicación entre diferentes localidades de un país. En estas redes por lo general se ven implicadas las compañías telefónicas.

Componentes Físicos

-

Línea de Comunicación: medios físicos para conectar una posición con otra con el propósito de transmitir y recibir datos.

Hilos de Transmisión: en comunicaciones telefónicas se utiliza con frecuencia el termino "pares" para describir el circuito que compone un canal. Uno de los hilos del par sirve para transmitir o recibir los datos, y el otro es la línea de retorno eléctrico.

Clasificación Líneas de Comunicación

Líneas Conmutadas: líneas que requieren de marcar un código para establecer comunicación con el otro extremo de la conexión.

Líneas Dedicadas: líneas de comunicación que mantienen una permanente conexión entre dos o más puntos. Estas pueden ser de dos o cuatro hilos.

Líneas Punto a Punto: enlazan dos DTE

Líneas Multipunto: enlazan tres o más DTE

Líneas Digitales: en este tipo de línea, los bits son transmitidos en forma de señales digitales. Cada bit se representa por una variación de voltaje y esta se realiza mediante codificación digital en la cual los códigos más empleados son:

NRZ (Non Return to Zero) Unipolar.
La forma de onda binaria que utilizan normalmente las computadoras se llama **Unipolar,** es decir, que el voltaje que representa los bits varia entre 0 voltios y +5 voltios. Se denomina NRZ porque el voltaje no vuelve a cero entre bits consecutivos de valor uno. Este tipo de código es inadecuado en largas distancias debido a la presencia de niveles residuales de corriente continua y a la posible ausencia de suficientes números de transiciones de señal para permitir una recuperación fiable de una señal de temporización.

Código NRZ Polar: este código desplaza el nivel de referencia de la señal al punto medio de la amplitud de la señal. De este modo se reduce a la mitad la potencia requerida para transmitir la señal en comparación con el Unipolar.

Transmisión Bipolar o AMI (Alternate Marks Inverted): es uno de los códigos **más empleados** en la transmisión digital a través de redes WAN. Este formato no tiene componente de corriente continua residual y su potencia a frecuencia cero es nula. Se verifican estos requisitos transmitiendo pulsos con un ciclo de trabajo del 50% e invirtiendo alternativamente la polaridad de los bits 1 que se transmiten. Dos valores positivos sin alternancia entre ellos serán interpretados como un error en la línea. los 0's son espacios sin presencia de voltaje. El formato Bipolar es en realidad una señal de tres estados (+V, 0, -V).

- ***Protocolos para WAN's***

Frame Relay

Es un protocolo de transporte, orientado a la tecnología de conmutación de paquetes con velocidades desde 2.4 bps hasta 45Mbps e incluso mayores en algunas implementaciones. Inicialmente fue concebido para el transporte de datos, pero nuevos desarrollos permiten el transporte de voz y ahora vídeo, su uso es generalizado en el backbone de redes de datos, para el transporte de protocolos heredados (legacy protocols) y conexión de enrutadores.

Frame Relay fue concebido originalmente como un protocolo para uso sobre interfaces ISDN (interfaces para la Red Digital de Servicios Integrados), proporciona la capacidad de comunicación de paquetes de conmutación de datos que es usada a través de la interface entre los dispositivos de usuario (por ejemplo, routers, puentes, máquinas hosts,...) y equipos de red (por ejemplo, nodos de intercambio). la red que proporciona la interface Frame Relay puede ser o una red pública o una red de equipos privados sirviendo a una sola empresa.

Su característica primaria más competitiva es el bajo coste (frente a ATM, más rápido pero también mucho más costoso). Hay dos condiciones básicas que deberían existir para justificar la utilización de frame relay. :

- La línea de transmisión debe ser buena. Frame Relay solo funcionará eficientemente si la tasa de error del medio físico es baja.

- Los nodos conectados a Frame Relay no deben ser terminales tontos, sino que correrán sus propios protocolos para control de flujo, recuperación de errores y envío de asentimientos.

Características de Frame Relay.

Como interface a una red, Frame Relay es del mismo tipo de protocolo que X.25. Sin embargo, Frame Relay difiere significativamente de X.25 en su funcionalidad y formato. En particular, Frame Relay es un protocolo más perfeccionado, que proporciona un desarrollo más alto y una mayor eficiencia.

Frame Relay es una forma simplificada de la conmutación de paquetes , similar en principio a X.25, en la cual las tramas de datos síncronas son enrutadas a diferentes destinos dependiendo de su información de cabecera.

La gran diferencia entre Frame Relay y X.25 es que X.25 garantiza la integridad de los datos y la red maneja el flujo de control, a costa de algún retraso en la red. Frame relay conmuta las tramas mucho más rápido extremo a extremo, pero no hay garantía de que la integridad de los datos se total.

Como interface entre usuario y equipo de red, Frame Relay proporciona unos métodos para multiplexar satisfactoriamente muchas conversaciones lógicas de datos (relacionados con circuitos virtuales) sobre un único enlace físico de transmisión. Esto contrasta con los sistemas que usan sólo técnicas de multiplexación por división en el tiempo (TDM) para soportar múltiples flujos de datos. Frame Relay tiene multiplexación estadística que proporciona un uso más flexible y eficiente del ancho de banda disponible. Puede ser usada sin técnicas TDM o sobre los canales proporcionados por sistemas TDM.

Otra característica importante de Frame Relay es que explota los recientes avances en la tecnología de transmisión en redes de área amplia (WAN). Los protocolos más tempranos de transmisión en WAN's como X.25 fueron desarrollados cuando los sistemas de transmisión analógica y por medios de cobre predominaban. Estos enlaces son mucho menos seguros que los medios de fibra y los enlaces de transmisión digital disponibles hoy en día. Sobre enlaces como éstos, los protocolos de la capa de enlace pueden prescindir del tiempo que se gasta en aplicar algoritmos de corrección de errores, dejando que éstos sean desarrollados por capas de niveles superiores.

Un mayor desarrollo y eficiencia es así posible sin sacrificar la integridad de los datos. Frame Relay incluye un algoritmo de chequeo cíclico redundante (CRC) para detectar bits corruptos (así el dato puede ser descartado), pero no incluye ningún mecanismo de protocolo para corregir los datos erróneos. Frame Relay, por tanto, no incluye procedimientos explícitos de control de flujo que duplique los existentes en capas superiores . De hecho, sólo se proporcionan unos mecanismos muy simples de notificación de congestión , para permitir a una red informar a un dispositivo de usuario que los recursos de red están cerca de un estado de congestión. Esta notificación puede avisar a los protocolos de las capas más altas de que el control de flujo puede necesitarse.

Frame Relay es de un coste efectivo, ello es debido en parte a que los requerimientos de almacenamiento en la red están cuidadosamente optimizados. También puede ser usada como una interface a un proveedor público de servicios o a una red de equipo privado. Un método típico de implementación de red privada es equipar los tradicionales multiplexores T1 con interfaces Frame Relay para dispositivos de datos, así como interfaces no-Frame Relay para otras aplicaciones tales como voz y video-teleconferencia.

Un servicio público Frame Relay es desplegado poniendo equipos Frame Relay de conmutación en las oficinas centrales de un proveedor de telecomunicaciones. En este caso, los usuarios pueden obtener beneficios económicos de las limitaciones de cargos sensibles al tráfico, y son relevados del trabajo necesario que conlleva administrar y mantener el equipo de red y el servicio.

De este modo, los tradicionales conmutadores de circuitos, conmutadores de paquetes, o una combinación híbrida de estas tecnologías pueden ser usadas.

Un servicio público Frame Relay es desplegado poniendo equipos Frame Relay de conmutación en las oficinas centrales de un proveedor de telecomunicaciones. En este caso, los usuarios pueden obtener beneficios económicos

de las limitaciones de cargos sensibles al tráfico, y son relevados del trabajo necesario que conlleva administrar y mantener el equipo de red y el servicio.

ATM

ATM (Asynchronous Transfer Mode / "Modo de Transferencia Asyncrono") es un protocolo de transporte de alta velocidad, sus implementaciones actuales son en la red local en compañías que requieren grandes anchos de banda (ATM es capaz de ofrecer servicios de hasta 155 Mbps) y en la red amplia como backbone de conmutación de las redes que lo requieren y que además tiene factibilidad de conexión a redes de alta velocidad (Principalmente carriers y proveedores de servicio).

ATM es radicalmente un nuevo tipo de tecnología de switching basada en celdas, está basada en ISDN Broadband (B-ISDN). ATM se dio a conocer en el mundo a partir de 1990. Si usamos ATM, la información a enviar es dividida en paquetes de longitud fija. Estos son mandados por la red y el destinatario se encarga de poner los datos en su estado inicial. Los paquetes en ATM tienen una longitud fija de 53 bytes. Siendo la longitud de los paquetes fija, permite que la información sea transportada de una manera predecible. El hecho de que sea predecible permite diferentes tipos de trafico en la misma red.

Los paquetes están divididos en dos partes, la cabecera y payload. El payload (que ocupa 48 bytes) es la parte del paquete donde viaja la información, ya sean datos, imágenes o voz. La cabecera (que ocupa 5 bytes) lleva el mecanismo direcccionamiento.

Otro concepto clave es que ATM está basado en el uso de conmutadores. Hacer la comunicación por medio de un conmutador (en vez de un bus) tiene ciertas ventajas: Reserva de ancho de banda para la conexión, Mayor ancho de banda, Procedimientos de conexión bien definidos, Velocidades de acceso flexibles. ATM es una arquitectura estructurada en capas que permite que múltiples servicios como voz y datos vayan mezclados en la misma red. Tres de las capas han sido definidas para implementar los rasgos del ATM.

La capa de adaptación garantiza las características apropiadas del servicio y divide todos los tipos de datos en payload de 48 bytes que conformaran el paquete ATM. La capa intermedia de ATM coge los datos que van a ser enviados y añade los 5 bytes de la cabecera que garantiza que el paquete se envía por la conexión adecuada. La capa física define las características eléctricas y los interfaces de la red. ATM no esta ligado a un tipo especifico de transporte físico.}

ATM y sus Beneficios:

Una única red ATM dará cabida a todo tipo de trafico(voz, datos y vídeo). ATM mejora la eficiencia y manejabilidad de la red.

- Capacita nuevas aplicaciones - debido a su alta velocidad y a la integración de los tipos de trafico, ATM capacitara la creación y la expansión de nuevas aplicaciones como la multimedia.

- Compatibilidad : porque ATM no esta basado en un tipo especifico de transporte físico, es compatible con las actuales redes físicas que han sido desplegadas. ATM puede ser implementado sobre par trenzado, cable coaxial y fibra óptica.

- Simplifica el control de la Red - ATM esta evolucionando hacia una tecnología standard para todo tipo de comunicaciones. Esta uniformidad intenta simplificar el control de la red usando la misma tecnología para todos los niveles de la red.

- Largo periodo de vida de la arquitectura- Los sistemas de información y las industrias de telecomunicaciones se están centrando y están estandarizado el ATM. ATM ha sido diseñado desde el comienzo para ser flexible en: Distancias geográficas, Numero de usuarios, Acceso y ancho de banda.

ATM y algunas debilidades:

Muchos analistas de la industria ven a ATM como un término largo, una tecnología estratégica, y que finalmente todas las LAN tenderán hacia ATM. Sin embargo, ATM es radicalmente distinto a las tecnologías LAN de hoy en día,

lo cual hace que muchos conceptos tomen años en ser estandarizados. los sistemas operativos actuales y las familias de protocolos en particular, requerirán de modificaciones significativas con el fin de soportar ATM. Esto será muy costoso, molesto y consumirá tiempo.

Algunas personas pagarán mucho por estar en la punta de la tecnología, pero por los momentos, las actuales tecnologías de alta velocidad como FDDI, Fast Ethernet e Ehernet Switched proveerán rendimiento a precios que los productos ATM no serán capaz de competir. Sólo una vez que las ventas de ATM alcancen volúmenes significativos el costo de los productos podrán competir con la tecnología de hoy en día.

ATM y Frame Relay, Competencia o Coexistencia.

Los Forums Frame Relay y ATM han ratificado ya algunas normas cuya importancia no sólo reside en ayudar a proteger las inversiones realizadas en equipos Frame Relay actuales, sino también en proporcionar un método adecuado de migración a ATM. Dichos estándares también facilitan accesos de bajo coste a usuarios de Frame Relay remotos a las redes troncales corporativas basadas en ATM.

Hay dos tipos de interoperatividad: de red y de servicio. Ambas son el campo respectivo de atención de los estándares Frame Relay/ATM Network interworking y Frame Relay/ATM Service Interworking, ratificados en diciembre de 1994 y abril de 1995, también respectivamente. Más reciente, la norma Frame UNI (FUNI) representa una tercera alternativa.

Interopertavidad de Red y Servicio

Frame Relay/ATM Network Interworking permite a los usuarios finales de dispositivos o redes Frame Relay comunicar entre sí a través de una red ATM sin necesidad de efectuar ningún cambio de equipamiento. La interoperatividad de red se produce cuando se utiliza un protocolo en cada extremo de la transmisión y otro distinto en el camino entre ambos puntos. En un punto de la red, y de forma totalmente transparente para el usuario, los paquetes Frame Relay son segmentados en celdas ATM, que, a su vez, serán reagrupadas en paquetes Frame Relay antes de alcanzar su destino.

La interoperatividad de servicio, por su parte, permite establecer comunicación directa entre dispositivos y usuarios Frame Relay, y dispositivos y usuarios ATM, mediante la conversión de los respectivos protocolos. Así, por ejemplo, Frame Relay/ATM Service Internetworking permite que los dispositivos Frame e Relay situados en oficinas remotas accedan a aplicaciones basadas en ATM residentes en las oficinas centrales. Como es lógico, para que ello sea posible es preciso compensar las diferencias entre ambas tecnologías, operación que corre a cargo de Interworking Function (IWF), localizada generalmente en los conmutadores situados en las fronteras de los servicios Frame Relay y ATM.

IWF se encarga de la conversión de diferentes parámetros entre redes Frame Relay y ATM, determinando, entre otras cosas, la forma y delimitación de tramas o celdas en el modo apropiado, la especificación de la "elección de descartes" (discard eligibility) y prioridad de pérdida de celdas, así como el envío o recepción de indicaciones de congestión y conversión de los Data Link Connection Identifier (DLCI) de Frame Relay a los Virtual Path Identifier/virtual Circuit Identifier (VPI / VCI) de ATM.

IWF, además, se encarga de la gestión de tráfico, del soporte de interoperatividad de gestión de circuito virtuales permanentes mediante indicadores de estado, y de encapsular el protocolo de usuario de nivel superior. En general, en un entorno Frame Relay/ATM Service Interworking, IWF afronta todas las tareas asociadas con la traducción del mensaje basado en UNI (User-to-Network Interface) Q.922 Core de Frame Relay al mensaje basado UNI AAL5 Class C de la red ATM. Este modo de mensaje es usado para la conexión ATM porque rinde algunas funciones básicas similares al servicio Q.922 DL Core de Frame Relay.

II. Protocolos e interfaces de comunicación de datos.

1. Protocolos e interfaces de bajo nivel.

- ***Interfaces en la capa física***

RS-232 en 23 Y 9 Pines: define una interfaz no balanceada empleando un intercambio en serie de datos binarios a velocidades de transmisión superiores a los 20,000 bps, opera con datos sincronos pero está limitada por una longitud de cable de aprox. 50 pies.

LA NORMA RS-232. Esta norma es la mas popular y a la vez es una de las mas antiguas de todas las normas empleadas en las comunicaciones seriales, esta norma cubre los tres aspectos siguientes, entre el equipo terminal de datos (DTE), y el equipo de comunicación de datos (DCE):
a).- Las características eléctricas de las señales
b).- Las conexiones mecánicas de los conectores y
c).- La descripción funcional de las señales usadas.

La norma RS-232 fue desarrollada en la década de los 60 para gobernar la interconexión de equipos terminales con MODEMS, entre los principales aspectos que son una desventaja para esta norma RS-232 esta en que sus niveles lógicos no son compatibles TTL, esto es porque con niveles lógicos TTL no se puede transmitir mas allá de los 15 metros de longitud y esto a muy bajas velocidades, los niveles de voltaje para la norma RS-232 son;
a).- Para un uno lógico desde -3.0 volts hasta -15.0 volts
b).- Para un cero lógico desde +3.0 volts hasta +15.0 volts

La longitud máxima no debe sobrepasar los 15 metros, esto depende de las velocidades de transmisión empleadas, aunque es posible generar los niveles de voltaje de la norma RS-232C con componentes discretos, existen en la actualidad circuitos integrados excitadores de línea y receptores integrados que satisfacen estas especificaciones, como por ejemplo los circuitos MC1488, MC1489 y el MAX232, se podría pensar que es necesario para la conexión un cable de 25 conectores, para muchas aplicaciones solamente se requieren 3 conductores. El término microcomputadora o microprocesador no esta incluido en la terminología de la norma RS-232C, pues cuando se hizo dicha norma no existían las computadoras, las computadoras en algunos casos se comportan como DTE y en otros casos como DCE, presentándose una mayor confusión alrededor de las terminales 2 y 3 de la norma RS-232.

RS-232-C y RS-449

· es la interfaz entre el computador o equipo terminal y el módem, representando un ejemplo de protocolo de la capa física.
· la especificación mecánica considera un conector de 25 pines, con todas sus dimensiones bien especificadas.
· la especificación eléctrica considera que para decidir si un bit está en 1, se deberá tener un voltaje más negativo que -3 volts; y para el bit 0, que el voltaje sea superior a +4 volts.
· es posible tener velocidades de hasta 20 Kbps y longitud máxima de 15 metros de cable.
· la especificación funcional indica los circuitos que están conectados a cada uno de los 25 pines, así como el significado de c/u de ellos.
· la RS-449 puede utilizarse en velocidades de hasta 2 Mbps, en cables de hasta 60 metros.

V.35: especifica una interfaz sincrono para operar a velocidades superiores a 1 Mbps. Este interfaz utiliza la mezcla de dos señales no balanceadas para control y de señales balanceadas para la sincronización y envío/recepción de los datos lo que facilita trabajar a latas velocidades.

X.21:Estándar ITU-T para las comunicaciones en serie sobre líneas digitales síncronas. El protocolo X.21 se utiliza principalmente en Europa y Japón.

X.21bis: Estándar ITU-T que define el protocolo de capa física para la comunicación entre DCE y DTE en una red X.25. Virtualmente equivalente a EIA/TIA-232

- ***Control de Flujo en los protocolos de bajo nivel***

CONTROL DE FLUJO

Es una técnica para que el emisor no sobrecargue al receptor al enviarle más dato al que pueda procesar, el receptor tiene un buffer de una cierta capacidad para ir guardando los datos recibiendo y tras procesarlos enviando a capas superior. Los métodos mas comunes de control de flujo son:

- **Control de flujo hardware:**

TS y CTS permiten al PC y al modem parar el flujo de datos que se establece entre ellos de forma temporal. Este sistema es el mas seguro y el que soporta una operación adecuada a altas velocidades.

- **Control de flujo software: XON/XOFF.-**

Aquí se utilizan para el control dos caracteres especiales XON y XOFF (en vez de las lineas hardware RTS y CTS) que controlan el flujo. Cuando el PC quiere que el modem pare su envío de datos, envía XOFF. Cuando el PC quiere que el modem le envíe mas datos, envía XON. Los mismos caracteres utiliza el modem para controlar los envíos del PC.

Ventajas:

- *Técnica para que el transmisor no sature al receptor .*
- *Receptor reserva memoria temporal para el almacenamiento de datos, los procesa y los envía a niveles superiores.*
- *Control de flujo evita que se sature esta memoria.*

Desventajas

- Se ha intentado utilizarlo para resolver congestión
- No es apropiado para trafico en rafajas
- Se restringe al usuario al trafico promedio pero no funciona para picos de grafico.

Técnicas de Control de Flujo

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

Esta limitación en el espacio de memoria hace que se presente un serio problema cuando un transmisor sistemáticamente quiere transmitir tramas a mayor velocidad que aquella con que puede recibirlas el receptor. Esta situación puede ocurrir fácilmente cuando el transmisor opera en una computadora rápida (o con baja carga) y el receptor en una máquina lenta (o con sobrecarga). El transmisor puede enviar tramas rápidamente hasta que satura al receptor, que comenzará a desechar aquellas a las que no pueda atender.

Para evitar esta situación se hace necesario llevar un control del flujo en el enlace, manejando la velocidad a la que el emisor envía las tramas para que no sature al receptor.

Este control de la velocidad generalmente requiere algún mecanismo de realimentación, para que el transmisor pueda saber si el receptor puede mantener el ritmo o no.

La mayoría de las técnicas de control de flujo tienen un principio de funcionamiento igual: el protocolo contiene reglas bien definidas sobre el momento en que el transmisor puede enviar alguna trama, y generalmente estas reglas prohiben el envío de información hasta que el receptor no lo haya autorizado.

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

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

Parada-y-Espera.

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

* El transmisor envía una trama al receptor.
* El receptor la recoge, y devuelve otra trama de aceptación (ACK).
* Cuando el transmisor recibe esta trama sabe que puede realizar un nuevo envío....
* Si pasado un cierto tiempo predeterminado no ha llegado acuse de recibo, el emisor retransmite la trama.

Consiste en que el emisor envía una trama y al ser recibida por el receptor , éste (el receptor) confirma al emisor (enviándole un mensaje de confirmación la recepción de la trama .
Este mensaje recibido por el emisor es el que le indica que puede enviar otra trama al receptor .

De esta forma, cuando el receptor esté colapsado (el buffer a punto de llenarse), no tiene más que dejar de confirmar una trama y entonces el emisor esperará hasta que el receptor decida enviarle el mensaje de confirmación (una vez que tenga espacio en el buffer) .

Sin embargo, la técnica de parada-y-espera presenta un importante inconveniente. Supongamos que el transmisor envía una trama y el receptor da el acuse de recibo, pero de alguna manera el ACK se pierde o se retrasa en llegar. En ambos casos el emisor piensa que el tiempo ha expirado y retransmite la trama, pero el receptor ya había recogido una y cree que ésta que le llega ahora es otra diferente. Para solucionar este problema, la cabecera de una trama del protocolo de parada-y-espera incluye un bit a modo de número de secuencia), que puede tomar los valores 0 y 1; los números de secuencia empleados para trama consecutivas son alternos.

PRESTACIONES.

Restringiéndonos al caso en que sólo se puede enviar una trama cada vez, encontramos dos posibles situaciones, definidas por el tiempo de transmisión y el tiempo de propagación:

1.- ***Tiempo de Transmisión, Ttx***: tiempo que tarda una máquina en pasar una trama al medio desde que sále el primer bit hasta el último. Se define como el cociente entre la ***longitud de la trama (L)*** y el ***régimen binario en el canal (R)***.

$$Ttx = L / R$$

2.- ***Tiempo de Propagación, Tprop***: tiempo que tarda una unidad de información en pasar de un extremo del canal al otro. Se define como el cociente entre la ***distancia (d)*** o longitud del enlace, y la ***velocidad del medio de transmisión (v)***.

$$Tprop = d / v$$

1.2 Ventana Deslizante.

Retomando el ejemplo del enlace que tenía un producto de ancho de banda x retraso de 8KB y las tramas de 1KB, se comprueba que la mejor utilización que se puede hacer del canal requiere que el emisor transmita la novena trama nada más recibir el acuse de recibo de la primera.

En este algoritmo el témino ***ventana de transmisión*** se refiere a un buffer en el cual se almacenan copias de las tramas enviadas, en espera de recibir el ACK correspondiente; si no llegan en el tiempo previsto, se realiza una nueva copia y se retransmite la trama. El ***número de secuencia de transmisión***, ***N(S)***, es la posición que ocupa la trama enviada en el buffer. El número de secuencia viaja en la cabecera de la trama, dentro del campo de control.

Por ***ventana de recepción*** se entiende el buffer donde se almacenan las tramas que llegan a una máquina por alguno de sus enlaces. En este buffer esperan a ser procesadas, y a que se devuelva el acuse de recibo correspondiente a cada una de ellas, para que la máquina origen sepa que la transmisión ha llegado sin problemas a su destino. El ***número de secuencia de recepción***, ***N(R)***, es la posición que ocupa la trama recibida en el buffer de recepción.

El tamaño de la ventana puede estar preestablecido, o puede negociarse durante el establecimiento de la conexión. En la figura se ilustra el mecanismo del algoritmo para una ventana de tamaño 4:

El algoritmo de ventana deslizante es como sigue: primero el emisor asigna un número de secuencia a cada trama. El emisor controla tres variables:

1. El ***tamaño de la ventana de transmisión (TVT)***: Que será finito. Representa el número máximo de tramas que el emisor puede enviar sin recibir ACK de la primera de ellas.

2. El ***número de secuencia del último ACK recibido (UAR)***.

3. El ***número de secuencia de la última trama enviada (UTE)***.

Control del flujo mediante ventana deslizante

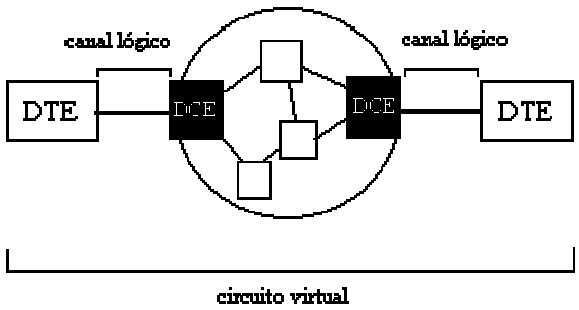
En este sistema , el receptor y el emisor se ponen de acuerdo en:

- El número de tramas que puede guardar el receptor sin procesar.
- Número de bits a utilizar para numerar cada trama. Por ejemplo, si en el buffer del receptor caben 7 tramas , habrá que utilizar una numeración con 3 bits ($2^3 = 8 > 7$) .

El emisor transmite tramas por orden (cada trama va numerada módulo $2^{\text{número de bits}}$) hasta un máximo de el número máximo de tramas que quepan en el buffer del receptor.

○ ***Protocolos de capa de red: X.25***

X.25 es un protocolo orientado a conexión. X.25 trabaja sobre servicios basados en circuitos virtuales. Un circuito virtual consiste en que el usuario cree que existe un circuito físico que lo conecta con el host que está utilizando, pero en realidad ese circuito físico es compartido por muchos usuarios. Mediante el uso de técnicas de multiplexación estadística, se entrelazan en un mismo canal físico paquetes procedentes de diversos usuarios. El circuito virtual corresponde a la conexión punto a punto entre dos DTE (Data Terminal Equipment). Otro concepto importante es el de canal lógico. El canal lógico es la conexión local entre el DTE y la red. El canal lógico sólo tiene relevancia en la interfaz DTE - DCE en cada lado de la red.



2. Conjunto de protocolos TCP/IP.

- ***Protocolos a nivel de red: IP, ARP, RARP, ICMP.***

El Protocolo Internet (*Internet Protocol - IP*)

El protocolo IP es el principal del modelo OSI, así como parte integral del TCP/IP. Las tareas principales del IP son el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas. El datagrama es la unidad de transferencia que el IP utiliza, algunas veces identificada en forma más específica como datagrama Internet o datagrama IP. Las características de este protocolo son:

- NO ORIENTADO A CONEXIÓN
- Transmisión en unidades denominadas **datagramas**.
- Sin corrección de errores, ni control de congestión.
- No garantiza la entrega en secuencia.

La entrega del datagrama en IP no está garantizada porque ésta se puede retrasar, enrutar de manera incorrecta o mutilar al dividir y reensamblar los fragmentos del mensaje. Por otra parte, el IP no contiene suma de verificación para el contenido de datos del datagrama, solamente para la información del encabezado. En cuanto al ruteo (encaminamiento) este puede ser :

- Paso a paso a todos los nodos.
- Mediante tablas de rutas estáticas o dinámicas.

Protocolos de resolución de direcciones.

El objetivo es diseñar un software de bajo nivel que oculte las direcciones físicas (MAC) y permita que programas de un nivel más alto trabajen sólo con direcciones IP. La transformación de direcciones se tiene que realizar en cada fase a lo largo del camino, desde la fuente original hasta el destino final. En particular, surgen dos casos. Primero, en la última fase de entrega de un paquete, éste se debe enviar a través de una red física hacia su destino final. La computadora que envía el paquete tiene que transformar la dirección IP de destino final en su dirección física (MAC). Segundo, en cualquier punto del camino, de la fuente al destino, que no sea la fase final, el paquete se debe enviar hacia un router intermedio. Por lo tanto, el transmisor tiene que transformar la dirección IP del router en una dirección física. El problema de transformar direcciones de alto nivel en direcciones físicas se conoce como *problema de asociación de direcciones* (Address Resolution Problem). Este problema se suele resolver, normalmente, mediante tablas en cada máquina que contienen pares de direcciones, de alto nivel y físicas. En el problema de asociación de direcciones en TCP/IP para redes con capacidad de difusión como Ethernet, se utiliza un protocolo de bajo nivel para asignar direcciones en forma dinámica y evitar así la utilización de una tabla de conversiones. Este protocolo es conocido como **Protocolo de Asociación de Direcciones** (**ARP** - *Address Resolution Protocol*). La idea detrás de la asociación dinámica con ARP es muy sencilla: cuando un host A quiere definir la dirección IP (IPb), transmite por difusión (broadcast) un paquete especial que pide al anfitrión (host) que posee la dirección IP (IPb), que responda con su dirección física (Pb). Todos los anfitriones reciben la solicitud, incluyendo a B, pero sólo B reconoce su propia dirección IP y envía una respuesta que contiene su dirección física. Cuando A recibe la respuesta, utiliza la dirección física para enviar el paquete IP directamente a B. En resumen: El ARP permite que un anfitrión encuentre la dirección física de otro anfitrión dentro de la misma red física con sólo proporcionar la dirección IP de su objetivo. La información se guarda luego en una tabla ARP de orígenes y destinos.

Protocolo de Asociación de Direcciones por Réplica (**RARP**):

Una máquina sin disco utiliza un protocolo TCP/IP para internet llamado RARP (Protocolo Inverso de Asociación de Direcciones) o Reverse Address Resolution Protocol, a fin de obtener su dirección IP desde un servidor. En el arranque del sistema, una máquina de estas características (sin HDD permanente) debe contactar con un servidor para encontrar su dirección IP antes de que se pueda comunicar por medio del TCP/IP. El protocolo RARP utiliza el direccionamiento físico de red para obtener la dirección IP de la máquina. El mecanismo RARP proporciona la dirección hardware física de la máquina de destino para identificar de manera única el procesador y transmite por difusión la solicitud RARP. Los servidores en la red reciben el mensaje, buscan la transformación en una tabla (de manera presumible en su almacenamiento secundario) y responden al transmisor. Una vez que la máquina obtiene su dirección IP, la guarda en memoria y no vuelve a utilizar RARP hasta que se inicia de nuevo.

Mensajes de error y control en IP (ICMP).

Como hemos visto anteriormente, el Protocolo Internet (IP) proporciona un servicio de entrega de datagramas, no confiable y sin conexión, al hacer que cada router direccione datagramas. Si un router no puede, por ejemplo, rutear o entregar un datagrama, o si el router detecta una condición anormal que afecta su capacidad para direccionarlo (v.q., congestionamiento de la red), necesita informar a la fuente original para que evite o corrija el problema. Para permitir que los routers de una red reporten los errores o proporcionen información sobre circunstancias inesperadas, se agregó a la familia TCP/IP un mecanismo de mensajes de propósito especial, el *Protocolo de Mensajes de Control Internet* (**ICMP**). El ICMP permite que los routers envíen mensajes de error o de control hacia otros routers o anfitriones, proporcionando una comunicación entre el software de IP en una máquina y el mismo software en

otra.Cuando un datagrama causa un error, el ICMP sólo puede reportar la condición del error a la fuente original del datagrama; la fuente debe relacionar el error con un programa de aplicación individual o debe tomar alguna otra acción para corregir el problema.

Formato de los mensajes ICMP:

Aunque cada mensaje ICMP tiene su propio formato, todos comienzan con los mismos tres campos; un campo TYPE (TIPO) de mensaje, de 8 bits y números enteros, que identifica el mensaje; un campo CODE (CODIGO), de 8 bits, que proporciona más información sobre el tipo de mensaje, y una campo CHECKSUM (SUMA DE VERIFICACIÓN), de 16 bits. Además, los mensajes ICMP que reportan errores siempre incluyen el encabezado y los primeros 64 bits de datos del datagrama que causó el problema. La razón de regresar más que el encabezado del datagrama únicamente es para permitir que el receptor determine de manera más precisa qué protocolo(s) y qué programa de aplicación son responsables del datagrama.El campo TYPE de ICMP define el significado del mensaje así como su formato. Los tipos incluyen:

CAMPO TYPE	Tipo de Mensaje ICMP
0	Respuesta de ECO
3	Destino inaccesible
4	Disminución de origen (source quench) - datagrama eliminado por congestión
5	Redireccionar (cambiar una ruta)
8	Solicitud de ECO
11	Tiempo excedido para un datagrama
12	Problema de parámetros de un datagrama
13	Solicitud de TIMESTAMP
14	Respuesta de TIMESTAMP
15	Solicitud de Información (obsoleto)
16	Respuesta de Información (obsoleto)
17	Solicitud de Máscara de dirección
18	Respuesta de máscara de dirección

Una de las herramientas de depuración más utilizadas incluye los mensajes ICMP de *echo request (8)* y *echo reply (0)*. En la mayoría de los sistemas, el comando que llama el usuario para enviar solicitudes de eco ICMP se conoce como **ping**.

- ***Protocolos de la capa de transporte: tcp, udp***

Servicio de transporte de flujo confiable (TCP).

En las secciones anteriores hemos visto el servicio de entrega de paquetes sin conexión y no confiable, que forma la base para toda comunicación en InterNet, así como el protocolo IP que lo defina. Ahora veremos el segundo servicio más importante y mejor conocido a nivel de red, la entrega de flujo confiable (Reliable Stream Transport), así como el Protocolo de Control de Transmisión (TCP) que lo define. En el nivel más bajo, las redes de comunicación proporcionan una entrega de paquetes no confiable. Los paquetes se pueden perder o destruir debido a errores (falla el hardware, sobrecarga de la red,...). Las redes que rutean dinámicamente los paquetes pueden entregarlos en desorden, con retraso o duplicados. En el nivel más alto, los programas de aplicación a menudo necesitan enviar grandes volúmenes de datos de una computadora a otra. Utilizar un sistema de entrega de conexión y no confiable para transferencias de grandes volúmenes de información resulta ser la peor opción. Debido a esto, el TCP se ha vuelto un protocolo de propósito general para estos casos. La interfaz entre los programas de aplicación y la entrega confiable (es, decir, las características del TCP) se caracterizan por cinco funciones:

Servicio Orientado a Conexión : El servicio de entrega de flujo en la máquina destino pasa al receptor exactamente la misma secuencia de bytes que le pasa el transmisor en la máquina origen.

Conexión de Circuito Virtual : Durante la transferencia, el software de protocolo en las dos máquinas continúa comunicándose para verificar que los datos se reciban correctamente. Si la comunicación no se logra por cualquier motivo (v.q. falla el hardware de red), ambas máquinas detectarán la falla y la reportarán a los programas apropiados de aplicación. Se utiliza el término *circuito virtual* para describir dichas conexiones porque aunque los programas de aplicación visualizan la conexión como un circuito dedicado de hardware, la confiabilidad que se proporciona depende del servicio de entrega de flujo.

Transferencia con Memoria Intermedia : Los programas de aplicación envían un flujo de datos a través del circuito virtual pasando repetidamente bytes de datos al software de protocolo. Cuando se transfieren datos, cada aplicación utiliza piezas del tamaño que encuentre adecuado, que pueden ser tan pequeñas como un byte. En el extremo receptor, el software de protocolo entrega bytes del flujo de datos en el mismo orden en que se enviaron, poniéndolos a disposición del programa de aplicación receptor tan pronto como se reciben y se verifican. El software de protocolo puede dividir el flujo en paquetes, independientemente de las piezas que transfiera el programa de aplicación. Para hacer eficiente la transferencia y minimizar el tráfico de red, las implantaciones por lo general recolectan datos suficientes de un flujo para llenar un datagrama razonablemente largo antes de enviarlo. Por lo tanto, inclusive si el programa de aplicación genera el flujo un byte a la vez, la transferencia a través de la red puede ser sumamente eficiente. De forma similar, si el programa de aplicación genera bloques de datos muy largos, el software de protocolo puede dividir cada bloque en partes más pequeñas para su transmisión. Para aplicaciones en las que los datos de deben entregar aunque no se llene una memoria intermedia, el servicio de flujo proporciona un mecanismo de *empuje* o *push* que las aplicaciones utilizan para forzar una transferencia. En el extremo transmisor, el push obliga al software de protocolo a transferir todos los datos generados sin tener que esperar a que se llene una memoria intermedia. Sin embargo, la función de push sólo garantiza que los datos se transferirán, por tanto, aún cuando la entrega es forzada, el software de protocolo puede dividir el flujo en formas inesperadas (v.q. el transmisor puede reducirlo en caso de congestión).

Flujo no estructurado: Posibilidad de enviar información de control junto a datos.

Conexión Full Duplex: Se permite la transferencia concurrente en ambas direcciones. Desde el punto de vista de un proceso de aplicación, una conexión full duplex permite la existencia de dos flujos independientes que se mueven en direcciones opuestas, sin ninguna interacción aparente. Esto ofrece una ventaja : el software subyacente de protocolo puede enviar datagramas de información de control de flujo al origen, llevando datos en la dirección opuesta. Este procedimiento de carga, transporte y descarga REDUCE EL TRAFICO en la red.

La "Contradicción"

Hemos visto que el servicio de entrega de flujo confiable garantiza la entrega de los datos enviados de una máquina a otra sin pérdida o duplicación. Surge ahora la pregunta contradictoria "del millón" : *¿ Cómo puede el software subyacente de protocolo proporcionar una transferencia confiable si el sistema subyacente de comunicación sólo ofrece una entrega NO confiable de paquetes ?*.La respuesta es complicada, pero la mayor parte de los protocolos confiables utilizan una técnica fundamental conocida como ***acuse de recibo positivo con retransmisión***. La técnica requiere que un receptor se comunique con el origen y le envíe un mensaje de acuse de recibo (***ACK***) conforme recibe los datos (ver los primeros temas para una descripción más detallada). El transmisor guarda un registro de cada paquete que envía y espera un ACK antes de enviar el siguiente paquete. El transmisor también arranca un temporizador cuando envía un paquete y lo retransmite si dicho temporizador expira antes de que llegue un ACK. El problema final de la confiabilidad surge cuando un sistema subyacente de entrega de paquetes los duplica. Los duplicados también pueden surgir cuando las redes tienen grandes retrasos que provocan la retransmisión

prematura. Para evitar la confusión causada por ACKs retrasados o duplicados, los protocolos de acuses de recibo positivos envían los números de secuencia dentro de los ACKs, para que el receptor pueda asociar correctamente los acuses de recibo con los paquetes. Pero, como casi todo en esta vida es un problema tras otro, el TCP no iba a ser menos ; uno de los problemas que acarrea lo anterior es que un protocolo simple de acuses de recibo positivos ocupa una cantidad sustancial de ancho de banda de red debido a que debe retrasar el envío de un nuevo paquete hasta que reciba un ACK del paquete anterior. La solución está en otra técnica conocida como ***ventana deslizante***, que es una forma más compleja de acuse de recibo positivo y retransmisión. Los protocolos de ventana deslizante utilizan el ancho de banda de red de mejor forma al permitir que el transmisor envíe varios paquetes sin esperar el ACK (remitirse a capítulos anteriores para una descripción de éste método).

Puertos, conexiones y puntos extremos.

Al igual que el UDP, el TCP reside sobre el IP en el esquema de estratificación por capas de protocolos. El TCP permite que varios programas de aplicación en una máquina se comuniquen de manera concurrente y realiza el demultiplexado del tráfico TCP entrante entre los programas de aplicación. Así mismo, al igual que el UDP, el TCP utiliza números de ***puerto de protocolo*** para identificar el destino final dentro de una máquina. Cada puerto tiene asignado un número entero pequeño utilizado para identificarlo. Para comprender el significado de un puerto hay que pensar de cada puerto como en una cola de salida en la que el software de protocolo coloca los datagramas entrantes, aunque en realidad los puertos TCP son más complejos, ya que un número de puerto no corresponde a un sólo objeto. El TCP utiliza la conexión, no el puerto de protocolo, como su abstracción fundamental; las conexiones se identifican por medio de un par de puntos extremos. ¿Qué es exactamente un punto extremo en TCP ? Un punto extremo es un par de números enteros **(host, puerto)**, en donde *host* es la dirección IP de un anfitrión y *puerto* es el un puerto TCP en dicho anfitrión. Las conexiones vienen definidas por dos puntos extremos, y es más: la abstracción de la conexión para TCP permite que varias conexiones compartan un punto extremo (por ejemplo, varias conexiones en los mismos puertos). Esto es posible a que el TCP identifica una conexión por medio de un par de puntos extremos, y por eso varias conexiones en la misma máquina pueden compartir un número de puerto TCP. El TCP combina la asignación dinámica y estática de puertos mediante un conjunto de *asignación de puertos bien conocidos* para programas llamados con frecuencia, pero la salida de la mayor parte de los números disponibles para el sistema se asigna conforme los programas lo necesitan.

Protocolo de datagrama de usuario (UDP).

La mayoría de los Sistemas Operativos actuales soportan multiprogramación. Puede parecer natural decir que un proceso es el destino final de un mensaje. Sin embargo, especificar que un proceso en particular en una máquina en particular es el destino final para un datagrama es un poco confuso. Primero, por que los procesos se crean y se destruyen dinámicamente, los transmisores rara vez saben lo suficiente para identificar un proceso en otra máquina. Segundo, nos gustaría poder reemplazar los procesos que reciben datagramas, sin tener que informar a todos los transmisores (v.q. reiniciar la máquina puede cambiar todos los PID de los procesos). Tercero, necesitamos identificar los destinos de las funciones que implantan sin conocer el proceso que implanta la función (v.q. permitir que un transmisor contacte un servidor de ficheros sin saber qué proceso en la máquina de destino implanta la función de FS). En vez de pensar en un proceso como destino final, imaginaremos que cada máquina contiene un grupo de puntos abstractos de destino, llamados ***puertos de protocolo***. Cada puerto de protocolo se identifica por medio de un número entero positivo. Para comunicarse con un puerto externo, un transmisor necesita saber tanto la dirección IP de la máquina de destino como el número de puerto de protocolo del destino dentro de la máquina. El UDP proporciona el mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación. El UDP proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma máquina. Esto es, además de los datos, cada mensaje UDP contiene tanto en número de puerto de destino como el número de puerto origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que éste envíe una respuesta. El UDP utiliza el Protocolo Internet subyacente para transportar un mensaje de una máquina a otra y proporciona la misma semántica de entrega de datagramas, sin conexión y no confiable que el IP. No emplea acuses de recibo para asegurarse de que llegan mensajes, no ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad del flujo de información entre las máquinas. Por tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden. Además, los paquetes pueden llegar más rápido de lo que el receptor los puede procesar. En resumen:

El UDP proporciona un servicio de entrega sin conexión y no confiable, utilizando el IP para transportar mensajes entre máquinas. Emplea el IP para llevar mensajes, pero agrega la capacidad para distinguir entre varios destinos dentro de la computadora anfitrión.

Formato de los mensajes UDP:

Cada mensaje UDP se conoce como *datagrama de usuario.* Conceptualmente, un datagrama de usuario consiste en dos partes: un encabezado UDP y un área de datos UDP. El encabezado se divide en cuatro campos de 16 bits, que

especifican el puerto desde el que se envió el mensaje, el puerto para el que se destina el mensaje, la longitud del mensaje y una suma de verificación UDP.

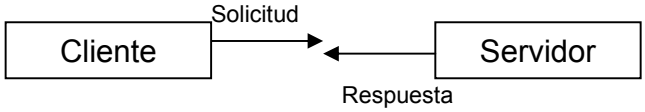
3. Protocolos de Alto Nivel

- ***Modelo cliente – servidor.***

Es un concepto muy importante en las redes locales para aplicaciones que manejan grandes volúmenes de información. Son programas que dividen su trabajo en dos partes, una parte cliente que se realiza en el ordenador del usuario y otra parte servidor que se realiza en un servidor con dos fines:

- Aliviar la carga de trabajo del ordenador cliente.
- Reducir el tráfico de la red.

Ejemplo: si disponemos de un ordenador que actúa como servidor de base de datos, con un enfoque tradicional, el servidor solamente lo es de ficheros. Si en algún momento el usuario quiere hacer una selección de personas mayores de 30 años por ejemplo, se deben leer todos los registros de la base de datos para comprobar cuáles cumplían la condición. Esto supone un elevado tráfico en la red. Con las aplicaciones cliente/servidor una consulta sobre una base de datos se envía al servidor, quien realiza la selección de registros y envía solo los campos que le interesan al usuario. Se reduce así considerablemente el tráfico en la red y el ordenador cliente se encuentra con el trabajo hecho. El sistema en sí resulta bastante más rápido, aunque a cambio requiere que los servidores tengan mejores prestaciones.



El cliente transmite una solicitud y el servidor transmite una respuesta:

- ***Protocolos de control de la capa de aplicación(SMTP, SNMP, DHCP)***

SMTP(simple mail transfer protocol).

Es un protocolo estándar del TCP/IP para la transferencia de mensajes de correo electrónico de una maquina a otra. SMTP especifica como actúan dos sistemas de correo y le formato de los mensajes de control que intercambian para transferir el correo. El SMTP se enfoca específicamente en como transfiere el sistema de correo subyacente los mensajes atreves de un enlace de una maquina a otra. El SMTP no especifica de que manera acepta el sistema de correo los mensajes de correo de un usuario o como presenta al usuario la interfaz de usuario el correo entrante. El SMTP tampoco especifica en que forma se almacena el correo o en que frecuencia el sistema de correo trata de enviar mensajes. La comunicación entre un cliente y un servidor consiste en texto ASCII que es posible leer, los usuarios pueden leer fácilmente una transcripción de interacciones entre un cliente y un servidor.

SNMP(simple network monitoring protocol).

Es decir, protocolo estándar para monitorear anfitriones, ruteadores y las redes a las que están conectados. La segunda versión del protocolo se conoce como SNMPv2. El SNMP define un protocolo de administración de bajo nivel que proporciona dos operaciones básicas: obtener un valor de una variable o almacenar un valor de una variable. En el SNMP, todas las operaciones sedan como consecuencia de los valores que se almacenan en las variables. El SNMP define le formato de los mensajes entre la computadora del administrador y una entidad supervisada. Un estándar asociado al SNMP define el conjunto de variables que una entidad administrada mantiene. El estándar se conoce como Management Information Base, o MIB. Las variables MIB se describen usando ASN.1, que es un lenguaje formal que proporciona una forma codificada concisa así como un notación precisa que es posible leer para los usuarios para nombres y objetos.

DHCP (dynamic host configuration protocol).

Es decir, protocolo de configuración dinámica de un anfitrión o DHCP, este protocolo extiende a su antecesor el BOOTP de dos formas:

En primer lugar, el DHCP permite que una computadora adquiera toda la información que necesita en un solo mensaje. P.e: además de una dirección IP, un mensaje DHCP puede tener una mascara de subred.

En segundo lugar, el DHCP permite que una computadora posea una dirección IP en forma rápida y dinámica.

El DHCP permite 3 tipos de asignación de direcciones:

- La configuración manual, mediante la cual un administrador puede configurar una dirección especifica para una computadora especifica.

- La configuración automática, por medio de la cual el administrador permite a un servidor DHCP asigna una dirección permanente cuando una computadora es conectada por primera vez a la red.
- La configuración dinámica, con la cual el servidor "presta" una dirección para una computadora por tiempo limitado.

- ***Protocolos de aplicación para transferencia de archivos(FTP, TFTP, HTTP)***

FTP (file transfer protocol).

Protocolo estándar de alto nivel del TCP/IP que sirve para transferir archivos de una maquina a otra. El FTP utiliza la TCP.

Características del FTP.

El FTP ofrece michas facilidades que van mas allá de la función de transferencia misma:

- ✓ Acceso interactivo. Aunque el FTP esta diseñado para usarse mediante programas, la mayor parte de las implantaciones proporciona una interfaz interactiva que permite a los usuarios interactuar fácilmente con los servidores remotos. P.e: un usuario puede pedir una lista de todos los archivos de un directorio en una maquina remota. También, el cliente suele responder a la entrada "help" (ayuda) mostrando la información del usuario acerca de los comandos posibles que se pueden invocar.
- ✓ Especificación de formato(representación). El FTP permite al cliente especificar el tipo y formato de datos almacenados. P.e: el usuario puede especificar si un archivo contiene enteros de texto o binarios, asi como, si los archivos de texto utilizan los conjuntos de caracteres ASCII o EBCDIC.
- ✓ **C**ontrol de autentificación**.** El FTP requiere que los clientes se autoricen así mismos con le envío de un nombre de conexión y una clave de acceso a clientes que no puedan abastecer una conexión o clave de acceso valida.

Modelo de proceso FTP.

Las conexiones de transferencia de datos y los procesos de transferencia de datos que los emplean pueden crearse de manera dinámica cuando se necesitan, pero la conexión de control continua atraves de una sesión. Una ves que la conexión de control desaparece, la sesión se termina y el software en ambos extremos termina todos los procesos de transferencia de datos. Un cliente y servidor FTP con una conexión de control TCP entre ambos y una conexión TCP separada entre sus procesos de transferencia de datos asociados. Además de enviar comandos del usuario al servidor, el FTP utiliza la conexión de control para permitir los procesos de control cliente y servidor, y así, coordinar el uso de puertos de protocolo TCP asignados dinámicamente y la creación de procesos de transferencia de datos que utilicen tales puertos. El FTP desde el punto de vista del usuario. Los usuarios ven al FTP como un sistema interactivo. Una ves que se invoca, el cliente ejecuta repetidamente las siguientes operaciones: leer una línea de entrada, analizar la línea para extraer un comando y sus argumentos, así como ejecutar el comando con los argumentos especificados. Por ejemplo. Para inicia la versión del FTP disponible bajo BSD de UNIX, el usuario invoca el formato FTP:

% **ftp**

El programa local de cliente FTP comienza y despliega un indicador para el usuario. Después del indicador, el usuario puede desplegar comandos como *help*.

ftp>**help**

Los comandos pueden abreviarse. Los comandos son:

!	cr	macdef	proxy	send	
$	delete	mdelete	sendport	status	
accountdebug	mdir	put	struct ...		

Para obtener mas información acerca de un comando, el usuario teclea el comando de ayuda (help command) con en los siguientes ejemplos:

ftp> **help ls**
ls lista el contenido del directorio remoto.
ftp> **help cdup**
cdup cambia el directorio de trabajo remoto por un directorio padre.
ftp> **help glob**
glob conmutación de metacaracteres de expansión de los nombres de archivo local.
ftp> **help bell**
bell hace un sonido cuando el comando se termina.

Para ejecutar un comando, solo se teclee el nombre del comando:

ftp> **bell**
Bell mode on. (Modo de sonido activado).

Ejemplo de una sesión con FTP anónimo.

Para proporcionar acceso a los archivos públicos, mucha de las localidades TCP/IP permiten el FTP anónimo. El acceso al FTP anónimo significa que el cliente no necesita una cuenta o clave de acceso, sino especificar un nombre de conexión anónimo y una clave de acceso de invitado. El servidor permite que usuario anónimo se conecte pero restringe su acceso solo a los archivos públicos disponibles(en muchos sistemas UNIX, el servidor restringe al FTP anónimo cambiando la raíz del sistema de archivos a un directorio pequeño y restringido(es decir, /usr/ftp)). Por ejemplo, supongamos que alguien un acopia en línea de un texto en el archivo **librotcp.tar** en el subdirectorio **pub/comer** en la maquina **arturo.cs.uv.edu**. un usuario conectado a la localidad, por ejemplo **usera**, podría obtener una copia de la archivo con solo hacer los siguientes pasos:

% ftp ftp .cs.uv.edu
Connected to arturo.cs.uv.edu.
220 arturo.cs.uv.edu. FTP Server (version 6.8) ready.
Name (ftp.cs.uv.edu:usera):**anonymous**
331 guest login ok, send e-mail address as password.
Password: **guest**
230 guest login ok, acces restrictions apply.
ftp> **get pub/comer/librotcp.tar bookfile**
200 PORT command okay.
150 opening ASCII mode data connection for librotcp.tar (9999967 bytes).
226 transfer complete.
9999967 bytes received in 22.76 second (4.3e+02 kbytes/s)
ftp>**close**
221 Goodbye.
ftp>**quit**

Los mensajes de control y error entre el cliente y el servidor FTP comienzan con un numero de tres dígitos seguido de texto. El software interpreta él numero; el texto esta dirigido a los usuarios.

TFTP (trivial file transfer protocol)

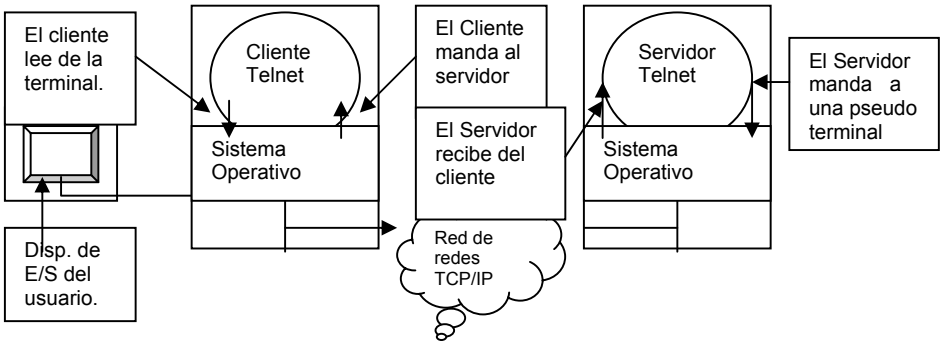
El conjunto de protocolos TCP/IP contiene un segundo protocolo de transferencia de archivos que proporciona un servicio económico y poco sofisticado. Se conoce como (TFTP o protocolo trivial de transferencia de archivos) y se diseño para aplicaciones que no necesitan interacciones complejas entre cliente y servidor. El TFTP restringe las operaciones de transferencia sencilla y no necesita y no proporciona autentificación. Es más pequeño que el FTP. La ventaja del TFTP es que al código de arranque que emplea los protocolos TCP/IP subyacentes en el sistema operativo una ves que empieza la ejecución. El TFTP no necesita del TCP ya que corre bajo UDP o cualquier otro sistema de entrega de paquetes no confiable. Las reglas del TFTP son sencillas.

- ***Protocolos de aplicación para la emulación de terminal (telnet, terminal virtual).***

Telnet

El conjunto de protocolos TCP/IP incluye un protocolo de terminal remota sencillo, llamado TELNET. TELNET permite al usuario de una localidad establecer una conexión TCP con servidor de acceso a otro. TELNET transfiere después de las pulsaciones de teclado directamente desde el teclado del usuario ala maquina remota. TELNET también transporta la salida de la maquina remota de regreso a la pantalla del usuario. El servicio se llama transparente porque da la idea de que tanto el monitor como el teclado están conectados directamente a la estación remota. El software de cliente TELNET suele permitir que el usuario especifique una maquina remota ya sea dando su nombre de dominio o su dirección IP. TELNET ofrece 3 servicios básicos:

1. Terminal virtual de red(network virtual terminal).Que proporciona una interfaz estandar para los sistemas remotos.
2. TELNET incluye un mecanismo que permite al cliente y al servidor negociar opciones.
3. TELNET permite que cualquier programa se convierta en cliente, cualquier extremo puede negocia las opciones.



C. Intercomunicación de redes.

I. Interconectividad.

1. Teoría de interconexiones.

- ***Clases de direcciones IP*.**

Cada máquina con TCP/IP tiene asociado un número de 32 bits al que se llama dirección IP, y que está dividido en dos partes:

- **Una parte que identifica la dirección de la red (NETID)**. Esta parte es asignada por el NIC (Network Information Center). En España se encarga de asignar estas direcciones REDIRIS. Si la red 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 8, 16 ó 24.
- **Una parte que identifica la dirección de la máquina dentro de la red (HOSTID).** Las direcciones de los hosts son asignadas por el administrador de la red.

Una dirección se representa por cuatro valores decimales separados por puntos, para que sea más fácil su escritura y memorización.
[0..255] . [0..255] . [0..255] . [0..255]

Máscara de subred

Cuando una red aparece segmentada (dividida en subredes), se debe utilizar un dispositivo que interconecte los segmentos y se hace necesario identificar de algún modo cada uno de los segmentos. Si todos los segmentos tienen la misma dirección IP, se hace necesaria la existencia de algún mecanismo que diferencia los segmentos. Este mecanismo es la máscara de la subred. A cada dirección IP de red, es decir, a cada red física, se le asocia una máscara que tiene 32 bits. La máscara sirve para dividir la parte de la dirección IP destinada a identificar el host en dos partes: la primera identificará el segmento, y la segunda el host dentro de este segmento. En esta máscara los bits a 1 significan que el bit correspondiente de la dirección IP será tratado como bit correspondiente a la dirección de la subred, mientras que los bits a 0 en la máscara, indican que los bits correspondientes de la dirección IP serán interpretados como identificadores del host. Así con una misma dirección de red se pueden direccionar muchas subredes.

Clases de redes

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

Redes de clase A: Las principales características son:
Se tratan de redes de mayor tamaño, redes que tengan más de 2^{16} hosts.
El espacio reservado para la dirección de red es más pequeño por dos motivos:
- Porque existen menos redes de este tipo.
- Porque al tener más hosts necesitamos dejar más espacios para direccionar a estos.

La parte que identifica la red consta de

- un cero (0)
- 7 bits más.

Se podrán direccionar por tanto 2^7 redes que hace un total de 128 redes diferentes. Cada una de estas redes podrá tener 2^{24} posibles hosts. La dirección 127 no se utiliza.

1……7	8……..32
Dirección de la red 0…..	Identificador de la máquina

Redes de clase B: Son redes de tamaño mediano que tienen entre 2^8 y 2^{16} hosts. La parte que identifica la red consta de

- La secuencia uno-cero (10).
- 14 bits con cualquier valor.

Por tanto, el rango de valores para el primer byte de los dos asignados a la red es de:128-191.
Estas redes pueden tener 2^{16}=65536 hosts cada una de ellas. El formato de las direcciones es:

1……..……16	17……..……..32
Dirección de la red 10…..	Identificador de la máquina

Redes de clase C: Son redes menor tamaño que pueden tener hasta 2^8 hosts. La parte que identifica la red consta de

- La secuencia uno-uno-cero (110).
- 21 bits con cualquier valor.

Por tanto, el rango de valores para el primer byte de los dos asignados a la red es de: 192-223. Estas redes pueden tener 2^8=256 hosts cada una de ellas. El formato de las direcciones es:

0……..…. 23	24…….31
Dirección de la red 110…	Identificador de la máquina

Tabla esquemática de los formatos de direcciones

	Byte 1	**Byte 2**	**Byte 3**	**Byte 3**
Clase A	0…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 clases de 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 un uso futuro.
Ejemplo: la dirección 156.35.41.20 identifica el host 41.20 de la red 156.35.

Convenciones de direcciones especiales
Existen algunas direcciones (combinaciones de unos y ceros) que no se asignan con direcciones IP, sin que tienen un significado especial. Estas combinaciones son:

dirección de la red	Todo unos

Esta dirección se llama difusión dirigida y permite direccionar a todas las máquinas dentro de la red especificada. Es un direccionamiento muy útil, ya que con un solo paquete podemos enviar el mismo mensaje a todas las máquinas de una red.

127	Cualquier combinación (normalmente 1)

Esta dirección se denomina **loopback** y se utiliza para realizar pruebas y comunicaciones entre procesos dentro de una misma máquina. Si un programa envía un mensaje a esta dirección, TCP/IP le devolverá los datos sin enviar nada a la red, aunque se comporta como si lo hubiera hecho.

Parte de la red a ceros	dirección de host

Esta dirección permite direccionar a un host interno de la red.

Todos unos	Todos unos

Esta dirección se denomina difusión limitada; realiza un direccionamiento a todos los host de la propia red.

Todos ceros	Todos ceros

Esta dirección, direcciona al propio host.
Una dirección Internet no identifica a un host, sino a una conexión a red. Un ejemplo: si se dispone de un gateway que conecta una red con otra, ¿qué dirección de Internet se le da a esta estación? , Ya que tiene dos posibles direcciones, una por cada red a la que esté conectada. En realidad, se le asigna a cada estación tantas direcciones IP como conexiones a redes tenga la estación.

DIRECCIONES UTILIZADAS EN LA REALIDAD

Cuando se intenta establecer una conexión con otra máquina, no se suele poner la dirección IP de esta, sin que se utiliza un nombre. La máquina se encarga de transformar ese nombre a una dirección IP. Cuando se quiere conectar con otra máquina que no está en la misma red, se suele utilizar un nombre que es más complejo que las conexiones dentro de la misma red. Dicho nombre consta de dos partes:

- Identificación del usuario@.
- Nombre de la máquina.

El nombre de la máquina se llama dominio, que a su vez puede estar dividido en subdominios. Lo normal es que un dominio tenga tres subdominios, de los cuales el de más a la derecha se denomina subdominio de primer nivel y es él más genérico de todos. Para entender los subdominios se deben mirar de derecha a izquierda. Existen dos tipos de subdominios de primer nivel:

1. Domínios de organizaciones, utilizados casi de manera exclusiva en Norteamérica.
2. Domínios geográficos utilizados en el resto del mundo.

Subdominio 1º nivel. Organizaciones	Significado
com	Organización comercial
edu	Educativa
gov	Gobierno
int	Organización internacional
mil	Organización militar
net	Gestión de redes
org	Organización no lucrativa

Subdominio 1º nivel. Geográficos	Significado
at	Austria
au	Australia
ca	Canadá
de	Alemania
es	España
fr	Francia
uk	Reino Unido

El siguiente dominio suele hacer referencia a la institución en concreto, no al tipo, a través de las iniciales de esta. El último domínio hace referencia al nombre de la máquina.

Ejemplos de direcciones

flopez@kant.dcs.cie.uva.es
zurita@horru.etsiig.uniovi.es
centauro.aulario.uniovi.es
cgomez@cat.es

Se suelen utilizar siempre letras minúsculas para los nombres asociados a las direcciones IP

Relación entre direcciones ip y direcciones físicas

Se debe relacionar la dirección IP con suministrada con una dirección física. Situándose en la jerarquía de niveles utilizada por Internet, se observa que por debajo del protocolo IP existe el nivel de enlace, en el se asientan protocolos como ARP o RARP. Estos protocolos resuelven problemas relacionados con las direcciones.

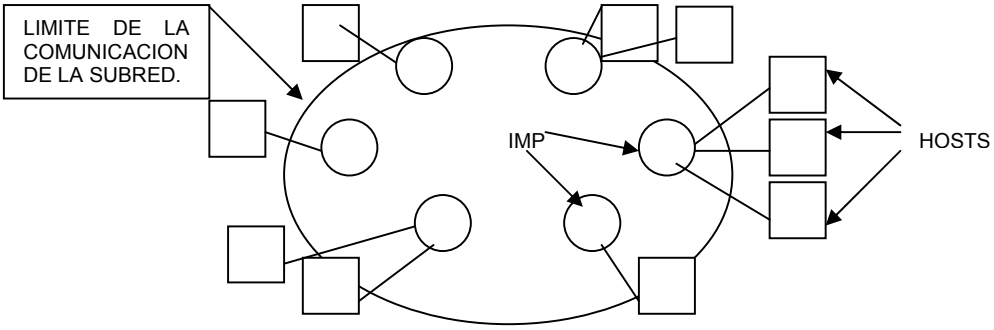
ARP: Convierte una dirección IP en una dirección física.
RARP: Convierte una dirección física en una dirección IP.

En cada host debe existir una tabla de encaminamiento, que está limitada a la red que pertenece. Si la dirección IP no pertenece a la red, entonces hace dirigir los paquetes IP hacia el gateway o router que esté conectado a esa red, el cual ya poseen unas tablas que referencias las redes que conocen. El contenido de estas tablas puede variar dinámicamente.

Subredes y mascaras.
Subredes:
En toda red existe una colección de maquinas destinadas para correr programas de usuario (aplicaciones), a estas les llamaremos host estos están conectados mediante una subred de comunicación, o simplemente subred. El trabajo de la subred consiste en envía mensajes entre host, de la misma manera como el sistema telefónico envía palabras entre las persona que habla y la que escucha. El diseño completo de la red se simplifica notablemente cuando se separa n los aspectos puros de comunicación de la red (la subred), de los aspectos de la aplicación(los host). Una subred en la mayor parte de las redes WAN consiste de 2 componentes diferentes:

- ✓ Las líneas de transmisión (también conocido como: circuitos, canales o troncales): se encargan de mover los bits entre las maquinas.
- ✓ Los elementos de conmutación (también conocido como: IMP procesadores de intercambio de mensajes.): son ordenadores especializados que se utilizan para conectar dos o más líneas de transmisión. Cuando los datos llegan por una entrada, el elemento de conmutación deberá de seleccionar la línea de salida para reexpedirlos.

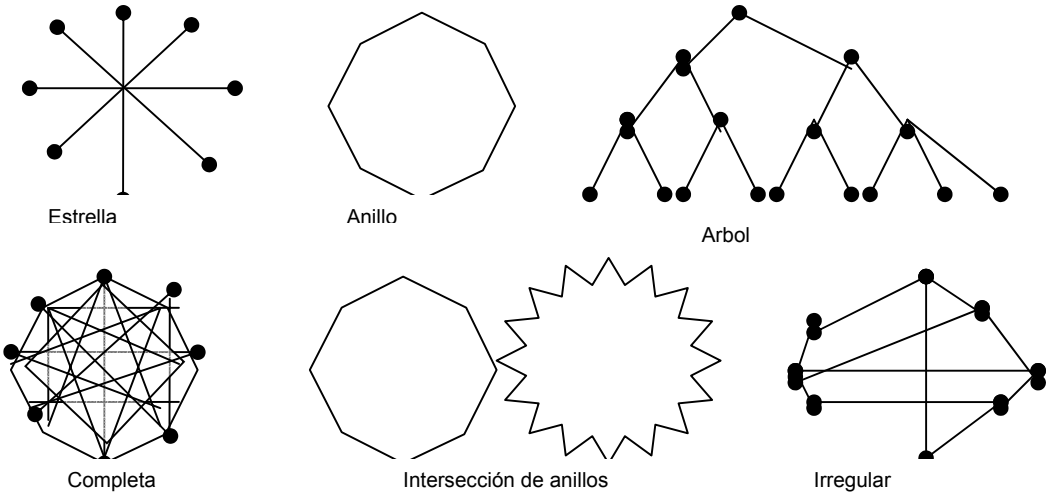
Relación entre los hosts y la subred.



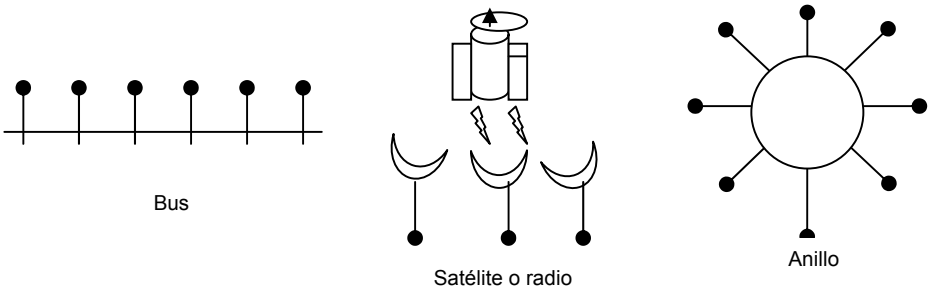
En general hay dos tipos para la red de comunicación:

1. Canales punto a punto.
2. Canales de difusión.

Canales punto a punto.
La red contiene varios cables o líneas telefónicas, conectadas cada una de ellas un par de IMP. Si dos IMP desean comunicarse y no comparten un cable común, deberán hacerlo indirectamente atraves de otros IMP. Cuando un mensaje (en le contexto de subred se llama: Paquete) se envía de un IMP a otro, atraves de 1 o mas IMP intermediarios. Se almacenará ahí y no continuara su camino hasta que la línea de salida este libre para reexpedirlo. La subred que usa este principio se denomina subred punto a punto, de almacenamiento y reenvío o de conmutación de paquetes. Casi todas las redes WAN tienen este principio. Un aspecto importante de diseño, cuando se utiliza una subred punto a punto, consiste en considerar como deberá ser la topología de interconexión de los IMP. En la figura se muestran varias topologías posibles para una subred punto a punto.



Canales de difusión.
La usan la mayoría de las redes LAN y un numero reducido de WAN, los sistemas de difusión tienen solo un canal de comunicación que, a su vez, es compartido con todas las máquinas que constituyen la red. El paquete que una máquina envía son recibidos por todas las demás. El campo de dirección en el interior del paquete especificará a quien va dirigido. Por ejemplo: Un individuo que esta parado en el extremo de un pasillo compuesto por varios cuartos, y desde de ese lugar empieza gritar "watson ven acá" aunque el paquete(el grito) es escuchado por varios personas en los cuartos, solo una persona (watson) responderá, y los demás solo lo ignorarán. Estos sistemas también tienen la capacidad de enviar un paquete todos los destinos empleando un código especial, incluido en le campo de dirección. Las subredes de difusión pueden dividirse en estáticas y dinámicas.
Comunicación de redes de difusión:



Mascara de subred:
Cuando los anfitriones utilizan el direccionamiento de subred, algunos de los bits en la porción hostid de su dirección IP identifican una red física. Para participar en el direccionamiento de la subred, un anfitrión necesita que saber que los bits de la dirección de red de redes de 32 bits corresponden a la red física, así como que bits corresponden a los identificadores del anfitrión. La información necesaria para interpretar la dirección se representa en una cantidad de 32 bits llamada mascara de subred(subnet mask).
DNS.
El mecanismo que implanta una jerarquía de nombres de maquina para alas redes TCP/IP se conoce como Domain Name System (sistema de nombres o nomenclatura de dominio o DNS). El DNS tiene 2 aspectos conceptualmente independientes. El primero es abstracto, especifica la sintaxis del nombre y las reglas para delegar la autoridad respecto a los nombres. El segundo es el concreto: especifica la construcción de un sistema de computación distribuido que transforma eficientemente los nombres en direcciones. El DNS se vale de un esquema de nombres jerárquico, conocido como nombre de dominio, este consiste de una secuencia de nombres separados por un carácter delimitador (el punto). Así el nombre de dominio: **cs.purdue.edu** En el ejemplo el dominio de nivel inferior es **cs.purdue.edu**(el nombre del dominio del depto. de ciencias de la computación de la U. de purdue) el segundo nivel de es **purdue.edu**(nombre de dominio para la U. de purdue), y el nivel superior es: **edu**(nombre de dominio para la institución educativa). El local primero y el dominio superior al ultimo.

Llamadas a procedimientos remotos.
En lugar de definir el protocolo NFS de cero, los diseñadores prefirieron construir tres piezas independientes. El protocolo NFS (sistema de archivos de red, proporciona un acceso de archivos compartidos en línea que es transparente e integrado) es en si, un mecanismo general de llamada de procedimiento remoto(remote procedure call o RPC por sus siglas en ingles) y una representación de datos externa(external data representation o XDR) de propósito general. La RPC es una tecnología en la que un programa invoca servicios atraves de una red haciendo modificaciones en los procedimientos de llamadas. La RPC y la XDR proporcionan mecanismos que los programadores pueden utilizar para construir programas distribuidos. por ejemplo, un programador puede dividir un programa de lado como cliente y de otro como servidor y que utilicen la llamada RPC como principal mecanismo de comunicación. Cuando el programa de lados del cliente que sé este ejecutando llama a uno de los procedimientos remotos, la RPC recolecta automáticamente los valores para los argumentos, forma un mensaje, envía el mensaje al servidor remoto, espera una respuesta y almacena los valores devueltos en los argumentos designados. El mecanismo RPC oculta todos los detalles de los protocolos, haciendo posible que los programadores que saben un poco acerca de los protocolos de comunicación subyacentes escriban programas distribuidos.

Programacion con sockets.

El Paradigma de E/S de UNIX y la E/S de la Red

En primer lugar hemos de distinguir entre los protocolos de interface y el TCP/IP, debido a que los estándares no especifican exactamente cómo es que interactúan los programas de aplicación con el software de protocolo. A pesar de la carencia de un estándar, veremos la interface del UNIX BSD como se emplea el TCP/IP en programación. En particular, la interface ***Winsock*** proporciona la funcionalidad socket para Ms Windows. Unix fue desarrollado y diseñado como un sistema operativo de tiempo compartido para computadoras uniprocesador. Se trata, como ya es sabido, de un S.O. orientado a proceso, en el que cada programa de aplicación se ejecuta como un proceso de nivel de usuario. Derivados de los MULTICS, los primitivos sistemas de E/S de UNIX siguen un paradigma conocido como "*Open-Read-Write-Close*": antes de que un proceso de usuario pueda ejecutar operaciones de E/S, llama a *Open* para especificar el archivo o dispositivo que se va a utilizar (recuerdese la independencia de dispositivo de UNIX) y obtiene el permiso. La llamada a *Open* devuelve un pequeño entero (el descriptor de archivo) que el proceso utiliza al ejecutar las operaciones de E/S en el archivo abierto. Una vez abierto un objeto, se pueden hacer las llamadas a *Read* y/o *Write*. Tanto Read como Write toman tres argumentos (descriptor de archivo, dirección del buffer y nº de bytes a transferir). Una vez completadas estas operaciones el proceso llama a *Close*. Originalmente, todas las operaciones UNIX se agrupaban como se ha descrito anteriormente, y una de las primeras implementaciones de TCP/IP también utilizó éste paradigma. Pero el grupo que añadió los protocolos TCP/IP al BSD decidió que, como los protocolos de red eran más complejos que los dispositivos convencionales de E/S, la interacción entre los programas de usuario y los protocolos de red debías ser más compleja. En particular, la interface de protocolo debía permitir a los programadores crear un código de servidor que esperaba las conexiones pasivamente, así como también un código cliente que formara activamente las conexiones. Para manejas datagramas, se decidió abandonar este paradigma.

La abstracción de SOCKET

La base para la E/S de red en UNIX se centra en una abstracción conocida como ***socket***. El socket es la generalización del mecanismo de acceso a archivos de UNIX que proporciona un punto final para la comunicación. Al igual que con el acceso a archivos, los programas de aplicación requieren que el S.O. cree un socket cuando se necesite. El S.O. devuelve un entero que el programa de aplicación utiliza para hacer referencia al socket recientemente creado. La diferencia principal entre los descriptores de archivo y los descriptores de socket es que el sistema operativo enlaza un descriptor de archivo a un archivo o dispositivo del sistema cuando la aplicación llama a Open, pero puede crear sockets sin enlazarlos a direcciones de destino específicas. Básicamente, el socket es una API en la que el servidor espera en un puerto predefinido y el cliente puede utilizar sin embargo un puerto dinámico.

EJEMPLOS:

- Creación de un socket:
  resultado = socket (pf, tipo, protocolo)

El argumento PF especifica la familia de protocolo que se va utilizar con el socket (v.q. PF_INET para TCP/IP). El argumento tipo especifica el tipo de comunicación que se desea (v.q.SOCK_DGRAM para servicio de entrega de datagramas sin conexión, o SOCK_STREAM para servicio de entrega confiable de flujo).

- Envío de datos:
  write (socket, buffer, lenght)
- Especificación de una dirección local:
  bind (socket, localaddr, addrlen)

Inicialmente, un socket se crea sin ninguna asociación hacia direcciones locales o de destino. Para los protocolos TCP/IP, esto significa que ningún número de puerto de protocolo local se ha asignado y que ningún puerto de destino o dirección IP se ha especificado. En muchos casos, los programas de aplicación no se preocupan por las direcciones locales que utilizan, ni están dispuestos a permitir que el software de protocolo elija una para ellos. Sin embargo, los procesos del servidor que operan en un puerto "bien conocido" deben ser capaces de especificar dicho puerto para el sistema. Una vez que se ha creado un socket, el servidor utiliza una llamada del sistema BIND (enlace) para establecer una dirección local para ello. BIND tiene la forma que se ha descrito arriba.

2 Teoría de Enrutamiento

Protocolo Spanning Tree

Tan pronto como cada dispositivo ha aprendido la configuración de la red, un bucle presenta la información de conflictos en el segmento en que una dirección específica se localiza y obliga al dispositivo a remitir todo el tráfico. El Algoritmo Spanning Tree Protocol es una norma del software (especificaciones IEEE 802.1d) para describir cómo los puentes y conmutadores pueden comunicarse para evitar bucles en la red.

Intercambiando paquetes denominados BPDU, los puentes y conmutadores establecen un único camino para alcanzar cada segmento de la red. En algunos casos, un puerto de un conmutador o puente puede ser desconectado si existe otro camino al mismo segmento. El proceso de transmitir los paquetes BPDU es continuo, por lo que si un puente o conmutador falla repentinamente, el resto de los dispositivos reconfiguran sus rutas para permitir que cada segmento sea alcanzado. En algunos casos, los administradores de la red diseñan bucles en redes con puentes, de forma que si un puente o conmutador falla, el algoritmo Spanning Tree calculará la ruta alternativa en la configuración de la red. Para que esto funcione correctamente, todos los conmutadores y puentes de la red deben de soportar este protocolo.

En inter-redes medias y grandes, cuando se usan puentes adicionales para conectar un número creciente de segmentos de LAN, es muy probable que se creen múltiples caminos entre los segmentos LAN inter-conectados. La creación de caminos múltiples causa "bucles activos" qué resultan en una rápida degradación de la actuación de la red global, porque múltiples puentes estarán transmitiendo el mismo tráfico entre los segmentos de LAN interconectados.

El Spanning Tree Protocol fue creado para superar automáticamente el problema de caminos múltiples entre los segmentos. Con todos los puentes en la red ejecutando STP, el puente(s) adicional(es) que este(n) creando un camino redundante, negociarán y sólo uno de ellos se usará para transferir el tráfico. Si el puente activo falla, un puente ocioso se apercibirá y empezará a transferir el tráfico en su lugar. Obsérvese que, de este modo, se puede emplear un puente redundante para proteger segmentos de la red críticos.

Cuando existe más de un camino de puente entre los segmentos LAN, el STP definirá un puente activo y el resto se pondrá en modo ocioso. El puente activo continúa enviando mensajes STP a la red de puentes STP para indicar que todavía está vivo. Si el puente activo falla, el STP reconfigurará la red automáticamente y activará un puente redundante previamente ocioso para asegurar que los datos continúan fluyendo.

Algoritmos de ruteo

- El *algoritmo de ruteo* decide en qué línea de salida se debiera transmitir un paquete que llega. Propiedades deseables:
    - Correctitud y sencillez.
    - Robustez. Una red puede tener que operar por años y experimentará fallas de software y hardware. El algoritmo de ruteo no debe requerer que se reinicializa la red después de fallas parciales.
    - Estabilidad. Debiera tener un equilibrio.
    - Justicia y optimalidad. Están frecuentemente contradictorias. Se necesita una balanza entre la eficiencia global y la justicia al individual. ¿Qué podemos optimizar? El retraso por paquete o la

utilización global de la red son posibilidades. Estos también están contradictorios, porque con 100% utilización los retrasos aumentan. Una solución intermedia es minimizar el número de saltos.

- Los algoritmos pueden ser adaptativos o no. Los primeros cambian sus decisiones de ruteo para reflejar la topología y el tráfico en la red. Los últimos son estáticos.

- **El principio de optimalidad.** Si el ruteador J está en el camino óptimo desde ruteador I a ruteador K, entonces la ruta óptima desde J a K está en la misma ruta. El conjunto de rutas óptimas forma el *árbol de hundir (sink tree).* El fin de los algoritmos de ruteo es descubrir y usar los árboles de hundir de todos los ruteadores. Un problema es que la topología cambia.

Algoritmos estáticos

- **Camino más corto.** Se calculan los caminos más cortos usando alguna métrica. Posibilidades: el número de saltos, la distancia física, el retraso de transmisión por un paquete de prueba, el ancho de banda, el tráfico promedio, el costo de comunicación, etc.

- **Inundación.** Se manda cada paquete que llega sobre todas las otras líneas. Puede generar un número infinito de paquetes, así que se necesita un método para restringir la inundación.

    - Se puede usar un contador de saltos en cada paquete que se decrementa después de cada salto. Cuando el contador es cero se descarta el paquete.

    - Se pueden guardar números de secuencia agregados por cada ruteador a los paquetes. Los ruteadores mantienen listas de los números de secuencia más altos vistos y descartan los paquetes que son duplicados.

    - En la *inundación selectiva* se mandan los paquetes solamente sobre las líneas que salen más o menos en la dirección correcta.

- **Ruteo basado en el flujo.** Usa la topología y la carga para determinar las rutas óptimas. Si el tráfico entre nodos es conocido, se lo puede analizar usando la teoría de colas. Probando conjuntos distintos de rutas se puede minimizar el retraso promedio de la red.

- En general las redes modernas usan los algoritmos dinámicos en vez de los estáticos.

Ruteo de vector de distancia

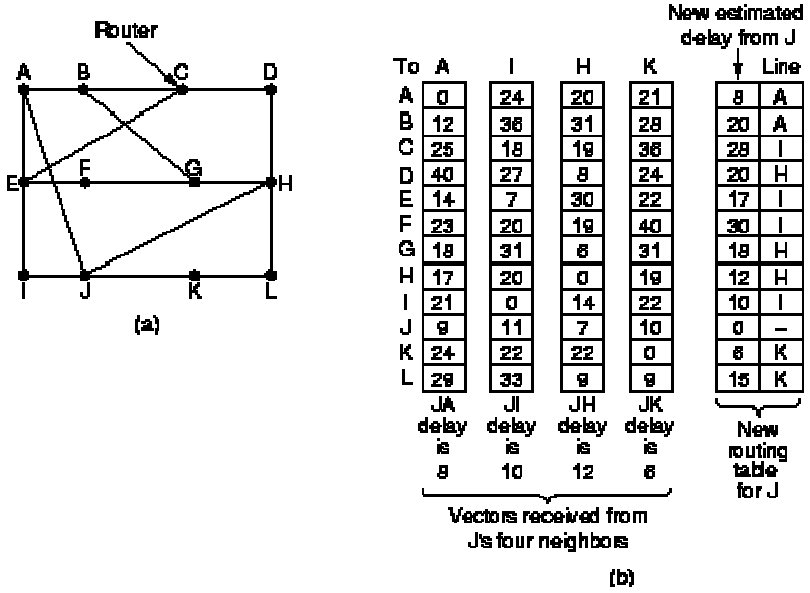
- Se llaman estos algoritmos también *Bellman-Ford* y *Ford-Fulkerson*. Eran los algoritmos originales de ruteo de la ARPANET.

- Cada ruteador mantiene una tabla (un vector) que almacena las mejores distancias conocidas a cada destino y las líneas a usar para cada destino. Se actualizan las tablas intercambiando información con los vecinos.

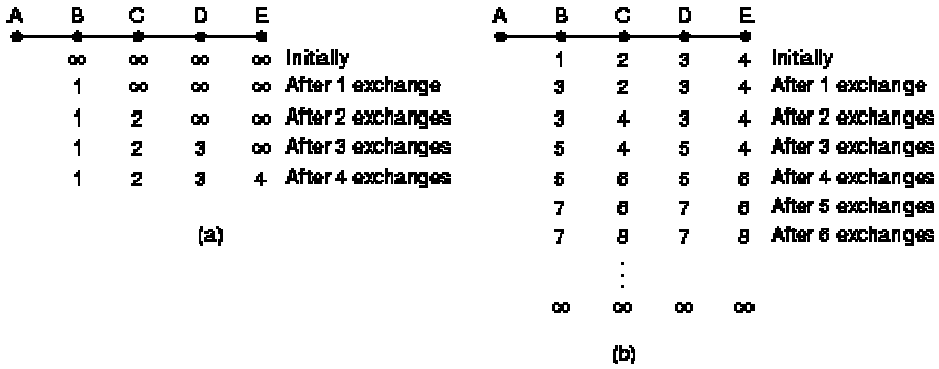
- La tabla de un ruteador almacena una entrada para cada uno de los ruteadores en la subred (los ruteadores son los índices). Las entradas almacenan la línea preferida de salida y una estimación del tiempo o la distancia al destino. Se pueden usar métricas distintas (saltos, retrasos, etc.).

- Cada ruteador tiene que medir las distancias a sus vecinos. Por ejemplo, si la métrica es el retraso, el ruteador la puede medir usando paquetes de eco.

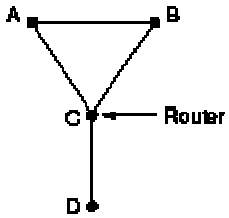
- Cada T msegs los ruteadores intercambian sus tablas con sus vecinos. Un ruteador usa las tablas de sus vecinos y sus mediciones de las distancias a sus vecinos para calcular una nueva tabla.



- El ruteo de vector de distancia sufre el problema que incorpora buenas noticias rápidamente pero malas noticias muy lentamente. Por ejemplo, en la parte (a) del dibujo siguiente el ruteador A acaba de subir. En esta red lineal la distancia nueva a A (en saltos) se propaga un salto por intercambio. Por contraste, en la parte (b) A acaba de bajar. Aunque B ahora no tiene una ruta a A, cree que hay una ruta a través de C, que cree que hay una ruta a través de B. Los ruteadores no pueden detectar el ciclo, y el número de saltos a A crece por solamente uno en cada turno. Este problema se llama *contar a infinito*, y hay que establecer un valor de infinito suficiente pequeño para detectarlo. Por ejemplo, el valor puede ser la longitud del camino más largo más uno.



- Hay muchas soluciones a este problema, pero ninguna lo soluciona completamente. Una usada frecuentemente es la del *horizonte partido.* En esta variación del algoritmo la única diferencia es que siempre se reporta una distancia infinita a ruteador X sobre la línea que se usa para rutear a X.
    - En nuestro ejemplo esta modificación permite que las malas noticias se propagan un salto por intercambio.
    - Por desgracia no funciona siempre. En el dibujo siguiente, A y B cuentan a infinito cuando D baja.



Ruteo de estado de enlace

- En 1979 se reemplazó el uso del ruteo de vector de distancia en la ARPANET. Tenía dos problemas principales:
    - La métrica era la longitud de las colas y no consideraba los anchos de banda de las líneas (originalmente todos eran 56 kpbs).
    - El tiempo para converger era demasiado grande.
- El nuevo algoritmo que se usa es el *ruteo de estado de enlace.* Tiene cinco partes. Cada ruteador tiene que
    - Descubrir sus vecinos y sus direcciones.
    - Medir el retraso o costo a cada vecino.
    - Construir un paquete con la información que ha averiguado.
    - Mandar este paquete a todo los ruteadores.
    - Calcular la ruta mínima a cada ruteador.
- **Descubrir los vecinos.** Cuando se bootea un ruteador, manda paquetes especiales de saludos sobre cada línea punto-a-punto suya. Los vecinos contestan con sus direcciones únicas. Si más de dos ruteadores están conectados por la LAN, se modela la LAN como un nodo artificial.
- **Medir el costo.** El ruteador manda paquetes de eco que los recipientes tienen que contestar inmediatamente. Se divide el tiempo por el viaje de ida y vuelta para determinar el retraso.
    - Un punto interesante es si debiera incluir en el retraso la carga de la línea. Esto corresponde a iniciar el reloj del viaje cuando se pone el paquete en la cola o cuando el paquete alcanza la cabeza de la cola.
    - Si incluimos la carga, se usan las líneas menos cargadas, que mejora el rendimiento.
    - Empero, en este caso es posible tener oscilaciones grandes en el uso de las líneas.
- **Construir el paquete.** El paquete consiste en la identidad del mandador, un número de secuencia, la edad, y la lista de vecinos y retrasos. Se pueden construir los paquetes periódicamente o solamente después de eventos especiales.
- **Distribuir los paquetes de estado de enlace.** Esto es la parte más difícil del algoritmo, porque las rutas en los ruteadores no cambian juntas. La idea fundamental es usar la inundación.
    - Para restringir la inundación se usan los números de secuencia que se incrementan cada vez se reenvía un paquete. Los ruteadores mantienen pares del ruteador de fuente y el número de secuencia que han visto, y descartan los paquetes viejos. Los paquetes nuevos se reenvían sobre todas las líneas salvo la de llegada.
    - Para evitar que el número de secuencia se desborda, se usan 32 bits.

  - Para evitar que los paquetes pueden vivir por siempre, contienen un campo de edad que se decrementa.
  - Si un ruteador cae o un número de secuencia se convierte malo, se perderán paquetes. Por lo tanto se incluye un campo de edad en cada entrada en la lista. Se decrementa este campo cada segundo y se descarta la información que tiene una edad de cero.

- **Calcular las rutas.** Se usa el algoritmo de Dijkstra. Un problema es que, debido a errores en los ruteadores, puede haber problemas en las rutas.

Ruteo jerárquico

- Las tablas de ruta crecen con la red. Después de algún punto no es práctico mantener toda la información sobre la red en cada ruteador.
- En el ruteo jerárquico se divide la red en regiones. Los ruteadores solamente saben la estructura interna de sus regiones.
- Para una subred de N ruteadores el número óptimo de niveles es lnN.

Ruteo de broadcast

- Para el broadcast de información hay algunas posibilidades.
- La más sencilla es mandar un paquete distinto a cada destino, pero esta malgasta ancho de banda.
- Otra posibilidad es la inundación pero genera demasiado paquetes y consume demasiado ancho de banda.
- En el *ruteo de destinos múltiples,* cada paquete almacena la lista de destinos. El ruteador divide el paquete en nuevos para cada línea de salida. Cada paquete tiene una nueva lista de destinos. Se divide la lista original sobre las líneas de salida.
  - Se puede usar el árbol de hundir o cualquier árbol de cobertura para la red, pero esto requiere que los ruteadores saben el árbol (que no es el caso en el ruteo de vector de distancia).
- En el *algoritmo que reenvía usando el camino inverso (reverse path forwarding),* se aproxima el comportamiento del uso de un árbol de cobertura. Cuando un paquete llega, se lo reenvía solamente si llegó sobre la línea que se usa para mandar paquetes a su fuente. Es decir, si el paquete llegó sobre esta línea, es probable que tome la ruta mejor a esta ruteador. Si no, es probable que sea un duplicado.

Hay dos técnicas básicas de enrutamiento:

  - Protocolos de Vector de Distancia: los enrutadores intercambian con sus vecinos información sobre cómo llegar a todos los destinos
    - Por ejemplo, RIP: Routing Information Protocol
  - Protocolos de Estado de Enlaces: los enrutadores intercambian con todos los enrutadores la información sobre sus enlaces.
    - Por ejemplo, OSPF: Open Shortest Path First

Enrutamiento estático vs. Dinámico

- **Enrutamiento estático**
  - Fácil de entender
  - Fácil de configurar para redes pequeñas

- **Enrutamiento dinámico**
    - Esencial para redes grandes
    - Potencialmente más difícil de configurar (p.e. OSPF)
    - **Conceptos básicos de RIP, IGRP,EGP,BGP,OSPF**

Internet se compone de múltiples subredes interconectadas por enrutadores.
Nombre - Dirección - Ruta
El DNS traduce el nombre de una computadora en una dirección IP.
Los enrutadores utilizan la dirección IP para transportar datagramas sobre una ruta en Internet hasta la computadora destino.
Los protocolos de enrutamiento son algoritmos que permiten decidir cuál es la mejor ruta que debe seguir un datagrama
para llegar a su destino.
Los protocolos de enrutamiento se utilizan para actualizar dinámicamente las tablas de enrutamiento.
Internet es una red formada por Sistemas Autónomos interconectados.
Un Sistema Autónomo está constituido por un conjunto de subredes y enrutadores que tienen una administración común.
Cada Sistema Autónomo – puede escoger su propio protocolo de enrutamiento
debe intercambiar información de enrutamiento con otros Sistemas Autónomos

Interior Gateway Protocol (IGP)
- Entre Sistemas Autónomos

Exterior Gateway Protocol (EGP)

• IGP
– Vectores de Distancias RIP-2 (RFC 2453)
- Estado de Enlaces OSPF-2 (RFC 2328)
-
• EGP
- Vectores de Ruta BGP-4 (RFC 1771)

RIP RIP Routing Information Protocol
• Utiliza un algoritmo de Vectores de Distancias.
• Este algoritmo fue usado en ARPANET desde 1969.
• Cada enrutador mantiene en su tabla de enrutamiento la distancia, en saltos, que lo separa de cada destino.
Cada enrutador envía a sus vecinos su vector de distancias cada 30 segundos.
Los mensajes RIP se encapsulan en datagramas UDP.
• En un mensaje RIP pueden enviarse hasta 25 entradas del vector de distancias.
• Para transportar vectores grandes se utilizan varios mensajes.
Cuando un enrutador A recibe de un vecino B su vector de distancias, actualiza la entrada de su tabla de enrutamiento
correspondiente a la red K si:
– A no conocía a K
– Bk < Ak + 1
– A enruta por B hacia K y Bk cambió
La actualización de la tabla de enrutamiento del enrutador A modifica el renglón correspondiente a la red K:
– la nueva distancia es Bk + 1
– el siguiente salto es B
• Una entrada de la tabla de enrutamiento se vuelve inválida si pasan 180 segundos sin que sea refrescada.

IGRP es un algoritmo propietario de Cisco que utiliza Vectores de Distancias.
El número de saltos no está limitado a 15.

Las actualizaciones se envían cada 90 segundos, por lo que se carga menos la red con información de enrutamiento.
Para evitar los ciclos que involucran más de dos enrutadores, un enrutador no toma en cuenta las actualizaciones recibidas para una ruta:
- durante 90 segundos después de haberla considerado inaccesible (*hold down)*, si el número de saltos ha crecido de manera importante (rutas envenenadas).
Utiliza como distancia una métrica compuesta ponderada:
- velocidad de transmisión, retardo, carga, tasa de error.
- Puede balancear la carga entre múltiples rutas que tienen una distancia equivalente.

OSPF Open Shortest Path First
• Los algoritmos de vectores de distancias son buenos para redes estables y pequeñas.
• Su principal desventaja es que no escalan bien: su desempeño es bajo en Sistemas Autónomos grandes ya que el tamaño de sus
mensajes es directamente proporcional al número de redes existentes.
OSPF • Es un protocolo de enrutamiento muy usado en Internet.
• Utiliza un algoritmo de Estado de Enlaces. La métrica utilizada por omisión por los enrutadores es inversamente proporcional a
la velocidad de transmisión del enlace:
– distancia = 108 / velocidad de transmisión
• Por ejemplo, para una red Ethernet a 10 Mbps, la distancia es 10.
Cada enrutador verifica continuamente los enlaces que lo unen con enrutadores adyacentes intercambiando mensajes *Hello.*
• Típicamente, los mensajes se envían cada 10 segundos y se considera que ha ocurrido una falla en un vecino si no se recibe un
mensaje de él durante 40 segundos. Cada enrutador difunde cada 30 minutos, o cuando hay un cambio en el estado de uno de sus enlaces, *Link State Advertisement*s a todos los enrutadores del Sistema Autónomo para notificarles el Estado de sus Enlaces.
Cada enrutador conoce entonces la topología completa del Sistema Autónomo (*link-state database*)y utiliza el algoritmo del camino más corto de Dijkstra para construir su tabla de enrutamiento.
• Cada enrutador construye un árbol de caminos más cortos con él como raíz.

BGP Border Gateway Protocol

Es el protocolo usado entre Sistemas Autónomos para intercambiar información de enrutamiento.
• Utiliza un algoritmo de Vectores de Rutas. Los enrutadores BGP deben configurarse para saber con quiénes deben intercambiar
información de enrutamiento.
• La adquisición de vecinos se realiza mediante el envío de mensajes *OPEN* y *KEEPALIVE*.
Los vecinos pueden ser otros enrutadores de frontera que se encuentran en el mismo
Sistema Autónomo (BGP interno).
• Los mensajes se intercambian a través de conexiones TCP.
Los mensajes *UPDATE* contienen anuncios de redes accesibles y la ruta correspondiente (trayectorias de Sistemas Autónomos), así
como retiros de redes que ya no son accesibles.
• Anunciar una ruta implica que el Sistema Autónomo correspondiente puede y acepta transportar información hacia un destino.
Cada enrutador BGP recibe de sus vecinos las rutas que emplean para llegar a cada posible destino y escoge la mejor.
• El criterio de selección no forma parte del protocolo.
Para tomar decisiones de enrutamiento, BGP puede tener en cuenta, por ejemplo, cuestiones políticas, económicas, de confiabilidad o de seguridad.
• Este tipo de consideraciones se configura manualmente en los enrutadores.

3. Dispositivos para interconexión.

- ***Modems***

Módem, equipo utilizado para la comunicación de computadoras a través de líneas analógicas de transmisión de datos. El módem convierte las señales digitales del emisor en otras analógicas susceptibles de ser enviadas por teléfono. Cuando la señal llega a su destino, otro módem se encarga de reconstruir la señal digital primitiva, de cuyo proceso se encarga la computadora receptora. En el caso de que ambos puedan estar transmitiendo datos simultáneamente, se dice que operan en modo full-duplex; si sólo puede transmitir uno de ellos, el modo de operación se denomina half-duplex. Para convertir una señal digital en otra analógica, el módem genera una onda portadora y la modula en función de la señal digital. El tipo de modulación depende de la aplicación y de la velocidad de transmisión del módem. Un módem de alta velocidad, por ejemplo, utiliza una combinación de modulación en amplitud y de modulación en fase, en la que la fase de la portadora se varía para codificar la información digital. El proceso de recepción de la señal analógica y su reconversión en digital se denomina demodulación. La palabra módem es una contracción de las dos funciones básicas: modulación y demodulación. Los primeros equipos eran muy aparatosos y sólo podían transmitir datos a unos 100 bits por segundo. Los más utilizados en la actualidad en los ordenadores personales transmiten la información a más de 33 kilobits por segundo. Pueden incluir funciones de fax y de contestador automático de voz.

- ***Repetidores***

Los **Repetidores** reexpiden bits de una red otra, haciendo que las dos se vean lógicamente como una sola red. A menudo las redes se dividen dos (o más) piezas, como consecuencia de las restricciones de máxima longitud de cable de cada pieza individual. Los repetidores son poco inteligentes (no hay software), solo copian los bits ciegamente y sin entender lo que están haciendo.

Sus principales características son:

- Conectan al nivel físico dos Intranets, o dos segmentos de Intranets. Hay que tener en cuenta que cuando la distancia entre dos host es grande, la señal que viaja por la línea se atenúa y hay que regenerarla.
- Permiten resolver problemas de limitación de distancias en un segmento de Intranet.
- Se trata de un dispositivo que únicamente repite la señal transmitida evitando su atenuación; de esta forma se puede ampliar la longitud del cable que soporta la red.
- Al trabajar al nivel más bajo de la pila de protocolos obliga a que:
  - Los dos segmentos que interconecta tenga el mismo acceso al medio y trabajen con los mismos protocolos.
  - Los dos segmentos tengan la misma dirección de red.

- ***Hubs (concentradores).***

Hubs (concentradores): Dispositivo que centraliza la conexión de los cables procedentes de las estaciones de trabajo. Dispositivo que interconecta host dentro de una red. Es el dispositivo de interconexión más simple que existe. Existen dos tipos de concentradores:

- ✓ **Pasivos.** Los concentradores pasivos son simplemente cajas que disponen de unos puertos a los que se conectan las estaciones de trabajo dentro de una configuración en forma de estrella. Únicamente se trata de un cuadro de uniones. Hubs pasivos: son simples armarios de conexiones. Permiten conectar nodos a distancias de hasta 30 metros. Generalmente suelen tener entre 8 y 12 puertos.
- ✓ **Activos.** Un concentrador activo es un concentrador que dispone de más puertos que un concentrador pasivo para la conexión de estaciones y que realiza más tareas, como puede ser la de amplificación de la señal recibida antes de su retransmisión. A veces se utilizan para estructurar la topología de una Intranet, permitiendo mayor flexibilidad en la modificación de ésta. Hubs activos: permiten conectar nodos a distancias de hasta 609 metros, suelen tener entre 8 y 12 puertos y realizan funciones de amplificación y repetición de la señal. Los más complejos además realizan estadísticas.

Sus principales características son:

- Se trata de un armario de conexiones 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.
- Se suelen utilizar para implementar topologías en estrella física, pero funcionando como un anillo o como un bus lógico.

- ***Conmutadores (switches).***

Redes conmutadas.
Consisten en un conjunto de nodos interconectados entre sí, a través de medios de transmisión (cables), formando la mayoría de las veces una topología mallada, donde la información se transfiere encaminándola del nodo de origen al nodo destino mediante conmutación entre nodos intermedios. Una transmisión de este tipo tiene 3 fases:

- Establecimiento de la conexión.
- Transferencia de la información.
- Liberación de la conexión.

Se entiende por conmutación en un nodo, a la conexión física o lógica, de un camino de entrada al nodo con un camino de salida del nodo, con el fin de transferir la información que llegue por el primer camino al segundo. Un ejemplo de redes conmutadas son las redes de área extensa. Las redes conmutadas se dividen en:

- Conmutación de paquetes.
- Conmutación de circuitos.

CONMUTACIÓN DE PAQUETES
Se trata del procedimiento mediante el cual, cuando un nodo quiere enviar información a otro, la divide en paquetes. Cada paquete es enviado por el medio con información de cabecera. En cada nodo intermedio por el que pasa el paquete se detiene el tiempo necesario para procesarlo. Otras características importantes de su funcionamiento son:

- En cada nodo intermedio se apunta una relación de la forma : "todo paquete con origen en el nodo A y destino en el nodo B tiene que salir por la salida 5 de mi nodo".
- Los paquetes se numeran para poder saber si se ha perdido alguno en el camino.
- Todos los paquetes de una misma transmisión viajan por el mismo camino.
- Pueden utilizar parte del camino establecido más de una comunicación de forma simultánea.

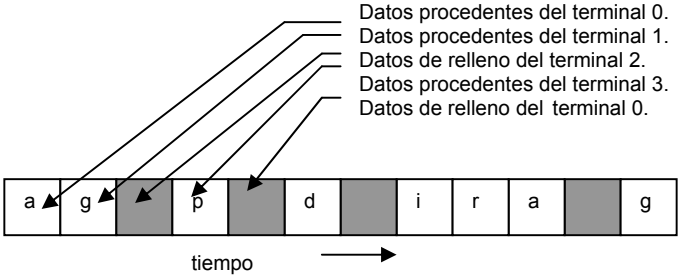
CONMUTACIÓN DE CIRCUITOS
Es el procedimiento por el que dos nodos se conectan, permitiendo la utilización de forma exclusiva del circuito físico durante la transmisión. En cada nodo intermedio de la red se cierra un circuito físico entre un cable de entrada y una salida de la red. La red telefónica es un ejemplo de conmutación de circuitos

- ***Multiplexores.***

Los controladores de terminal se dividen en dos clases generales:

- ✓ Multiplexores y,
- ✓ Concentradores

Un multiplexor es un dispositivo que acepta entradas procedentes de un conjunto de líneas con una secuencia estática y determinada; y genera salidas de datos en una sola línea de salida con la misma secuencia. Dado que cada ranura de tiempo de las salidas esta dedicada a una línea especifica de entrada. Un multiplexor con cuatro terminales:



A cada uno de los terminales, manejados por un TDM (multiplexor por división de tiempo) de 4 terminales, se les asigna la cuarta parte de las ranuras de tiempo de salida, independientemente de lo que ocupada que pudiera estar. Si cada uno de los 4 terminales funcionara a 1200 bps (bit x segundo), la línea de salida deberá ser de 4 x 1200 = 4800 bps, dado que deberán enviarse 4 caracteres durante cada ciclo de sondeo. La gran desventaja de los TDM, es que cuando no existe trafico en un terminal, se desperdicia una ranura de tiempo de salida. Estas se van llenado de información bajo una estricta rotación, como se muestra en la figura anterior. Si no hay datos, se usan unos

caracteres de relleno. No es posible saltar u omitir una ranura de tiempo, debido que el extremo receptor mantiene un seguimiento estricto sobre que carácter proviene de que terminal, mediante su posición en el flujo de salida. Inicialmente, el multiplexor y el ordenador se sincronizan por si mismos; ambos saben que el orden que deben utilizar esta dado, p.e: Por el patrón: 012301230123 .... los datos por si mismo no llevan una identificación indicativa de su origen. Si el multiplexor llegara a omitir una ranura de tiempo, suponiendo que no hubiera datos por transmitir procedentes del terminal, el receptor quedaría fuera de fase e interpretaría el origen de los caracteres siguientes de una manera incorrecta.

- ***Bridges (puentes)***

Nos permiten dos cosas: primero, conectar dos o más Intranets entre sí, aun teniendo diferentes topologías, pero asumiendo que utilizan el mismo protocolo de red, y segundo, segmentar una Intranet en otras menores. Los puentes trabajan en el nivel de enlace del modelo OSI de la ISO. Algunos de los motivos que nos pueden inducir a instalar un puente son ampliar la extensión de una Intranet y/o el número de nodos que la componen; reducir el cuello de botella del tráfico causado por un número excesivo de nodos unidos o unir Intranets de topologías similares como bus y anillo. Los puentes se pueden crear incorporando dos tarjetas de red (una de cada una de las Intranets a interconectar) dentro del mismo servidor (conectado obviamente a ambas redes), siempre que el sistema operativo de red de dicho servidor sea capaz de gestionarlo. Existen dos tipos de puentes: locales y remotos. Los puentes locales sirven para segmentar una Intranet y para interconectar Intranets que se encuentren en un espacio físico pequeño, mientras que los puentes remotos sirven para interconectar redes lejanas. **Sus principales características son:**

- Son dispositivos que ayudan a resolver el problema de limitación de distancias, junto con el problema de limitación del número de nodos de una red.
- Trabajan al nivel de enlace del modelo OSI, por lo que pueden interconectar redes que cumplan las normas del modelo 802 (3, 4 y 5). Si los protocolos por encima de estos niveles son diferentes en ambas redes, el puente no es consciente, y por tanto no puede resolver los problemas que puedan presentársele.
- Se utilizan para:
  - Ampliar la extensión de la red, o el número de nodos que la constituyen.
  - Reducir la carga en una red con mucho tráfico, uniendo segmentos diferentes de una misma red.
  - Unir redes con la misma topología y método de acceso al medio, o diferentes.
  - Cuando un puente une redes exactamente iguales, su función se reduce exclusivamente a direccionar el paquete hacia la subred destino.
  - Cuando un puente une redes diferentes, debe realizar funciones de traducción entre las tramas de una topología a otra.
- Cada segmento de red, o red interconectada con un puente, tiene una dirección de red diferente.
- Los puentes no entienden de direcciones IP, ya que trabajan en otro nivel.
- Los puentes realizan las siguientes funciones:
  - Reenvío de tramas: constituye una forma de filtrado. Un puente solo reenvía a un segmento a aquellos paquetes cuya dirección de red lo requiera, no traspasando el puente los paquetes que vayan dirigidos a nodos locales a un segmento. Por tanto, cuando un paquete llega a un puente, éste examina la dirección física destino contenida en él, determinado así si el paquete debe atravesar el puente o no.
  - Técnicas de aprendizaje: los puentes construyen tablas de dirección que describen las rutas, bien sea mediante el examen del flujo de los paquetes (puenteado transparente) o bien con la obtención de la información de los “paquetes exploradores” (encaminamiento fuente) que han aprendido durante sus viajes la topología de la red.
- Los primeros puentes requerían que los gestores de la red introdujeran a mano las tablas de dirección.
- Los puentes trabajan con direcciones físicas

- ***Router (encaminador).***

Los Routers (encaminadores): se tratan de dispositivos que interconectan Intranets al nivel de red del modelo OSI de la ISO. Realizan funciones de control de tráfico y encaminamiento de paquetes por el camino más eficiente en cada momento. La diferencia fundamental con los bridges es que éstos no son capaces de realizar tareas de encaminamiento en tiempo real, es decir, una vez que tiene asignado un camino entre un nodo origen y uno destino siempre lo utilizan, aunque esté saturado de tráfico, mientras que los routers son capaces de modificar el camino establecido entre dos nodos dependiendo del tráfico de la red y otros factores.

Sus principales características son:

- Es como un puente incorporando características avanzadas.
- Trabajan al nivel de red del modelo OSI, por tanto trabajan con direcciones IP.
- Un router es dependiente del protocolo.
- 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.
- La forma que tiene de funcionar es la siguiente.
    - Cuando llega un paquete al router, éste examina la dirección destino y lo envía hacia allí a través de una ruta predeterminada.
    - Si la dirección destino pertenece a una de las redes que el router interconecta, entonces envía el paquete directamente a ella; en otro caso enviará el paquete a otro router más próximo a la dirección destino.
    - Para saber el camino por el que el router debe enviar un paquete recibido, examina sus propias tablas de encaminamiento.
- Existen routers multiprotocolo que son capaces de interconectar redes que funcionan con distintos protocolos; para ello incorporan un software que pasa un paquete de un protocolo a otro, aunque no son soportados todos los protocolos.
- Cada segmento de red conectado a través de un router tiene una dirección de red diferente.

- ***Enrutadores.***

Enrutadores multiprotocolo.
Existen routers multiprotocolo que son capaces de interconectar redes que funcionan con distintos protocolos; para ello incorporan un software que pasa un paquete de un protocolo a otro, aunque no son soportados todos los protocolos.

- ***Gateways (pasarelas).***

Las Gateways (pasarelas): se tratan de ordenadores que trabajan al nivel de aplicación del modelo OSI de la ISO. Es el más potente de todos los dispositivos de interconexión de Intranets. Nos permiten interconectar Intranets de diferentes arquitecturas; es decir, de diferentes topologías y protocolos; no sólo realiza funciones de encaminamiento como los routers, sino que también realiza conversiones de protocolos, modificando el empaquetamiento de la información para adaptarla a cada Intranet.
Sus características principales son:

- Se trata de un ordenador u otro dispositivo que interconecta redes radicalmente distintas.
- Trabaja al nivel de aplicación del modelo OSI.
- Cuando se habla de pasarelas al nivel de redes de área local, en realidad se está hablando de routers.
- Son capaces de traducir información de una aplicación a otra, como por ejemplo las pasarelas de correo electrónico.

D. Seguridad de la información.

1. Seguridad.

Que es Encriptación

Toda encriptación se encuentra basada en un Algoritmo, la función de este Algoritmo es básicamente codificar la información para que sea indescifrable a simple vista , de manera que una letra *"A"* pueda equivaler a :*"5x5mBwE" o bien a "xQE9fq"*, el trabajo del algoritmo es precisamente determinar como será transformada la información de su estado original a otro que sea muy difícil de descifrar.

Una vez que la información arrive a su destino final, se aplica el algoritmo al contenido codificado *"5x5mBwE" o bien a "xQE9fq"* y resulta en la letra *"A"* o según sea el caso, en otra letra. Hoy en día los algoritmos de encriptación son ampliamente conocidos,es por esto que para prevenir a otro usuario "no autorizado" descifrar información encriptada, el algoritmo utiliza lo que es denominado **llave ("key")** para controlar la encriptación y decriptación de información. Algunos algoritmos son DES (algoritmo simétrico) AES que posiblemente suplantará a **DES** y uno de los más conocidos RSA (algoritmo asimétrico)

Que función tiene la llave ("key") ?

Existen dos tipos de llaves ("key's") , pero la de mayor uso en Internet es denominada "public key" o algoritmo asimétrico. El nombre "public" proviene de su funcionamiento: existe una llave pública que es dada a conocer a cualquier persona que así lo desee (todo Internet), esta llave pública es utilizada por los emisores de mensajes para encriptar información , sin embargo, existe otra llave (su pareja por llamarla de alguna manera) *única* que es conocida *exclusivamente* por el destinatario del mensaje, y es mediante esta llave *única* | *secreta* que el destinatario descifra ("decripta") los mensajes encriptados por el emisor.

Firmas Digitales ("Digital Signatures")

Una **firma digital** utiliza el mismo funcionamiento del "public key" o algoritmo asimétrico mencionado anteriormente.

Como se mencionó, existe una "llave pública" y una "llave secreta", en el caso de **firmas digitales** la llave pública que es ampliamente conocida es capaz de identificar si la información proviene de una fuente fidedigna.En otras palabras, la llave pública será capaz de reconocer si la información realmente proviene de la "llave secreta" en cuestión.Ejemplo:

El departamento de compras posee las *llaves públicas* de todos los empleados de la compañía, si llega un pedimento con la dirección de email del Director de Finanzas, Cómo puede asegurarse el departamento de compras que en realidad esta persona realizó el pedimento y no alguna otra que sobrepuso el email ?. La *llave secreta* del director de finanzas debe de encontrarse solo en su computadora, por lo tanto al enviar el mensaje electrónico esta *llave pública* se añadió al email,y por lo tanto las *llave publicas* determinarán si la *llave secreta* coincide con la del director.

Firmas Digitales en Internet

En el caso anterior de un Intranet, todas las *llaves públicas* provienen de una fuente fidedigna, esto es, las llaves "publicas" que posee el departamento de compras son autenticas ya que TODAS pertenecen sólo a empleados dentro de la compañía , la única posibilidad de fraude que existe,es si alguien trata de forjar la "llave secreta" de un empleado para hacerse pasar por otro.

Pero que sucede cuando este departamento de compras empiece a realizar transacciones en Internet ?

Ellos anuncian su "llave publica" para todos los usuarios de Internet, y como solo ellos poseen la "llave secreta" sólo ellos podrán descifrar("decriptar") la información. Pero ahora, surge la siguiente pregunta: Quien le garantiza a los usuarios de Internet que esta "llave publica" REALMENTE proviene de este departamento de compras ?

Para esto existen los **certificados digitales** que son emitidos por "agencias autorizadas" como Thawte o Verisign las cuales dan el VoBo("Visto Bueno") sobre la "llave publica".

Existen pocas compañías que realizan este servicio,pero debido a la naturaleza de las "llaves publicas" siempre debe de existir una agencia central que sea capaz de decir "Si, esta llave publica proviene del departamento de compras" eso es todo su servicio, esto garantiza a los usuarios finales de "Internet" que la "llave publica" ha sido reconocida por una autoridad confiable Thawte o Verisign

La secuencia de eventos es la siguiente:

1. Se adquiere un "Certificado Digital" de Thawte o Verisign (Costo aprox:$100-$350 Dlls U.S Anuales,variación depende de su uso)

2. Se coloca este certificado digital ("llave publica") en el servidor de páginas y se configura para que éste envíe información encriptada según sea necesario.

3. Cuando un usuario en Internet solicite información encriptada de nuestro sitio se envía esta "llave publica" para que pueda encriptar la información y enviarla de una manera segura al sitio.

4. Al recibir la "llave publica" el navegador ("Netscape" o "Explorer") del usuario final corrobora que en realidad esta "llave publica" proviene de quien dice, en este caso, la "llave publica" dice: "Soy la llave publica de osmosislatina.com y fui emitida por *Verisign* mi serie es:u7767DbXs4br342Dbnn6".

5. El navegador corrobora con *Verisign* (en este caso) y *continua* o *avisa* al usuario final el estado de la "llave publica".

- **NOTA:** Si el navegador ("Netscape" o "Explorer") no corrobora la veracidad del "certificado digital" *no implica que la información será enviada de manera insegura* , la encriptación seguirá siendo valida. Lo que sucederá es que cuando sus visitantes entren a páginas que requieran encriptación (transacciones financieras) , el Navegador desplegara un mensaje a sus visitantes indicándoles que la fuente de encriptación ("llave publica") es insegura; esto se debe a que nadie puede avalar su "llave publica", de nuevo **lo anterior no implica que la encriptación es invalida** solo insegura.

- En ocasiones lo anterior es suficiente para hacer desconfiar al usuario final o inclusive exponerse a que un tercero este generando esta "llave publica"

Encriptación de 40-bits y 128-bits.

Existen varios niveles de encriptación, pero las combinaciones más comunes son 40-512 bits ("llave secreta--llave pública") y 128-1024 bits ("llave secreta--llave pública"). La versión 128-1024 bits es el tipo de encriptación más fuerte que existe en el mercado. Actualmente U.S.A prohibe la exportación de productos con este tipo de Tecnología, pero cabe mencionar que ya existen varios productos producidos en Europa con esta Tecnología que no poseen tales restricciones de exportación.

La gran mayoría de los sitios en Internet utilizan la encriptación 40-512 bits, la encriptación 128-1024 bits es utilizada generalmente en transacciones de alto riesgo, como las bancarias.

¿Es segura la encriptación que existe hoy en día ?

Depende quien la intente observar !, aunque la información sea enviada encripatada, cualquier persona en Internet con entrenamiento mínimo puede interceptar esta información encriptada, sin embargo, para observarla requiere de su "llave privada".

Y es aquí donde depende quien intente observar esta información, considere que una computadora personal (PC) puede realizar *millones de operaciones por segundo*, debido a esto, no es tan ilusorio **generar una "llave privada"** a partir de cierta información interceptada ; las "llaves privadas" generalmente constan de 40-bits, en una PC es posible (aunque tardado) **procesar** estas *2^40 alternativas*, ahora bien, si se tienen varios servidores en *paralelo* realizando *trillones de operaciones por segundo* probablemente sea posible **procesar** estas *2^40 alternativas* en cuestión de **minutos**.

Lo anterior es una de la razones por las que U.S.A cuida (cuidaba!) con tanto recelo la exportación de encriptación de 128-bits, la cual es 3 veces más poderosa (*2^128 alternativas*) que la de 40-bits.

Públicamente se conoce que en los servidores más poderosos del mercado es posible descubrir una "llave privada" en cuestión de **días** de procesamiento. Esto obviamente detiene aquellas personas ("hackers") con servidores "comunes" y en este caso hasta oficinas de seguridad gubernamentales en "decriptar" información con este tipo de encriptación

- ***Autentificación: código de acceso y confirmación de identidad.***

En los sistemas orientados a conexión, la autentificación puede realizarse en le momento en que se establece una sesión. El planteamiento tradicional consiste en hacer que el usuario compruebe su identidad, mediante la presentación de una contraseña. Este método no solo expone al usuario a una interceptación pasiva, sino que también puede exigirle a la computadora que autentifique (por ejemplo, el banco) mantener una lista interna de contraseñas, lo cual, en si mismo, viene a ser un problema potencial de seguridad. Mediante le empleo de una clave publica criptográfica, es posible efectuar la autentificación de una manera fiable, sin la necesidad de almacenar ninguna contraseña. Para continuar con el ejemplo del banco, en el momento en que se abre una cuenta, el cliente escoge una clave publica y una clave privada; entregándole al banco la clave publica y conservando, para si, la privada. Cuando el cliente llama al banco para establecer una sesión. Este selecciona un numero aleatorio, lo pone en clave utilizando clave publica del supuesto cliente, y lo envía al usuario, que hace la llamada al banco desafiándolo para que lo devuelva descifrado. Solo la persona que conoce la clave de descifrado será capaz de efectuar el proceso, por lo que los impostores no podrán pasar de esta prueba. Además, el intruso que este registrando todo el

trafico no tendrá beneficio alguno, porque en la siguiente ocasión el banco escogerá un numero aleatorio diferente. El código de redundancia hace muy improbable que un intruso pueda falsificar o modificar un mensaje (en texto cifrado), y todavía obtenga el código de redundancia correcto (del texto en claro).

Proxy

Los servidores *proxy* son un invento que permite el acceso directo a la Internet desde detrás de un cortafuegos. Funcionan abriendo un *socket* en el servidor y permitiendo la comunicación con la Internet a través de él.
Por ejemplo: si una computadora, estuviera dentro de la red protegida y quisiera ver el Web, pondría un servidor proxy en el cortafuegos. El servidor proxy estaría configurado para hacer que las peticiones de
conexión de esa computadora al puerto 80 de otra máquina, se conectara a su puerto 1080, y él mismo establecería una conexión con el puerto 80 de la máquina deseada. A partir de entonces reenviaría todos los datos de esa conexión a la otra máquina.Un servidor proxy es ante todo un *dispositivo de seguridad*
Este tipo de servidores se usa principalmente para controlar, o supervisar, el tráfico hacia el exterior. Algunos proxy de aplicación almacenan en una memoria de almacenamiento intermedio una copia local de los datos
solicitados. Esto reduce el ancho de banda preciso y acelera el acceso a los mismos datos para el siguiente usuario. Ofrece una inequívoca prueba de lo que fue transferido.

Existen dos tipos de servidores proxy
• Servidores proxy de aplicación - son los que hacen el trabajo por nosotros.
• Servidores proxy SOCKS - establecen conexiones entre puertos.

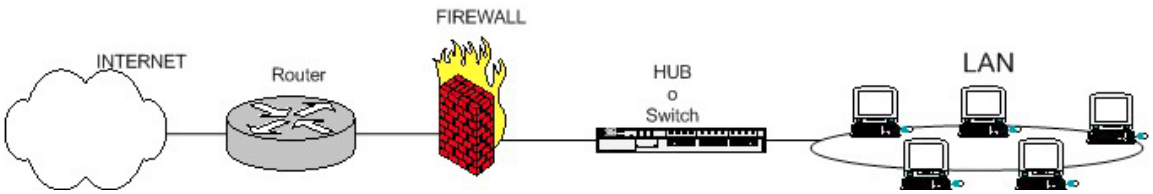
Servidor proxy de aplicación

Cuando un usuario quiere comunicarse con el mundo exterior, el programa cliente envía al usuario primero al servidor proxy.
El servidor proxy establece la comunicación con el servidor que ha solicitado (el mundo exterior) y le devuelve al usuario los datos.
Los servidores proxy de aplicación pueden autenticar a los usuarios.
Antes de establecer una conexión con el exterior, el servidor le puede pedir que se identifique primero. A un usuario de la red le pediría una identificación para cada sitio que visite.

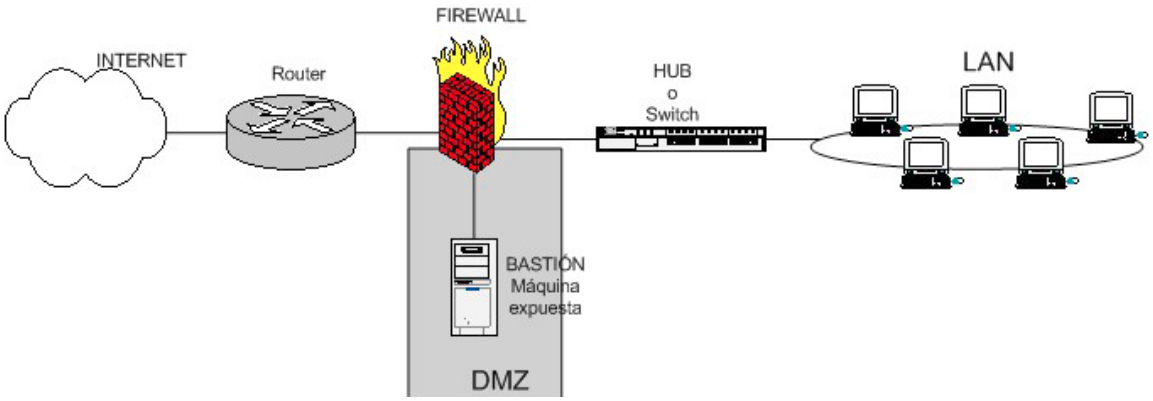
FIREWALL

Un *firewall* es un dispositivo que filtra el tráfico entre redes, como mínimo dos. El *firewall* puede ser un dispositivo físico o un software sobre un sistema operativo. En general debemos verlo como una caja con dos o mas interfaces de red en la que se establecen una reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT.
Esa sería la definición genérica, hoy en día un *firewall* es un hardware especifico con un sistema operativo o IOS que filtra el tráfico TCP/UDP/ICMP/../IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un *firewall* entre redes funcione como tal debe tener al menos dos tarjetas de red.

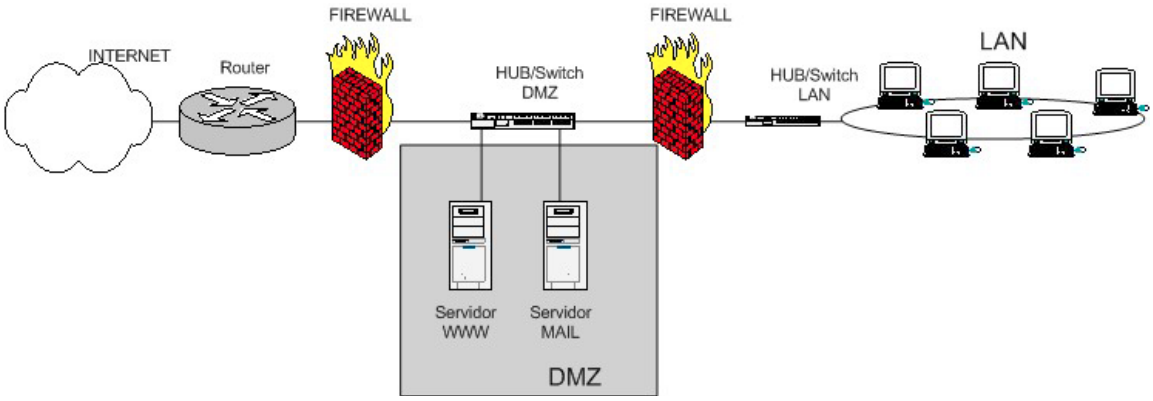
Esquema típico de *firewall* para proteger una red local conectada a Internet a través de un router. El *firewall* debe colocarse entre el router (con un único cable) y la red local (conectado al switch o al hub de la LAN).



Dependiendo de las necesidades de cada red, puede ponerse uno o más *firewalls* para establecer distintos perímetros de seguridad en torno a un sistema. Es frecuente también que se necesite exponer algún servidor a internet (como es el caso de un servidor web, un servidor de correo,etc..), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos. Lo que se recomienda en esa situación es situar ese
servidor en algún lugar aparte de la red, el que denominamos DMZ o zona desmilitarizada. El *firewall* tiene entonces tres entradas:



En la zona desmilitarizada se pueden poner tantos servidores como se necesiten. Con esta arquitectura, permitimos que el servidor sea accesible desde internet de tal forma que si es atacado y se gana acceso a él, la red local sigue protegida por el *firewall*.



-