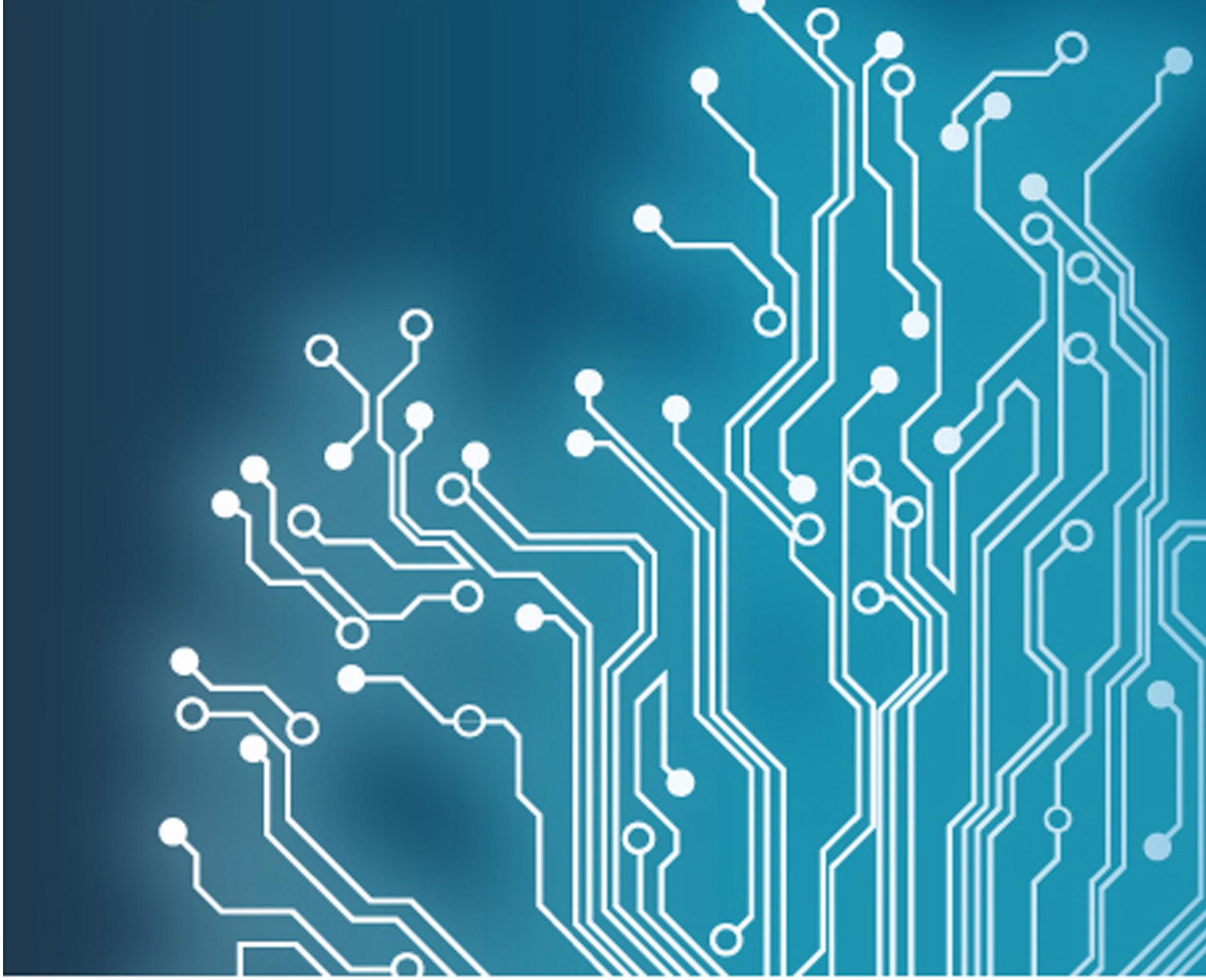


Redes

Transporte de información y telecomunicacion

UMB virtual

Introducción

Este primer módulo del curso Transporte de información y Telecomunicaciones, presenta los principios básicos de las comunicaciones en red, partiendo desde el concepto mismo de qué es comunicación y cuáles son sus elementos básicos para que pueda establecerse la misma. El contenido del módulo está compuesto por los siguientes tópicos o grandes temas: componentes de un proceso de comunicación, visión histórica de las redes, modelos conceptuales en redes de comunicación, tipos de comunicación, topología de redes, tipos de canal, orientación a la conexión, modelos de referencia, y protocolos entre otros.

Elementos básicos de la comunicación.

Cualquier proceso de comunicación está constituido por un EMISOR o TRANSMISOR que envía información, a través de un CANAL de transmisión que es recibido por el RECEPTOR. (Ver figura 0.1). Por lo tanto es posible hablar de comunicación oral, escrita, gestual, etc., donde el canal puede ser el aire, el papel, señales eléctricas, etc.

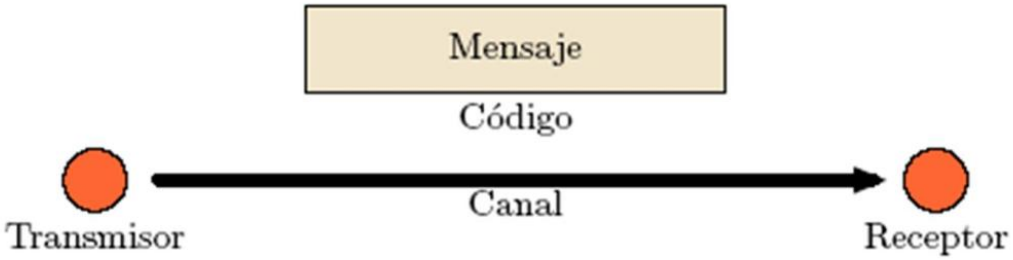


Figura 0.1 Elementos de la comunicación

Llamaremos telecomunicaciones a aquellos sistemas de comunicación que permiten extender el alcance de un mensaje más allá de los medios naturales.

Esta extensión es generalmente en distancia espacial, pero también podemos aplicar los conceptos cuando la comunicación se extiende en el tiempo.

Uno de los objetivos del proceso de comunicación, es que, permite que la información que se desea transmitir sea idéntica a la información recibida.

Visión histórica de las redes de comunicaciones

Los primeros sistemas de comunicación, como el telégrafo, utilizaban un código digital para transmitir la información, el mayor peso de los desarrollos necesarios para dar lugar a estas redes de comunicación se ha dirigido hacia la transmisión de voz e imagen de forma analógica. Con la aparición de los computadores, la situación ha cambiado nuevamente permitiendo que la información sea enviada de forma digital.

Escritura y registros

Según Rossi (2010), el hombre y la mujer han tenido siempre la necesidad de comunicarse, no solo con palabras y gestos, sino, también de manera tal que su mensaje viaje a través del tiempo y el espacio. Antes de la invención de la escritura había otra forma de enviar mensajes no escritos. Las señales de humo podían verse a grandes distancias y el retumbar de los tambores escucharse mucho más lejos que la misma voz sonora humana: pero como a la palabra hablada se las llevaba el viento.

Igualmente en la etapa del hombre primitivo la única forma de transmitir noticias y acontecimientos era la narración oral. Sin embargo, este procedimiento es de una gran inexactitud por lo que pronto les obligó a buscar un método más seguro y duradero.

De esta forma aparecieron las pinturas en las cavernas, las pinturas rupestres en los abrigos de las montañas,... que muestran el poder imaginativo de estos hombres. Estos dibujos reciben el nombre de "petrogramas" si están dibujados o pintados en las paredes o rocas, o "petroglifos" si están tallados o grabados. Normalmente representan hombres y animales en distintas posiciones. (Rossi 2010).

Por otra parte Rossi, 2010, afirma que "en muchos casos es muy difícil averiguar la intención o el impulso que movió al hombre a dibujar o grabar una imagen, dicho impulso podía haber sido mágico, religioso, estético, comunicativo,... etc. Además de no

conocer ciertamente el impulso que las promueve, tampoco se pueden constituir como escritura puesto que no forman parte de un sistema convencional de signos".

Lo que sí podemos afirmar de la pintura, es su importancia como precedente de la escritura, ya que la escritura comenzó como imitación de los objetos o seres reales, es decir, la pintura se encuentra en la raíz de toda escritura. Todas las escrituras primitivas modernas (el sumerio, el egipcio, el cretense, el chino, el hitita,...) tuvieron un origen pictórico, ya que sus signos lineales y geométricos no son más que el desarrollo esquemático de las pinturas propiamente dichas. Las imágenes primitivas, ya sean pintadas o grabados, fueron evolucionando a estadios más desarrollados como: el sistema representativo – descriptivo; El sistema de identificación mnemónica o rememorativa; Los sistemas limitados.

Así mismo, la escritura permitió a los seres humanos una comunicación que podía superar las barreras del tiempo y el espacio, de una forma que no dependiera de la memoria del intermediario.

Tomado de http://www.maestrosdelweb.com/editorial/emailhis/ consultado el 11 de enero de 2012.

La escritura no ha sido el único medio de comunicación. Desde que los seres humanos somos seres humanos (*Homo Sapiens*) hemos representado nuestra realidad por métodos pictóricos. La tecnología actual ha permitido ampliar el espectro de los medios de registro. Además de la pintura y la escritura sobre papel, tablillas o rocas; existe la imprenta, la fotografía, los registros de audio y video y los archivos y bases de datos en computador en una gran diversidad de formatos y propósitos. La tecnología ha permitido ampliar el espectro de los medios de registro. Además de la pintura y la escritura sobre papel, tablillas o rocas; existe la imprenta, la fotografía, los registros audio y video y los archivos y bases de datos en computador en una gran diversidad de formatos y propósitos.

Correos

A lo largo de la Historia, las sociedades han evolucionado a través del contacto entre sus miembros. El comercio y la comunicación han sido indispensables en ese proceso. Por ello, la transmisión de noticias entre distintos grupos humanos es tan remota como su

propia historia, siendo el mensajero uno de los personajes más antiguos, cuya labor sigue siendo necesaria aun en la actualidad. (Sosa, 2005).

Aunque su existencia se remonte a un pasado más antiguo, la organización del correo en España se debe a los romanos. El cursus publicus, como se denominaba, recorría toda la geografía de Hispania a través de una cuidada red de caminos portando los mensajes para el ejército o los administradores romanos.

Posteriormente, durante la Edad Media, los numerosos reinos en los que se dividió España, crearon sus propios sistemas de correo. Los mandaderos iban de una corte a otra con los encargos de sus reyes. También los comerciantes o las instituciones religiosas o universitarias tenían sus propios mensajeros. La organización postal en España fue transformándose progresivamente con la unificación de los reinos bajo la monarquía de los Reyes Católicos, con el descubrimiento de América y luego con la ampliación de territorios en Europa durante el reinado de Carlos I.

Más recientemente, las nuevas tecnologías han crecido y se han consolidado en todos los ámbitos, en general, y en el de las comunicaciones, en particular. Correos ha respondido a los nuevos retos incorporando los medios más innovadores a todos los procesos postales, desde los Centros de Tratamiento Automatizados hasta el empleo de terminales informáticos portátiles por su personal de reparto, pasando por el lanzamiento de su oficina postal virtual www.correos.es, desde los servicios postales tradicionales hasta los creados específicamente para el entorno electrónico.

En cuanto al correo electrónico también conocido como e-mail, es un recurso tecnológico que nos permite comunicarnos desde cualquier parte del mundo a través de Internet.

Como todos sabemos, nos encontramos en una era denominada la era de la información, debidoa que con la llegada del Internet y nuevas tecnologías la acción de comunicarnos ya no es tan complicado como lo era antes, ahora contamos con más medios de comunicación masiva que aunados con la tecnología podemos estar informados del acontecer mundial a cada minuto.

Pero como todo, detrás de los grandes resultados, están los primeros pasos y las primeras pruebas que hacen la historia de los inventos e inventores de las grandes tecnologías.

El correo fue creado por Ray Tomlinson en 1971, aunque no lo consideró un invento importante. Su gran difusión promueve servicios para chequear una cuenta POP desde cualquier navegador.

El texto del primer mensaje enviado por e-mail fue algo así como "QWERTYUIOP" (teclas pulsadas al azar en el teclado por razones de pruebas) según su inventor, fue enviado a través de un programa llamado SNDMSG que él escribió. El invento se estaba terminando en 1971 cuando Tomlinson, un ingeniero de la firma Bolt Beranek y Newman, contratada por el gobierno de los Estados Unidos para construir la red Arpanet (la precursora de Internet), tuvo la idea de crear un sistema para enviar y recibir mensajes por la red.

Tomlinson había escrito un programa para que los desarrolladores de la Arpanet se dejaran mensajes en las computadoras que compartían (15 en toda la red nacional). Jugando con otro protocolo para transferir archivos entre las máquinas diseminadas por la red, notó que juntos podían usarse para acceder a todas las casillas de correo.
(eggers, 2002).

¿Cómo surge la arroba?

Tomlinson eligió la arroba, que en inglés se lee "*at* (en tal lugar)", para especificar el destinatario del mensaje: *Fulano en tal lugar*. Acto seguido, se envió un mensaje a sí mismo y dio inicio a la era del e-mail.

Tomlinson, no creyó que su invento fuera a quedar registrado en la historia porque consideraba al e-mail como un paso previsible en la informática, no un invento genial. Actualmente el e-mail es un estándar de comunicación, y las cuentas POP (que permiten pasar mensajes de un servidor a una computadora) su lenguaje común. Se recomienda consultar el siguiente link para ampliar información sobre POP:
http://www.consumer.es/web/es/tecnologia/internet/2005/02/03/116251.php.
Consultado el 6 de enero de 2012.

El uso de cuentas POP requiere de un software para conectarse a un servidor,

subir y descargar mensajes. Los principales programas en el mercado son Eudora, Outlook o Thunderbird.

El otro acceso que se ha popularizado es el del Webmail, que no requiere ningún software especial, sino únicamente un navegador de Internet.
Con el tiempo, el servicio de e-mail es uno de los más competitivos para las grandes empresas como Yahoo, Hotmail y Google, principales servicios que ofrecen cuentas de correo gratuito con muy buenas características en la búsqueda de incrementar su número de usuarios inscritos.
En conclusión, a pesar de que Tomlinson consideró que su invento no era de relevancia histórica, ahora es una gran herramienta de comunicación a nivel mundial

Por último, podemos asegurar entonces, que el concepto del correo en una forma técnica consiste en que si una fuente A desea pasar un mensaje a un receptor B que se encuentra en otra localización geográfica, utiliza un mensajero C el cual se desplaza desde la ubicación de A a la ubicación de B, portando el mensaje.

Este mensaje puede ser oral, o puede ser un registro en cualquiera de las modalidades vistas. El mensajero puede ser una persona, o un sistema de personas y/o de máquinas.

Sistemas de señales (semáforos).

El semáforo o sistema de transmisión y recepción de mensajes de forma manual empleando banderas, es un antiguo método de comunicación visual a corta distancia muy simple, que emplean fundamentalmente las marinas de guerra de diferentes países para comunicarse entre un barco y tierra, entre dos barcos, o entre dos puntos fijos en tierra.
Tomado de http://www.asifunciona.com/tablas/semaforo/semaforo.htm, consultado el 11 de enero de 2012.

Para transmitir los mensajes se utilizan dos banderas cuadradas, de iguales medidas y con los mismos colores (amarillo y rojo), ubicados diagonalmente. Esas banderas corresponden, a su vez, a la letra "O" del Código Internacional de Banderas de Señales Marítimas.

Para representar cada letra, la persona encargada de enviar los mensajes se sitúa de frente al receptor (que también puede actuar como transmisor para contestar los mensajes) y mueve ambas banderas con los brazos describiendo círculos. Por ejemplo las banderas cruzadas abajo indican el inicio y final de cada palabra transmitida.
La forma en que se sitúa la bandera en cada uno de los movimientos que se realizan, corresponden a una letra determinada del alfabeto o a un número.

En primer lugar las señales no tienen gran interés en sí mismas si no es posible transmitirlas y recibirlas. Por lo tanto las señales están muy ligadas a la **comunicación** y su procesamiento es muy importante en la llamada era de la información.

La información no es transmitida tal como la emitimos, sino que es necesario utilizar unos códigos comprensibles por el emisor y receptor, los cuales se comunican a través de señales físicas. Los códigos son el lenguaje utilizado y las señales son las ondas electromagnéticas, sonoras, luminosas, etc. La utilización de códigos y señales precisa que la información sea CODIFICADA en la transmisión y DECODIFICADA en la recepción.

Durante la era napoleónica los códigos visuales fueron refinados a tal punto que podían transmitir de forma completa cualquier tipo de mensaje, utilizando señales realizadas con banderas y apoyados por un telescopio.

Tomado de: http://www.asifunciona.com/tablas/semaforo/semaforo.htm. Consultado el 11 de enero de 2012.

En conclusión, la comunicación oral y visual, tiene una serie de limitaciones en la distancia. El desplazamiento de un mensajero toma tiempo, el cual puede llegar a ser crítico.

Esto ha dado lugar a distintos tipos de comunicaciones a la distancia usando códigos sonoros o visuales. Estos códigos han sido generalmente muy limitados.

Durante la era napoleónica los códigos visuales fueron refinando a tal punto que podían transmitir de forma completa cualquier tipo de mensaje, utilizando señales realizadas con banderas y apoyadas por un telescopio.

Telegrafía y radiotelegrafía.

En un principio, los sistemas telegráficos eran muy rudimentarios, y algunos de ellos todavía perduran en ciertas comunidades primitivas; por ejemplo, algunos pueblos continúan utilizando instrumentos de percusión o de viento, como tambores, trompas, cuernos, etcétera, o bien ópticos, como espejos, señales de humo, banderas, etcétera.

Pero hasta 1793 no aparece la primera red regular para la transmisión de noticias, basada en el telégrafo aéreo, inventado por el francés Chappe, que consiste en el empleo combinado de los gemelos y ciertas señales. En 1805, a raíz de los descubrimientos de Galvani y Volta se idearon sistemas telegráficos basados en la descomposición del agua por la electrólisis, producida por una corriente eléctrica variable enviada por la estación transmisora (telégrafo-electrolítico). En 1820, el físico Oersted introdujo el electromagnetismo, y en el 1833 los físicos Weber y Gauss realizaron los primeros ensayos de lo que sería el telégrafo electromagnético, basado en la acción de la corriente eléctrica sobre una aguja magnética. (Davila, J 2008).

Los telégrafos eléctricos construidos desde entonces se clasifican en dos grupos generales: Indicadores y escritores. Los primeros se basan en el prototipo creado por Bréguet, pero han sido desplazados por los segundos, iniciados por el modelo de Morse, entre 1832 y 1837.

El telégrafo experimentó en poco tiempo un considerable desarrollo, por lo que hubo que recurrir a la telegrafía automática con el fin de aumentar la capacidad de transmisión. La firma Siemens mejoró el sistema de perforación ideando un aparato con teclado, de tal manera que al pulsar una tecla se imprimen en código Morse, las perforaciones de una letra determinada; se transmiten directamente a la línea las señales, o ambas cosas a la vez.

Existieron también otros sistemas telegráficos que tuvieron una gran importancia durante el tiempo que se practicaron, los de contenidos ópticos semafóricos, así

teníamos, el telégrafo óptico de las costas, para comunicarse con los buques por medio de señales. Semáforos, banderas, persianas, etc. Esta forma de comunicarse al igual que la del heliógrafo, sistema este que utilizaba la refracción de los rayos solares sobre una pantalla generalmente circular y los convertía en señales mediante la acción de un conmutador, eran utilizados casi exclusivamente por los buques de guerra.
(Erausquin, 2009).

Ya hemos visto cómo sucesivos descubrimientos científicos lograron disminuir la cantidad de hilos empleados en las líneas telegráficas, hasta reducirlos a uno solo, y también cómo, después de obtener de esa línea de un hilo único el rendimiento máximo con los sistemas de transmisión múltiple, se llegó a la deducción lógica que con el tiempo también desaparecería este elemento como conductor de la telegrafía.

Uno de los precursores fué el español Salva, quien a comienzos del siglo XIX, tuvo la intuición de que era posible enviar despachos telegráficos sin utilizar **hilo metálico** alguno, sirviéndose para ello del agua del mar.

Por otra parte, Branly, físico francés, inventor del cohesor; Hertz, descubridor de las ondas eléctricas que llevan su nombre y de la manera de producirlas y anunciar su presencia; Lodge, físico inglés que en 1894, después de muchos experimentos, pudo demostrar que era posible utilizar las ondas para señales, y muchos otros hombres de ciencia hicieron factible, con sus descubrimientos, llegar a la maravillosa invención de la telegrafía inalámbrica, gracias a la cual se salvaron miles de vidas y se lograron incalculables beneficios y progresos materiales en brevísimo tiempo. (Erausquin, 2009).

Pero no fue por medio de las corrientes del mar, ni de las olas, sino de las ondas eléctricas, como pudo Marconi llegar a la portentosa realización de las comunicaciones radio- eléctricas. La electricidad permitió la comunicación entre puntos distantes sin línea de vista. Manipulando las señales eléctricas nace la telegrafía.

Con el descubrimiento de la transmisión inalámbrica de electricidad, que hoy conocemos como radiación electromagnética (o radio), surge la telegrafía sin hilos.

Las señales eléctricas, y de forma similar las señales electromagnéticas, pueden ser manipuladas de formas diversas, más allá de abrir y cerrar circuitos, propios de la telegrafía. La señal eléctrica puede ser modulada para llevar mensajes de voz y este es el principio de la telefonía y de la transmisión de voz por radio.

Radiodifusión

La aparición de la radio no se produce de forma directa. Su invento, desde un punto de vista tecnológico, no se puede atribuir a una sola persona, sino que es consecuencia de varias aportaciones a lo largo del tiempo. Desde un punto de vista social, el uso que se le da más tarde a la radio no es el mismo que en sus orígenes.

La transmisión de voz por radio ha permitido múltiples aplicaciones. Muchas de ellas son básicamente una extensión de la telegrafía: enviar un mensaje entre dos puntos.

El antecedente de la radiodifusión es un dispositivo técnico llamado radioteléfono. Se conoce desde 1901 que se caracteriza por ser una telegrafía sin hilos pero de carácter individual. A partir de 1920, los términos de radioteléfono y radiodifusión van a estar totalmente definidos: El primero se refiere a un uso individual; el segundo, a uno colectivo.

Una aplicación que se desarrolló con la radio ha sido la radiodifusión: Una persona produce y programa contenidos que son recibidos por un amplio público, el cual posee los receptores adecuados. Este es también el principio de la televisión pública.

La telefonía pública conmutada.

El servicio de Telefonía Pública Básica Conmutada Local (TPBCL) es de los más antiguos del sector de telecomunicaciones en Colombia, inicia su prestación hacia finales del siglo XIX, donde eran las empresas privadas las que lideraban el sector en las nacientes ciudades de Bogotá, Barranquilla y Cúcuta. (Tomado de la tesis de licenciatura de Montoya (2008); "Análisis descriptivo de los mecanismos de regulación económica de la telefonía pública básica conmutada local en Colombia entre los año 1990 a 2008". Consultado el 24 de octubre de 2011.

En Cali se inició la prestación del servicio hacia 1912 con la "Empresa de Teléfonos de Cali", fecha por la que operaban 12 empresas a nivel municipal en Colombia, la mayoría de ellas de carácter privado. (Arenas, 2008).

Entrada la mitad del siglo XX y como consecuencia de la expansión gracias a la alta demanda, llevaron a que dichas empresas de capitales privados fueran municipalizadas para poder enfrentar las necesidades de capital. Hacia 1940 se municipaliza la empresa de teléfonos de Bogotá, cuatro años después la de Cali, hecho que sucedió con la mayoría de empresas de las capitales del país.

Hacia 1947 se crea la Empresa Nacional de Telecomunicaciones (TELECOM), la cual integró los servicios de larga distancia, telegráficos y telefónicos en ciertas regiones del país. (Arenas 2008).

Desde esta época el modo estatal monopólico nacional y municipal fue el que operó en el país. Pero este modo de prestación generó distorsiones en los mercados, las tarifas de telefonía local estaban por debajo de los costos de prestación del servicio y del promedio internacional, y las de larga distancia eran muy superiores a las del promedio internacional. (Arenas, 2008).

El cambio que se presentó con la entrada de la competencia y de capitales privados en el mercado de telefonía local y de larga distancia, fue enmarcado bajo la ley 142 de 1994, llamada la Ley de Servicios Públicos Domiciliarios, pasando de 26 empresas de telefonía local en 1993, a 41 en 2002.

En este sentido, la red de TPBCL, ha tenido a lo largo de su existencia diversos cambios institucionales y orgánicos, pero no han sido ajenos los tecnológicos, como por ejemplo, cuando las antiguas redes de conmutación eran manuales y sólo se utilizaban pares de cobre para transmitir voz, y cuando eran personas llamadas “operadoras”, quienes conmutaban las llamadas de los usuarios.

Con el transcurrir de los años se pasó a conmutadores electromecánicos que remplazaron a las operadoras y estos conmutadores a su vez, fueron remplazados por conmutadores electrónicos, analógicos y después digitales, para finalmente llegar a la tecnología basada sobre el protocolo IP, la cual es la utilizada ampliamente en la actualidad soportada con conmutadores IP.

Dicha tecnología permite transportar voz, a manera de paquetes de datos, a través de una red de Internet. Cabe resaltar que el protocolo IP no es un servicio, es un protocolo, que permite la comunicación de dos o más personas y disfrutar de nuevas funcionalidades en la telefonía.

Por lo tanto, y por políticas de la CRT, en Colombia la regulación se realiza por servicios y mercados. Y para la prestación de estos servicios, se debe de obtener licencia por medio de la cual se autoriza la prestación de determinado tipo de servicio. Tomado de Colombia CRT "Cual es la regulación vigente para prestar servicios VoiP (1992).

Aunque los cambios tecnológicos y estructurales del mercado del servicio de TPBCL han sido muchos a lo largo de los años, en Colombia se continua manteniendo en el tiempo las funciones esenciales de una red fija de telecomunicaciones: acceso, conmutación, y transmisión, así como también se mantiene su estructura de costos, más

no sus niveles, lo que hace que el servicio posea ciertas características económicas que pueden aprovechar las empresas, como la presencia de economías de escala, alcance y densidad, logrando disfrutar de los rendimientos crecientes a escala, dependiendo de la parte de la red en cuestión.

Por otra parte permite aprovechar los efectos externos positivos de red, cuando los usuarios incrementan su utilidad en el momento que más usuarios se suman a la red así como también aprovechar la conceptualización del servicio en el sentido de "servicio universal" llegando a la mayor cantidad de hogares posible.

Los cargos de acceso e interconexión son fundamentales para el desarrollo competitivo del sector, puesto que se trata de generar un bienestar general al reducir las externalidades negativas que se puedan presentar, así como también ineficiencias productivas o asignativas en la prestación del servicio de TPBCL.
(Telefonía Pública Básica Conmutada Local).

La transmisión punto a punto requiere de una "línea de transmisión" entre los dos nodos que intervienen en la misma. Cuando se quiere lograr una comunicación punto a punto entre dos nodos, se debe proveer de las líneas suficientes para cualquier tipo de comunicación. Cuando se conectan más de dos nodos se tiene una red.

Radioaficionados y banda civil

Existen muchos más esquemas bajo los cuales puede funcionar un sistema de telecomunicación.

Además de los esquemas vistos, se pueden incluir los servicios de radio afición y banda civil. Estos servicios se basan en que cada usuario posee su propio sistema de comunicación con el cual tiene acceso a un medio compartido y público.

En el año en que nació la actividad de los radioaficionados fue posiblemente en 1907, en el cual la revista: "Electrician & Mechanic Magazine", inicia con el título "Como se hace", la descripción de los componentes y aparatos para las comunicaciones TSF (Telecomunicaciones Sin Frontera), de débil potencia, explicando todos los detalles para la autoconstrucción.

Estos artículos escritos por radioaficionados, divulgan con todo detalle sus experiencias y sus resultados. Tales escritos se diferencian de los experimentadores profesionales divulgando el concepto según el cual el aficionado se dedica a los estudios técnicos sin ningún provecho económico.

Hasta el año 1908 es difícil distinguir entre los experimentadores por motivos profesionales, comerciales y los aficionados verdaderos o bandas civiles.

Hoy en día están apareciendo diferentes modalidades digitales con la fusión de la radio y el mundo de la computación. El Sistema de Posicionamiento Satelital (GPS), e Internet, de tal forma que tenemos ya comunicación a cualquier hora del día, cualquier día de la semana, de cualquier mes y año y cada vez mayor cantidad de ciudades en el mundo, a través de Radio-Internet Radio o el seguimiento de móviles en mapas satelitales con el sistema APRS (Automatic Position Reporter System) que utiliza la Radio, el GPS y la Internet.

Modelos conceptuales en redes de comunicaciones

Conceptos básicos de redes

Aquí definiremos algunos de los conceptos que se continuarán desarrollando en el presente curso, y que permiten describir a los sistemas de comunicación. Estos conceptos incluyen los tipos de comunicación, Topología de red, orientación a conexión, y confiabilidad.

Tipos de comunicación entre nodos

Punto a punto

En la comunicación punto a punto hay sólo dos nodos. Todo lo que transmite uno, es recibido por el otro, tal como lo muestra la figura 2.1.

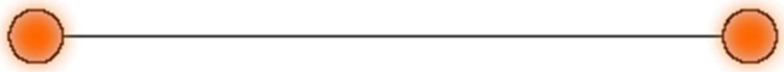


Figura 2.1: Comunicación punto a punto

Por Ejemplo telefonía tradicional entre abonados.

Punto-multipunto

En la comunicación punto-multipunto hay un nodo central y varios nodos periféricos. Todo lo que transmite el nodo central es recibido por todos los nodos periféricos. Todo lo que transmiten los nodos periféricos es recibido sólo por el nodo central. La topología lógica se ve en la figura 2.2

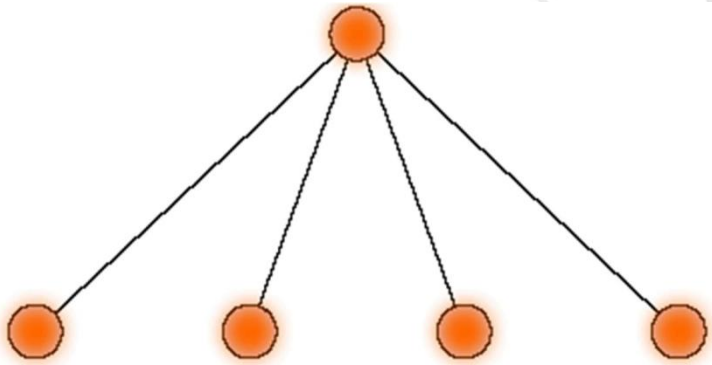


Figura 2.2: Comunicación punto-multipunto

Por ejemplo servidor de base de datos.

Medios compartidos

En la comunicación por medio compartido hay más de dos nodos y lo que transmite un nodo cualquiera es recibido por todos los demás, tal como lo muestra la figura 2.3

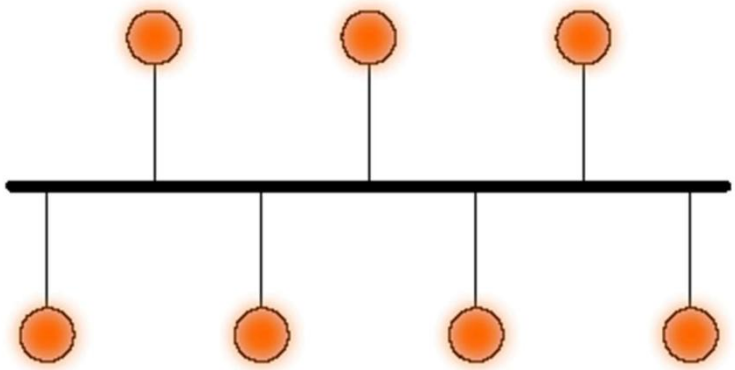


Figura 2.3: Comunicación por medio compartido

Por ejemplo sala de conversación.

Emisión o difusión

La comunicación por emisión o difusión (*Broadcast* en inglés), es un sistema punto-multipunto sin retorno, y sobre la cual el nodo central no tiene control sobre los nodos periféricos, tal como lo muestra la figura 2.4.

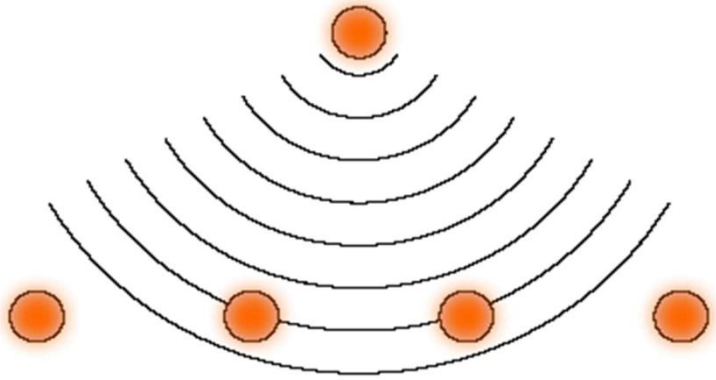


Figura 2.4: Comunicación por difusión

Por ejemplo radiodifusión.

Red

Siempre que existan dos o más nodos interconectados existe una red. En una red compleja algunos nodos sirven de tránsito para un mensaje que va de un nodo final a otro.

Por ejemplo red de telefonía pública conmutada (RTPC).

Topologías de red

Las topologías de red hacen referencia a la forma como se realizan las conexiones entre nodos.

Topología de malla completa

En la topología de malla completa (mesh en inglés), cada nodo está comunicado con todos los demás nodos, tal como lo muestra la figura 2.5.

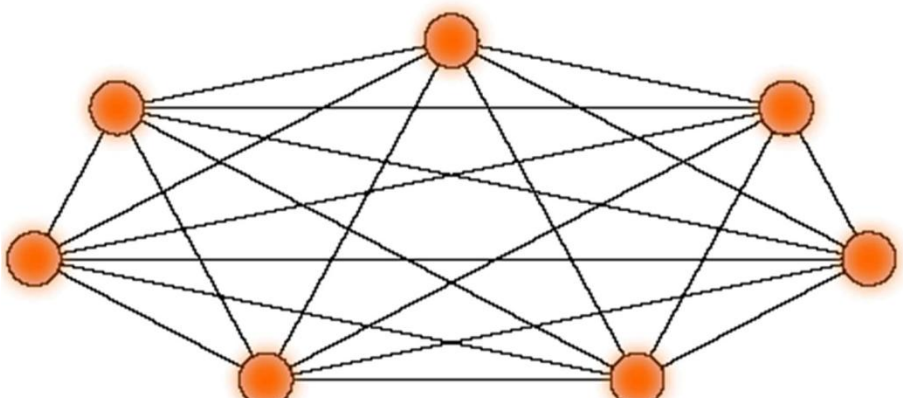


Figura 2.5: Topología de malla completa

Dados n nodos, una topología de malla completa requiere n(n-1)/2 enlaces. El número de enlaces crece así de forma cuadrática respecto al número de nodos, como lo muestra la tabla 2.1.

Adicionalmente, en una topología de malla completa cada nodo debe poder soportar tantos enlaces como nodos diferentes haya en la red. La comunicación entre nodos finales se realiza sobre un solo enlace.

nodos	enlaces	nodos	enlaces
2	1	3	3
4	6	5	10
6	15	7	21
⋮	⋮	⋮	⋮
10	45	20	190
100	4.950	200	19.900
1.000	499.500	10.000	49'995.000

Punto de vista matemático: En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos.

Punto de vista físico: Este tipo de cableado tiene ventajas y desventajas muy específicas. Una de las ventajas es que cada nodo está físicamente conectado a todos los demás nodos (lo cual crea una conexión redundante). Si fallara cualquier enlace, la información podrá fluir a través de una gran cantidad de enlaces alternativos para

llegar a su destino. Además, esta topología permite que la información circule por varias rutas al regresar por la red. La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces y la cantidad de conexiones con los enlaces se torna abrumadora.

Punto de vista lógico: El comportamiento de una topología de malla completa depende enormemente de los dispositivos utilizados.

Topología de estrella

En la topología de estrella, existe un nodo central y todos los demás nodos se conectan a éste, tal como lo muestra la figura 2.6.

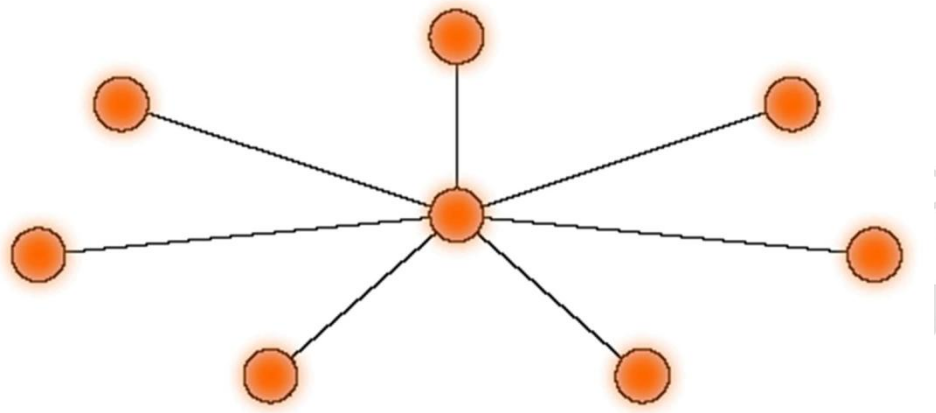


Figura 2.6: Topología de estrella

El nodo central puede ser de la misma categoría que los demás nodos, o puede ser un nodo de tránsito. El nodo central debe poder soportar tantos enlaces como nodos periféricos existen. La comunicación entre nodos periféricos finales pasa sobre el nodo central y dos enlaces.

Punto de vista matemático: La topología en estrella tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos y no permite otros enlaces.

Punto de vista físico: La topología en estrella tiene un nodo central desde el que se irradian todos los enlaces. La ventaja principal es que permite que todos los demás nodos se comuniquen entre sí de manera conveniente. La desventaja principal

es que si el nodo central falla, toda la red se desconecta. Según el tipo de dispositivo para networking que se use en el centro de la red en estrella, las colisiones pueden representar un problema.

Punto de vista lógico: El flujo de toda la información pasaría entonces a través de un solo dispositivo. Esto podría ser aceptable por razones de seguridad o de acceso restringido, pero toda la red estaría expuesta a tener problemas si falla el nodo central de la estrella.

Topología de estrella extendida

Cuando la complejidad de la red aumenta, una solución consiste en tener estrellas pequeñas uniendo un número manejable de nodos, y unir los nodos centrales de cada una de las estrellas en un nodo central de mayor jerarquía, tal como lo muestra la figura 2.7. Este proceso puede iterarse.

En el primer nivel de iteración (estrella extendida de dos niveles), la comunicación entre dos nodos periféricos finales puede necesitar pasar por tres nodos intermedios y cuatro enlaces. Si se hace una estrella extendida de tres niveles, la comunicación podrá requerir de cinco nodos intermedios y seis enlaces.

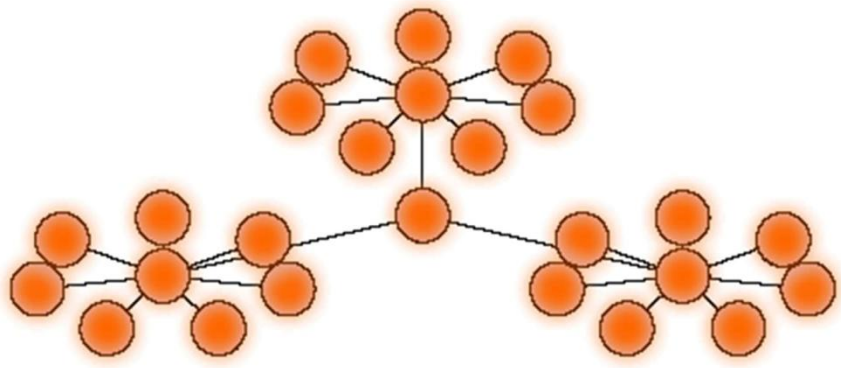


Figura 2.7: Topología de estrella extendida

Punto de vista matemático: La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella.

Punto de vista físico: La topología en estrella extendida tiene una topología en estrella central, en la que cada uno de los nodos finales actúa como el centro de su propia topología en estrella. La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central.

Punto de vista lógico: La topología en estrella extendida es sumamente jerárquica, y "busca" que la información se mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico.

Topología de anillo

En la topología de anillo, cada nodo se conecta a un nodo anterior y a un nodo siguiente, como lo muestra la figura 2.8. Cuando un mensaje se transmite entre nodos no consecutivos, este pasa por todos los nodos intermedios. Esto implica que todos los nodos son a la vez nodos finales y nodos intermedios.

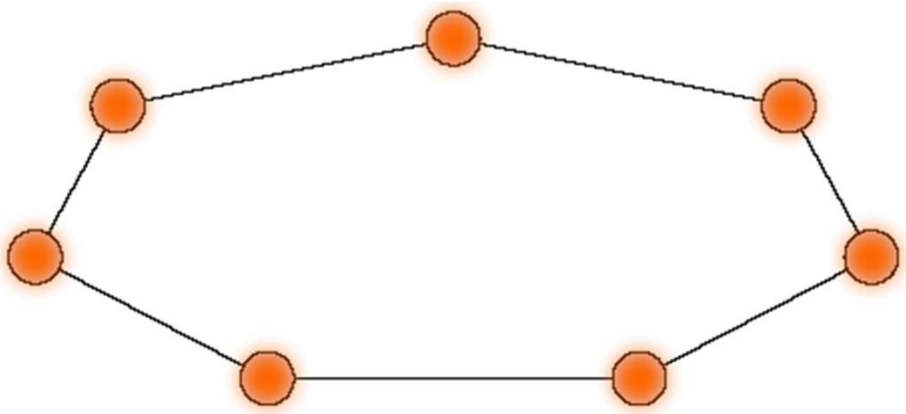


Figura 2.8: Topología de anillo

Usualmente el anillo tiene un solo sentido. Una variación es el anillo doble en el cual cada nodo tiene enlaces de ida y de venida con los dos nodos adyacentes.

Anillo simple: punto de vista matemático: Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado con sólo dos nodos adyacentes.

Anillo simple: punto de vista físico: La topología muestra todos los dispositivos interconectados directamente en una configuración conocida como cadena margarita. Esto se parece a la manera en que el mouse de un computador Apple se conecta al teclado y luego al computador.

Anillo simple: punto de vista lógico: Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

Anillo doble: punto de vista matemático: Una topología en anillo doble consta de dos anillos concéntricos, cada uno de los cuales se conecta solamente con el anillo vecino adyacente. Los dos anillos no están conectados.

Anillo doble: punto de vista físico: La topología de anillo doble es igual a la topología de anillo, con la diferencia de que hay un segundo anillo redundante que conecta los mismos dispositivos. En otras palabras, para incrementar la confiabilidad y flexibilidad de la red, cada dispositivo de networking forma parte de dos topologías de anillo independiente.

Anillo doble: punto de vista lógico: La topología de anillo doble actúa como si fueran dos anillos independientes, de los cuales se usa solamente uno por vez.

Topología de bus

En la topología de bus, existe un solo medio de comunicación común para todos los nodos, como lo muestra la figura 2.9. Ya que todos los nodos pueden acceder al mismo medio, se requiere un método para evitar las colisiones (interferencia presentada cuando dos o más nodos intentan utilizar el medio al mismo tiempo).

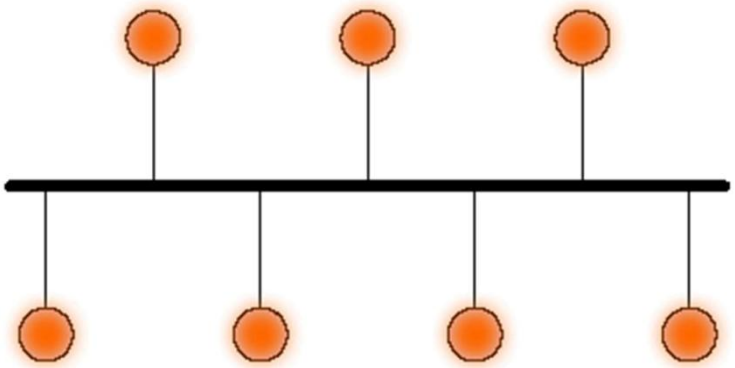


Figura 2.9: Topología de bus

Punto de vista matemático: La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos.

Punto de vista físico: Cada host está conectado a un cable común. En esta topología, los dispositivos clave son aquellos que permiten que el host se "una" o se "conecte" al único medio compartido. Una de las ventajas de esta topología es que todos los hosts están conectados entre sí y, de ese modo, se pueden comunicar directamente. Una desventaja de esta topología es que la ruptura del cable hace que los hosts queden desconectados.

Punto de vista lógico: Una topología de bus hace posible que todos los dispositivos de la red vean todas las señales de todos los demás dispositivos. Esto representa una ventaja si desea que toda la información se dirija a todos los dispositivos. Sin embargo, puede representar una desventaja ya que es común que se produzcan problemas de tráfico y colisiones.

Topologías mixtas o irregulares

También conocidas como topologías de malla incompleta, se presentan cuando la red no puede clasificarse de ninguna de las formas anteriores.

Punto de vista matemático: En la topología de red irregular no existe un patrón obvio de enlaces y nodos.

Punto de vista físico: El cableado no sigue un patrón; de los nodos salen cantidades variables de cables. Las redes que se encuentran en las primeras etapas de construcción, o se encuentran mal planificadas, a menudo se conectan de esta manera.

Punto de vista lógico: Los enlaces y nodos no forman ningún patrón evidente.

Topología de red celular

Punto de vista matemático: La topología celular está compuesta por áreas circulares o hexagonales, cada una de las cuales tiene un nodo individual en el centro.

Punto de vista físico: La topología celular es un área geográfica dividida en regiones (celdas) para los fines de la tecnología inalámbrica - una tecnología que se torna más importante cada día. En la topología celular, no hay enlaces físicos, sólo ondas electromagnéticas. A veces los nodos receptores se desplazan (por ejemplo teléfono celular de un automóvil) y a veces se desplazan los nodos emisores (por ejemplo enlaces de comunicaciones satelitales). La ventaja obvia de una topología celular (inalámbrica) es que no existe ningún medio tangible aparte de la atmósfera terrestre o el del vacío del espacio exterior (y los satélites). Las desventajas son que las señales se encuentran presentes en cualquier lugar de la celda y, de ese modo, pueden sufrir disturbios (provocados por el hombre o por el medio ambiente) y violaciones de seguridad (monitoreo electrónico y robo de servicio).

Punto de vista lógico: Las tecnologías celulares se pueden comunicar entre sí directamente (aunque los límites de distancia y la interferencia a veces hacen que esto sea sumamente difícil), o se pueden comunicar solamente con las celdas adyacentes (lo que es sumamente ineficiente). Como norma, las topologías basadas en celdas se integran con otras topologías, ya sea que usen la atmósfera o los satélites.

Tipos de canal

Cada canal, por ejemplo el enlace entre dos nodos, está diseñado para comunicar un transmisor y un receptor (ver figura 2.10).

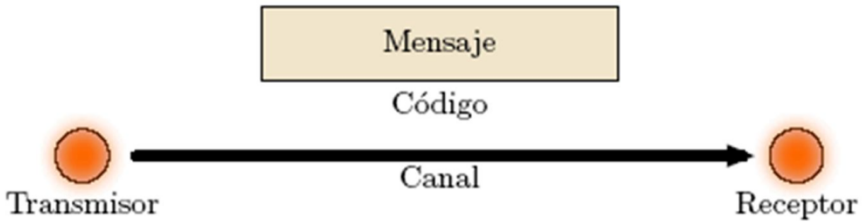


Figura 2.10: Canal en comunicaciones

El canal puede ser en un solo sentido (el transmisor siempre transmite y el receptor sólo recibe), o en dos sentidos (el canal permite que ambos extremos puedan recibir y transmitir). De acuerdo con esta característica los canales se clasifican en símplex o dúplex.

Símplex: Permite la comunicación en una sola vía. El transmisor es sólo transmisor y el receptor es sólo receptor. Por ejemplo radiodifusión.

Semidúplex: También conocido en inglés como *half duplex*, permite la comunicación en dos sentidos, pero sólo un sentido a la vez. Los roles del transmisor y el receptor se turna. Por ejemplo comunicación a través de AVANTEL.

Dúplex completo: También conocido en inglés como *full duplex*, permite la comunicación en dos sentidos simultáneamente. Ambos nodos son transmisores y receptores al mismo tiempo. Por ejemplo telefonía tradicional.

Orientación a conexión

Orientado a conexión: En este tipo de enlace se debe realizar primero una conexión antes de trasmitir o intercambiar información. Al término de la sesión la conexión se cierra. Por ejemplo telefonía tradicional.

No orientado a conexión: En este tipo de enlace la línea está abierta para la transmisión o intercambio de información. Es responsabilidad del receptor estar listo para recibir el mensaje. Por ejemplo televisión, coctel.

Confiabilidad

La confiabilidad (*reliability*) es un factor de calidad de una conexión. En el uso más simple del término implica si existen o no acuses de recibo de los mensajes o sus partes.

Confirmaciones: Las confirmaciones o acuses de recibo son enviadas por el receptor para indicar al transmisor que un mensaje ha sido recibido satisfactoriamente o no.

Secuenciación: Cuando un mensaje es enviado en varias partes (*fraccionamiento*), la secuencia es un número que indica el orden en el que el mensaje debe ser recompuesto.

Códigos de control: Los códigos de control son números que se obtienen por fórmulas matemáticas aplicadas al mensaje. Contrastando el código calculado por el receptor y el código recibido con el mensaje se puede establecer si el mensaje llegó correctamente.

Modelo conceptual por capas OSI

El modelo OSI (*Open System Interconection*) es un modelo conceptual jerárquico que permite describir los elementos que conforman una red de transmisión de datos.

El modelo OSI está compuesto por capas, cada una de ellas cumple una función específica.

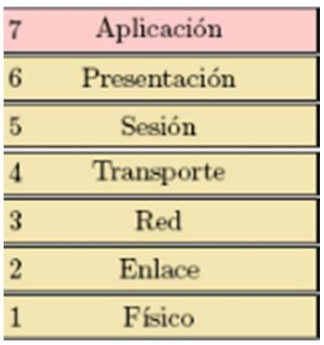
La comunicación entre nodos se realiza siempre en la misma capa. Por ejemplo, un navegador de web y un servidor se comunican en capa 7 (aplicación); un computador con un enrutador se comunican en capa 3 (red), etc.

Los siguientes criterios se tuvieron en cuenta al definir el modelo conceptual por capas OSI:

1. Debería crearse una capa cuando se necesite un nivel de abstracción distinto.
2. Cada capa debería realizar una función bien definida.
3. La función de cada capa debería escogerse pensando en la definición de protocolos estandarizados internacionalmente.
4. Los límites entre capas deberían escogerse para minimizar el flujo de información entre las interfaces.
5. El número de capas debería ser suficientemente grande para que funciones distintas no se agrupen en la misma capa, y suficientemente pequeño para que la arquitectura sea útil y manejable.

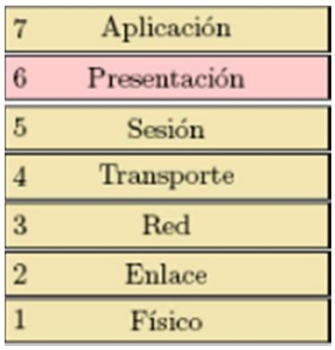
La forma como la Organización de Normas Internacionales ISO desarrolló este concepto no es perfecto y, de por sí, está lleno de fallas que se evidenciarán cuando se compare el modelo OSI con el modelo por capas TCP/IP. Sin embargo el modelo se sigue utilizando para describir los sistemas de red y es importante su comprensión.

Capa 7: Aplicación



En el contexto del modelo de referencia OSI, la capa de aplicación (Capa 7) brinda soporta al componente de comunicación de una aplicación. No proporciona servicios a ninguna otra capa del modelo OSI. Por otra parte, sí brinda servicios a los procesos de aplicación que no se encuentran cubiertos por el modelo OSI (por ej., programas de hoja de cálculo, Telnet, WWW, etc.). La capa de aplicación (*Application Layer* en inglés) define los protocolos que sirven de interfaz a las aplicaciones de usuario con la red. Por ejemplo HTTP, FTP, SMPT, POP3, Telnet, SNMP, DNS, etc.

Capa 6: Presentación}



La capa de presentación (*Presentation Layer* en inglés) es responsable por la presentación de datos en un formato que un dispositivo receptor pueda comprender. Provee servicios de codificación y transformación de datos entre la aplicación y la red.

La capa de presentación no sólo se ocupa del formato y representación de los datos, sino también de la estructura de los datos que usan los programas. La Capa 6 organiza los datos para la Capa 7.

Para comprender cómo funciona esto, supongamos que hay dos sistemas. Un sistema usa **EBCDIC**, y el otro usa **ASCII** para representar los datos. Cuando los dos sistemas necesitan comunicarse, la Capa 6 convierte y traduce los dos formatos diferentes.

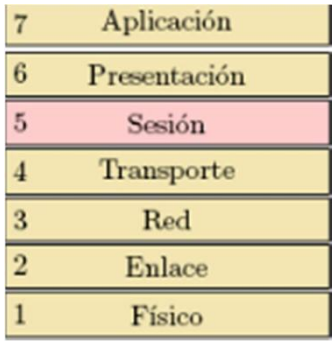
Otro ejemplo muy común se presenta cuando se intercambian archivos de texto entre sistemas MS Windows y Unix/Linux. Aun cuando ambos sistemas usan ASCII, la diferencia entre el formato de salto de línea puede producir resultados inesperados si no se corrige la diferencia durante la transmisión. Los tres elementos principales de la capa de presentación son el de formato de datos, encripción y compresión.

Formato de datos: Los formatos de datos incluye los sistemas de codificación de texto (ascii, Unicode, ...), de gráficos (jpeg, png, ...), de sonido (au, MP3, ...), etc.

Encripción: La encripción consiste en alterar la codificación de un mensaje por medio de una clave, de tal forma que en ausencia de la clave de desencripción el mensaje no sea reconocible. En IPSec, la encripción se realiza en capa 3.

Comprensión: La comprensión consiste en remplazar patrones redundantes de un mensaje por secuencias de menor tamaño.

Capa 5: Sesión



La capa de sesión (*Session Layer* en inglés) se encarga de mantener un canal lógico abierto entre dos puntos para el intercambio de información, incluyendo características como la autenticación, contraseñas, monitorización e información de la red. La capa de sesión establece, administra y termina las sesiones entre aplicaciones. Coordina las peticiones de servicio y las respuestas que se producen cuando las aplicaciones establecen comunicaciones entre hosts diferentes.

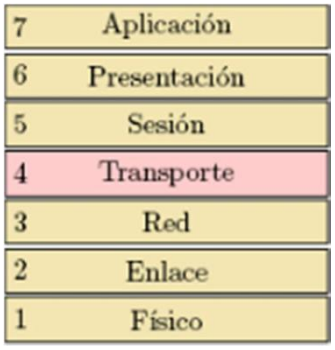
La capa de sesión tiene la responsabilidad de asegurar la entrega correcta de la información a la siguiente capa (capa de presentación). Esta capa tiene que revisar que la información que recibe sea correcta. Para esto la capa de sesión debe realizar algunas funciones:

1. Detección y corrección de errores.

2. Controlar los diálogos entre dos entidades que se estén comunicando, y definir los mecanismos para hacer las Llamadas a Procedimientos Remotos RPC.

La capa de sesión permite a los usuarios de máquinas diferentes establecer sesiones entre ellos. Una sesión permite el transporte ordinario de datos, como lo hace la capa de transporte, pero también proporciona servicios mejorados que son útiles en algunas aplicaciones. Se podría usar una sesión para que el usuario se conecte a un sistema remoto de tiempo compartido o para transferir un archivo entre dos máquinas.
Algunos protocolos de capa 5 incluyen NetBIOS, RPC y SSL.

Capa 4: Transporte



La capa de transporte (*Transportation Layer* en inglés) se encarga de la transferencia confiable entre nodos finales, permitiendo múltiples conexiones entre nodos de forma confiable y precisa. Sus funciones incluyen:

- Sincronización de conexión
- Control de flujo
- Recuperación de errores
- Confiabilidad a través del uso de ventanas

Las unidades de información relevantes a la capa de transporte son los segmentos (segments) o los datagramas. Algunos protocolos de capa 4 incluyen TCP, UDP y SPX.

Para muchas de las explicaciones tomaremos como ejemplo TCP:

La capa de transporte permite que un dispositivo de usuario divida en segmentos varias aplicaciones de capa superior para colocarlas en la misma corriente de datos de Capa 4, y permite que un dispositivo receptor pueda recomponer los segmentos de las aplicaciones de las capas superiores. La corriente de datos de Capa 4 es una conexión lógica entre los extremos de una red, y brinda servicios de transporte desde un host hasta un destino. Este servicio a veces se denomina servicio de extremo a extremo.

A medida que la capa de transporte envía sus segmentos de datos, también garantiza la integridad de los datos. Este transporte es una relación orientada a conexión entre sistemas finales que se comunican. Algunas de las razones por las cuales se debe lograr el transporte confiable son:

- Garantizar que los emisores reciban el acuse de recibo de los segmentos entregados.
- Realizar la retransmisión de cualquier segmento que no genere acuse de recibo.
- Volver a colocar los segmentos en su secuencia correcta en el dispositivo destino.
- Evitar y controlar la congestión.

Uno de los problemas que se pueden producir durante el transporte de datos es el desbordamiento de los búferes en los dispositivos receptores. Los desbordamientos pueden producir serios problemas que tienen como resultado la pérdida de datos. La capa de transporte usa un método denominado control de flujo para resolver este problema.

Funciones de la capa de transporte

Cada una de las capas de nivel superior ejecuta sus propias funciones. Sin embargo, sus funciones dependen de los servicios de las capas inferiores. Las cuatro capas superiores (de aplicación (Capa 7), presentación (Capa 6), sesión (Capa 5) y transporte (Capa 4)) pueden encapsular datos en segmentos extremos a extremo.

La capa de transporte da por sentado que puede usar la red como una nube para enviar paquetes de datos desde el origen al destino. Si examina las operaciones que tienen lugar dentro de la nube, se puede ver que una de las funciones involucra la selección de los mejores recorridos para una ruta determinada. Se empieza a ver el papel que desempeñan los routers en este proceso.

Segmentación de las aplicaciones de capa superior: Una de las razones para utilizar un modelo de múltiples capas como el modelo de referencia OSI es que múltiples aplicaciones pueden compartir la misma conexión de transporte. La funcionalidad de transporte se logra segmento por segmento. Esto significa que diferentes segmentos de datos de diferentes aplicaciones que se envían al mismo destino o a varios destinos diferentes se envían según un método "el que llega primero, es atendido primero".

Para comprender cómo funciona esto, supongamos que se envía un mensaje de correo electrónico y se transfiere un archivo (FTP) a otro dispositivo en una red. Al enviar el mensaje de correo electrónico, antes de que comience la transmisión en sí, el software en el dispositivo establece el número de puerto SMTP (correo electrónico) y el número de puerto del programa origen. A medida que cada aplicación envía un segmento de corriente de datos, utiliza el número de puerto definido previamente. Cuando el dispositivo destino recibe la corriente de datos, separa y clasifica los segmentos de manera tal que la capa de transporte pueda pasar los datos a la aplicación destino correspondiente.

TCP establece una conexión: Para que comience la transferencia de datos, el usuario de la capa de transporte debe establecer una sesión orientada a conexión con su sistema par. Entonces, los programas de aplicación emisores y receptores deben informar a sus sistemas operativos respectivos que se iniciará una conexión. El concepto es que un dispositivo realiza una llamada a otro dispositivo, que este último debe aceptar. Los módulos de software de protocolo en los dos sistemas operativos se comunican enviando mensajes a través de la red a fin de verificar que la transferencia esté autorizada y que ambos lados estén preparados. Después de que se haya producido toda la sincronización, se establece una conexión, y comienza la transferencia de datos. Durante la transferencia, los dos dispositivos siguen comunicándose con su software de protocolo para verificar que estén recibiendo los datos correctamente.

El gráfico ilustra una conexión típica entre sistemas emisores y receptores. El primer saludo solicita la sincronización. El segundo y el tercer saludo acusan recibo de la petición inicial de sincronización, y sincronizan los parámetros de conexión en sentido opuesto. El segmento final del saludo envía un acuse de recibo al destino y ambos lados aceptan que se ha establecido una conexión. A partir del momento en que se establece la conexión, comienza la transferencia de datos.

TCP envía datos con control de flujo: Mientras la transferencia de datos está en marcha, se puede producir congestión por dos motivos diferentes. En primer lugar, un computador de alta velocidad puede generar tráfico a una velocidad mayor que la capacidad de una red para transferirla. En segundo lugar, si varios computadores envían datagramas simultáneamente a un solo destino, este destino puede sufrir congestión. Cuando los datagramas llegan demasiado rápido como para que un host o gateway los procese, se almacena temporalmente en la memoria. Si el tráfico continúa, tarde o temprano el host o el gateway agota su memoria y descarta cualquier otro datagrama que llegue.

En lugar de permitir que los datos se pierdan, la función de transporte puede emitir un indicador de "no está listo" al emisor. Este indicador funciona como una señal de "pare" e indica al emisor que debe dejar de enviar datos. Cuando el receptor está en condiciones de aceptar más datos, envía un indicador de transporte de "listo", que es como una señal de "siga". Cuando el dispositivo emisor recibe este indicador, reanuda la transmisión de segmentos.

TCP logra la confiabilidad con el uso de ventanas. Una transferencia confiable de datos orientada a conexión significa que los paquetes de datos llegan en el mismo orden en el que se envían. Los protocolos fallan si algún paquete se pierde, se daña, se duplica o se recibe en el orden incorrecto. Para garantizar la confiabilidad de transferencia, los dispositivos receptores deben mandar un acuse de recibo de todos y cada uno de los segmentos de datos.

Si un dispositivo emisor debe esperar el acuse de recibo después de enviar cada segmento, es fácil ver que el rendimiento será bastante bajo. Sin embargo, como hay un período de tiempo no utilizado disponible después de cada transmisión de paquetes de datos y antes de procesar cualquier acuse de recibo recibido, se puede usar el intervalo

para transmitir más datos. La cantidad de paquetes de datos que se permite que un emisor transmita sin recibir un acuse de recibo se denomina ventana.

El uso de ventanas es un acuerdo entre el emisor y el receptor. Es un método para controlar la cantidad de información que se puede transferir de un extremo al otro. Algunos protocolos miden la información en términos de la cantidad de paquetes; TCP/IP mide la información en términos de cantidad de bytes.

Técnica de acuse de recibo de TCP La entrega confiable garantiza que una corriente de datos enviada desde un dispositivo sea entregada a través de un enlace de datos a otro dispositivo sin que se dupliquen o pierdan los datos.

El acuse de recibo positivo con retransmisión es un proceso que garantiza la entrega confiable de corrientes de datos. Exige que un receptor envíe un mensaje de acuse de recibo al emisor siempre que reciba datos. El emisor mantiene un registro de cada paquete de datos enviado y luego espera el acuse de recibo antes de enviar el siguiente paquete de datos. El emisor también inicia un temporizador cada vez que envía un segmento y retransmite el segmento si el temporizador expira antes de que llegue el acuse de recibo.

Capa 3: Red

La capa de red (*Network Layer* en inglés) se encarga de que un mensaje llegue del nodo transmisor al nodo receptor a través de una red de múltiples nodos. Los nodos intermedios que trabajan en capa 3 se conocen como enrutadores (routers).

Esta capa tiene ciertas misiones:

- Asignación de direcciones de red únicas
- Interconexión de subredes distintas
- Encaminamiento de paquetes
- Control de gestión

Los nodos intermedios que trabajan en capa 3 se conocen como enrutadores (*routers*). Las unidades de información relevantes a la capa de red son los paquetes (*packets*). Algunos protocolos de capa 3 incluyen ARP, IP, X.25, ICMP, NetBEUI, IPX y Appletalk.

Capa 2: Enlace

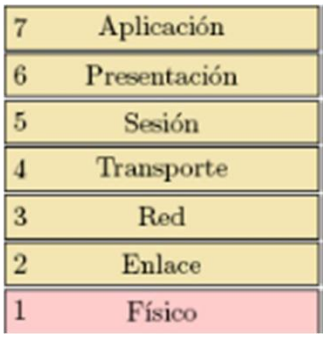
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace
1	Físico

La capa de enlace (*Data Link Layer* en inglés) se encarga del formato de los bloques de datos (tramas), de los códigos de dirección (en medios compartidos), de la detección y recuperación de errores y del control de flujo entre equipos (para evitar que un equipo más rápido desborde a uno más lento), para proveer servicios de conexión entre nodos adyacentes.

Esta capa suele dividirse en dos subniveles: el de enlace lógico, siempre presente, y el de acceso al medio, exclusivo de medios compartidos. Los elementos de red que trabajan como intermediarios en capa 2 se conocen como conmutadores (*switches*) o puentes (*bridges*).Las unidades de información relevantes a la capa de enlace se conocen como

tramas (*frames*). Algunos protocolos de capa 2 incluyen Ethernet, Token Ring, FDDI, ATM y HDLC.

Capa 1: Físico



La capa física (*Physical Layer* en inglés) se encarga de la transmisión de los bits entre nodos adyacentes. Las unidades de información relevantes son así los bits.

En este nivel se definen las características eléctricas, mecánicas y procedimentales de la comunicación en red, así como las formas de codificación de bit en los diferentes tipos de enlace.

La capa física define las características mecánicas, eléctricas y de codificación de bit de los diferentes tipos de enlace.

Los elementos de red que trabajan como intermediarios en capa 1 se conocen como repetidores. Un tipo especial de repetidores son los concentradores o hubs.

Encapsulamiento

El encapsulamiento es equivalente a introducir una carta en un sobre y marcarlo:
esconde la información de nivel superior para la capa respectiva, y proporciona la información que necesita la respectiva capa para manejar adecuadamente la pieza de información. El proceso de encapsulamiento puede también partir la información en piezas más pequeñas: en este caso el protocolo respectivo tiene la responsabilidad de recomponer las piezas en su destino.

Cada capa usa su propio protocolo de capa para comunicarse con su capa equivalente (su par) en otros sistemas. El protocolo de cada capa intercambia información, denominada unidades de datos de protocolo (PDU), con su capa par. Una capa puede usar un nombre más específico para su PDU. Por ejemplo, en TCP/IP la capa de transporte de TCP se comunica con su función TCP par mediante "segmentos". Cada capa usa los servicios de la capa inmediatamente inferior para comunicarse con su capa par. El servicio de la capa inferior usa la información de las capas superiores como parte de las PDU que intercambia con su par.

Los segmentos de TCP pasan a formar parte de los paquetes de la capa de red (datagramas) que se intercambian entre pares IP. Por su parte, los paquetes de IP pasan a formar parte de las tramas de enlace de datos que se intercambian entre dispositivos directamente conectados. Por último, estas tramas se transforman en bits a medida que los datos son transmitidos finalmente por el hardware utilizado por el protocolo de la capa física.

Cada capa depende de los servicios de la capa del modelo de referencia OSI inmediatamente inferior. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la unidad de datos de protocolo (PDU) de la capa superior en su campo de datos; entonces puede agregar los encabezados e información final que la capa necesite para cumplir su función.

Por ejemplo, la capa de red presta un servicio a la capa de transporte, y la capa de transporte presenta datos al subsistema de red. La capa de red tiene la tarea de desplazar estos datos a través de la red. Realiza esta tarea encapsulando los datos dentro de un paquete.

Este paquete incluye un encabezado que contiene la información necesaria para completar la transferencia, por ejemplo, las direcciones lógicas origen y destino.

La capa de enlace de datos por su parte presta un servicio a la capa de red. Encapsula el paquete de la capa de red en una trama. El encabezado de trama contiene la información necesaria para completar las funciones de enlace de datos (por ejemplo, direcciones físicas). Finalmente, la capa física proporciona un servicio a la capa de

enlace de datos: Codifica la trama de enlace de datos en un patrón de unos y ceros para su transmisión a través del medio (por lo general un cable).

Los cinco pasos del encapsulamiento de datos

A medida que las redes prestan servicios a los usuarios, el flujo y la organización en paquetes de la información original del usuario pasan por diversos cambios. En este ejemplo de redes, se pueden distinguir cinco pasos de conversión.

- **Paso 1.** Un computador convierte un mensaje de correo electrónico en caracteres alfanuméricos que pueden ser utilizados por el sistema de redes. Estos son los datos.
- **Paso 2.** Los datos del mensaje son segmentados para su transporte en el sistema de red por la capa de transporte. La capa de transporte garantiza que los hosts del sistema de correo electrónico que intercambian mensajes desde ambos extremos de la red se puedan comunicar de manera confiable. La función de cada capa debería escogerse pensando en la definición de protocolos estandarizados internacionalmente.
- **Paso 3.** Los datos entonces son convertidos en un paquete, o datagrama, por la capa de red. El paquete también contiene un encabezado de red que incluye una dirección lógica origen y destino. La dirección ayuda a los dispositivos de red a enviar el paquete a través de la red por una ruta seleccionada.
- **Paso 4.** Cada dispositivo de la capa de enlace de datos coloca el paquete en una trama. La trama permite que el dispositivo se conecte al siguiente dispositivo de red directamente conectado en el enlace.
- **Paso 5.** La trama se transforma en un patrón de unos y ceros para su transmisión en el medio (por lo general un cable). Una función de temporización permite que los dispositivos distingan los bits a medida que se desplazan por el medio.

El medio en la red física puede variar a lo largo de la ruta. Por ejemplo, un mensaje de correo electrónico se puede originar en una LAN, atravesar el backbone de un campus, y continuar a lo largo de un enlace WAN hasta llegar a su destino en otra LAN remota.

Modelo conceptual TCP/IP

El departamento de Defensa de EE.UU, (DoD), creó el modelo de referencia TCP/IP porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia. Para tener una mejor idea, podemos imaginarnos un mundo, cruzado por numerosos tendidos de cables, alambres, microondas, fibras ópticas y enlaces satelitales. Entonces, vemos la necesidad de transmitir datos independientemente del estado de un nodo o red en particular. El DoD requería una transmisión de datos confiable hacia cualquier destino de la red, en cualquier circunstancia. La creación del modelo TCP/IP ayudó a solucionar este difícil problema de diseño. Desde entonces, TCP/IP se ha convertido en el estándar en el que se basa INTERNET.

El modelo TCP/IP tiene cuatro capas: la capa de aplicación, de transporte, de Internet y la capa de acceso de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI. Resulta fundamental no confundir las funciones de las capas de los dos modelos ya que estas se desempeñan de diferente manera en cada modelo.

Este modelo se basa en protocolos para comunicación por red de datos. Es un protocolo DARPA que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP/IP Proviene de dos protocolos importantes de la familia, el *Transmission Control Protocol* (TCP) y el *Internet Protocol* (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto.

El modelo TCP/IP es una simplificación del modelo OSI. Sus principales protocolos son el protocolo de red IP y los protocolos de transporte TCP y UDP; aunque incluye otros protocolos de capa de red y transporte.

El *Protocolo de Control de Transmisión* (TCP) es un servicio orientado a conexión que se implanta en host. La entidad de TCP en cada extremo de una conexión debe asegurar que los datos se entreguen a su aplicación local de forma precisa, en secuencia, completa y libre de duplicados y errores.

El mecanismo básico para conseguirlo se ha utilizado desde el inicio de las comunicaciones de datos.

El TCP emisor de datos:

1. Enumera los segmentos.

2. Fija un temporizador. (TDV o TTL)

3. Transmite el segmento.

El TCP Receptor de datos:

Tiene que mantener informado al (TCP emisor) del número de datos correctos recibidos mediante una confirmación (ACK) para un segmento dentro del plazo del temporizador; TCP reenvía el segmento. Esta estrategia se denomina retransmisión con confirmación positiva. En algunas ocasiones, la retransmisión puede causar que se entreguen segmentos repetidos al TCP receptor.

El receptor debe reordenar todos los segmentos entrantes en el orden correcto, descartando los repetidos y por último entregar los datos a la aplicación en orden y sin pérdida de trozos. Hasta este punto, parece como si hubiera un lado que envía y otro que recibe. TCP es un protocolo dúplex, es decir, es capaz de enviar y recibir datagramas simultáneamente haciendo el papel de emisor y receptor al mismo tiempo.

Entremos un poco más en lo técnico, el modelo conceptual de una conexión es que una aplicación envía un flujo de datos a otra aplicación pareja, al mismo tiempo, recibe un flujo de datos de la otra. TCP proporciona un servicio Dúplex que maneja simultáneamente los dos flujos de datos.

TCP debe convertir los flujos de datos salientes de una aplicación en segmentos, de forma que se puedan entregar a las aplicaciones remotas. ¿Cómo se hace?

Bien, la aplicación traslada los datos a TCP y TCP sitúa estos datos en un bufer de envío. TCP toma un trozo de los datos y le añade una cabecera , creando un segmento, luego traslada este segmento a IP para que lo entregue como un único datagrama. El empaquetado de datos en trozos del tamaño adecuado permite usar de manera eficiente los servicios de transmisión, por lo que TCP debería esperar a recoger una cantidad razonable de datos antes de crear un segmento.

Puertos de Aplicación TCP

Un cliente debe ser capaz de identificar el servicio que necesita y para establecer conexiones TCP es necesario un puerto de entrada que identifique dicho servicio y permita la sesión, los números de puerto de TCP están desde 0 hasta 65.535, los puertos que están desde 0 hasta 1.023 se encuentran reservados por servicios de uso estándar.

¿Y los puertos que usan los clientes?

En este caso, existen ocasiones en que los clientes pueden trabajar con números de puertos que no se encuentran estandarizados, es decir, en la mayoría de los casos los clientes que requieren una conexión pide al sistema operativo que le asigne un numero de puerto en desuso, sin reservar. Al finalizar la sesión, el cliente devuelve el puerto al sistema y lo puede utilizar otro cliente.

Funciones de TCP

- Asociar puertos de conexiones.
- Establecer conexiones utilizando un acuerdo en tres pasos.
- Realizar un arranque lento para no sobrecargar la red.
- Dividir los datos en segmentos para su transmisión.
- Numerar los datos.
- Manejar los segmentos entrantes duplicados.
- Calcular las sumas de control.
- Regular el flujo de datos usando las ventanas de envío y recepción.
- Terminar las conexiones de manera ordenada.
- Abortar conexiones.
- Marcar datos urgentes.

- Confirmación positiva con retransmisión.
- Calculo de los plazos de retransmisión.
- Reducir el tráfico cuando la red se congestiona.
- Indicar los segmentos que llegan en desorden.
- Comprobar si las ventanas de recepción están cerradas.

Establecimiento de una Conexión

¿Cómo se inicia una conexión entre dos aplicaciones?

Siempre, antes de poder comunicarse, ambas partes llaman a una subrutina que crea un bloque de memoria para almacenar los datos de TCP y de IP durante la conexión, como las direcciones de los conectores (sockets), los números actuales de secuencia, el valor inicial de IP para el tiempo de vida y otros. La aplicación servidora espera a los clientes. Un cliente que desee acceder al servidor lanza una solicitud de conexión mediante la dirección IP y el puerto del servidor.

Escenario de una conexión

El proceso de conexión se lleva a cabo mediante un acuerdo de tres pasos, ya que se intercambian tres mensajes para establecer la conexión, llamados SYN, SYN y ACK. Durante el establecimiento de conexión se intercambian importantes elementos de información. Cada parte notifica a la otra:

1. Del espacio disponible en su búfer.

2. La cantidad máxima de datos que puede llevar un segmento.

3. El numero inicial de secuencia que se usara para numerar los datos de salida.

Tenga en cuenta que cada parte usa los elementos 1 y 2 para establecer los límites de lo que puede hacer la otra parte. Se presenta el caso en que el bufer de almacenamiento de datos de una supercomputadora es mayor que la de un PC, por lo tanto la estructura de memoria de la PC se reduciría a 1K, la posibilidad de poder controlar como la otra parte envía los datos, es una característica interesante en las próximas implementaciones de IP. Por ejemplo, tenga en cuenta que en este caso el cliente maneja mayores segmentos que el servidor.

1. El servidor se inicializa y está listo para aceptar conexiones de clientes. A esto se le denomina apertura pasiva. (*passive open*)

2. El cliente solicita a TCP que abra una conexión con un servidor en una determinada dirección y puerto de IP. A esto se le denomina apertura activa,(*active open*)

3. El TCP cliente recoge un número inicial de secuencia, 1000 en el ejemplo. El TCP cliente envía un segmento de sincronización llamado SYN, con este número de secuencia, el tamaño de la ventana de recepción (4K) y el tamaño del mayor segmento que puede recibir el cliente (1460 bytes).

4. Cuando llega SYN, el TCP servidor genera su número inicial de secuencia (3000). El TCP servidor envía un segmento SYN con su número inicial de secuencia (3000), un ACK 1001, que significa que el primer bytes enviado por el cliente debería tener el número 1001, el tamaño de su ventana de recepción (4K) y el tamaño del mayor segmento que puede recibir (1024 bytes).

5. Cuando el TCP cliente recibe el mensaje SYN/ACK del servidor, envía de vuelta un ACK 3001, lo que significa que el primer bytes de datos enviado por el servidor debería tener el 3001.

6. El TCP cliente notifica a la aplicación que la conexión está abierta.

7. Cuando el TCP servidor recibe el ACK del TCP cliente, el servidor notifica a su aplicación que la conexión está abierta.

El cliente y el servidor han establecido reglas para el inicio de sesión y están listos para empezar a transferir datos.

Transferencia de Datos

Comienza una vez terminado el proceso de los tres pasos iniciales. Para que la numeración resulte sencilla, se usan mensajes de 1000 bytes. Todas las cabeceras de los segmentos de TCP llevan un campo ACK que identifica el número de secuencia del siguiente byte que se espera del otro extremo.

El primer segmento que envía el cliente contiene los bytes del 1001 al 2000. Su campo ACK anuncia que el número de secuencia del byte que se espera del servidor comienza en 3001. El servidor responde con un segmento que contiene 1000 bytes de datos que empieza en el 3001. El campo ACK de la cabecera de TCP indica que se han recibido correctamente los bytes 1001 al 2000 por lo que el siguiente número de secuencia que se espera del cliente es el 2001.

Por lo que el cliente comienza a enviar segmentos que empiezan en los bytes 3001, 4001 y, 5001. Tenga en cuenta que el cliente no tiene que esperar a que llegue el ACK de cada segmento enviado. Se pueden enviar datos al otro extremo siempre y cuando exista espacio libre en el bufer.

Finalización de un Conexión TCP

La terminación normal de una conexión se lleva a cabo mediante tres pasos similares a los de inicialización, cualquiera de las partes puede lanzar el proceso de terminación, que suele seguir el siguiente proceso:

A. < He terminado, no tengo más datos para enviar> B. <OK>

B. <Yo también he terminado> A. <OK>

En un escenario en el que TCP experimente una Terminación Abrupta causada por problemas serios que TCP no pueda resolver, se envían uno o varios mensajes de RESET al otro extremo para cerrar la conexión.

Rendimiento: ¿Qué tan Bien se Comporta TCP?

Hay muchos factores que afectan el rendimiento de TCP. Los básicos son los recursos como la memoria y el ancho de banda. El ancho de banda y los retardos de la red subyacente imponen límites al rendimiento. Una baja calidad de transmisión implica un

gran número de datagramas descartados. Al descartarlos se desencadenan retransmisiones con lo que se reduce el ancho de banda efectivo.

Un receptor que dispone de un gran bufer de entrada permite que el emisor continúe transmitiendo sin interrupción. Resulta muy importante en redes grandes con gran retardo.

Otro factor que afecta el rendimiento TCP son las características y la capacidad del servidor o hots para reaccionar rápidamente ante eventos de alta prioridad y realizar cambios de contexto, es decir, dejar una tarea y comenzar otra de mayor importancia. Un servidor puede estar dando servicios a muchos usuarios locales interactivos, procesos de fondo y docenas de comunicaciones.

Se necesitan recursos suficientes de CPU para procesar rápidamente las cabeceras de TCP, un procesador que no pueda calcular de manera eficaz los valores de la suma de control de una cabecera TCP suele ralentizar la transmisión de datos. Por último, los fabricantes deben ser capaces de implementar técnicas de configuración más sencillos para los administradores de red y de esta manera puedan ajustarlos a su entorno.

Protocolo de Enrutamiento o Protocolo de Internet (IP)

El protocolo de IP proporciona los mecanismos necesarios para el transporte de los segmentos creados por TCP. Las unidades creadas por IP se les llaman datagramas de IP, que son transportadas por la red a través de rutas aleatorias de manera independiente una de otras. IP es un protocolo que se desenvuelve en el nivel (3) de OSI, su función es hacer lo mejor que se pueda para entregar un datagrama al host destino. IP no garantiza la entrega fiable de los datagramas al host destino, los datagramas se pueden destruir en el camino debido a:

- Errores en los bits durante la transmisión por el medio.
- Que un en caminador congestionado descarto el datagrama debido a la falta de espacio en el búfer.
- Temporalmente, no había camino hasta el destino.

Todas las funciones que aseguran la fiabilidad del envío y entrega de datos se ha concentrado en la capa de TCP como vimos con anterioridad. IP sólo hace lo mejor por entregar estos datagramas de un extremo a otro.

Características del Protocolo IP

- Protocolo orientado a no conexión.
- Fragmentación y reensamblado de paquetes si es necesario.
- Enrutamiento por medio de direcciones lógicas IP de 32 bits.
- Asignación de tiempos de vida (TDV) a los datagramas de IP.
- Realiza el "mejor esfuerzo" para el transporte de paquetes y no garantiza su entrega.
- Tamaño máximo del paquete de 65635 bytes.
- Un protocolo 100% adaptativo.

Funciones Principales de IP

1. Aceptar y transportar los datos provenientes de TCP o UDP.
2. Crear un datagrama de IP, encaminarlo por la red y entregarlo a una aplicación destino.
3. Adaptarse a las características del medio.

Cada datagrama se encamina de manera independiente por la red, IP confía en dos herramientas que le ayudan a encaminar los datagramas:

1. La máscara de Subred.

2. La tabla de encaminamiento IP.

¿Cómo sucede esto?

Supóngase que su computadora tiene datos que enviar a través de la red, la dirección IP que se ha asignado a su PC es: 192.168.10.131, tiene que enviar datos a 192.168.10.12, es decir,

- Desde: 192.168.10.131
- Hacia : 192.168.10.12

Puede suponer que las dos computadoras se encuentran dentro de la misma subred, sin embargo, su computadora debe comprobar si esto es cierto o no, esto es posible comprobando la máscara de subred:

255.255.255.0

La computadora realmente realiza un AND lógico entre cada una de las direcciones IP y la Máscara de subred, en este ejemplo el encaminamiento es directo debido a que ambos sistemas están ubicados en la misma subred. En caso de que el host destino se encuentre en un sistema vecino, es decir, otra red, IP debe verificar su tabla de enrutamiento mediante un protocolo ARP y determinar cuál es la dirección que se utilizara como una pasarela a la red vecina. Este trabajo se lleva cabo generalmente por equipos de enrutamiento lógico o físico.

Para explicar el tema de manera superficial, IP no necesita conocer la ruta completa que lo llevara a la red destino, sólo necesita descubrir cuál es el siguiente salto (gateways o puerta de enlace) y enviar allí el datagrama.

Para enviar un datagrama a la interfaz de un encaminador (X) hay que envolver el datagrama en una trama cuya cabecera contenga la dirección física de la tarjeta de interfaz de encaminador. Cuando el encaminador recibe la trama, elimina la cabecera y la cola de la trama y examina la cabecera del datagrama de IP para decidir hacia

donde debe ir a continuación. Si no existe se busca en la tabla un prefijo de encaminamiento. Si no existe se usa el encaminamiento por defecto.

IP es un protocolo adaptativo, es decir, en todo momento se realiza una comprobación de la mejor ruta a seguir para el siguiente salto comprobando la tabla de encaminamiento del nodo actual, las entradas de la tabla de encaminamiento pueden cambiar en cualquier momento dependiendo de las condiciones de la red.

Por ejemplo si un enlace deja de funcionar se enviaran los datagramas por una ruta diferente, si es que existe. Un cambio en la topología de la red puede hacer que los datagramas se re encaminen automáticamente. El encaminamiento adaptativo es la base de la flexibilidad y la robustez de IP.

IP utiliza también, técnicas de fragmentación y reensamblado más temporizadores de datagramas que permiten encaminar los datagramas a través de Routers congestionados o pasar de redes con grandes prestaciones a redes pequeñas y de baja calidad de tráfico. Esto hace posible que un datagrama de IP atraviese el continente pasando por una gran variedad de tecnologías de comunicación que van desde las redes de telefonía básica hasta los enlaces dedicados por satélite o fibra óptica y viceversa.

Cada datagrama de IP tiene un Tiempo de Vida (TDV o TTL) que expira según se configure el temporizador por TCP, ésto provoca la retransmisión del datagrama por parte de TCP.

La MTU e IP

La Unidad de Transmisión Máxima determina la longitud máxima, en bytes, que podrá tener un datagrama de IP para ser transmitida por una red física. Obsérvese que este parámetro está determinado por la arquitectura de la red: para una red Ethernet el valor de la MTU es de 1500 bytes. Dependiendo de la tecnología de la red los valores de la MTU pueden ir desde 128 hasta unos cuantos miles de bytes. Algunas características:

- Indica la longitud de una trama que podrá ser enviada a una red física en particular.
- Es determinada por la tecnología de la red física.

- Para el caso de Ethernet es de 1500 bytes.

Rendimiento de IP ¿Qué tan bien trabaja IP?

Se aplican las mismas características que el caso de TCP. Siempre tener en cuenta que los puntos más importantes a considerar se encuentran en:

1. Ancho de banda de la transmisión. (Depende de la Certificación de la Red)

2. Memoria de los Búfer. (Depende del software, Router, y equipos de LAN)

3. Capacidad de procesamiento de la CPU. (Características de los Servidores) Estos son los puntos críticos que afectan el rendimiento de una Red IP, no se conocen

Mecanismos de control. El diseño de un protocolo es una lucha constante contra entre ganancias y pérdidas de eficiencia.

Formas de trabajo en red

El establecimiento de una red telemática implica diversas alternativas de distribución de las tareas y del procesamiento de la información entre los elementos que la conforman. Para ello es importante comprender cuáles son los elementos de una aplicación y posteriormente analizar los diferentes modelos posibles de trabajo entre ellos se tienen: Modelos de niveles, modelo de tres capas, redes distribuidas, entre otros.

Elementos de una aplicación

Una aplicación requiere de una serie de elementos: estos incluyen el código del programa o los programas que ejecutan la aplicación, los datos sobre los cuales trabaja la aplicación y la interfaz de usuario.

Código

El código es el conjunto de instrucciones que permiten la manipulación de los datos y las entradas para obtener los resultados deseados. El código radica en una unidad de almacenamiento como un disco duro o un servidor de archivos mientras no está siendo usado. Al ejecutarse radica en la memoria de un computador y utiliza recursos de procesamiento de éste.

Datos

Los datos consisten en el conjunto de la información sobre la cual trabaja una aplicación. Estos datos pueden ser archivos de documentos, bases de datos, archivos de configuración, etc. La recuperación de datos requiere, en muchos casos, recursos de procesamiento.

Presentación

La presentación es la definición de la interfaz de usuario; es decir el conjunto de pantallas y procedimientos por medio de los cuales el usuario utiliza la aplicación. La presentación siempre requiere algún tipo de procesamiento en la máquina local (es decir, donde se encuentra el usuario). Es posible, sin embargo, que parte de la presentación esté determinada en un lugar remoto.

Modelo de dos niveles

En un modelo de trabajo en red de dos niveles, los elementos de una aplicación (código, datos y presentación) se distribuyen entre una máquina local y una máquina remota.

Terminal remota

En un esquema de terminal remota (o terminal bruta), el código, datos y presentación utilizan recursos de la máquina remota, y en la máquina local se presentan los resultados de la presentación.

Ejemplos: terminales brutas de un *Mainframe*, o acceso a una aplicación vía Telnet.

Servidor de archivos

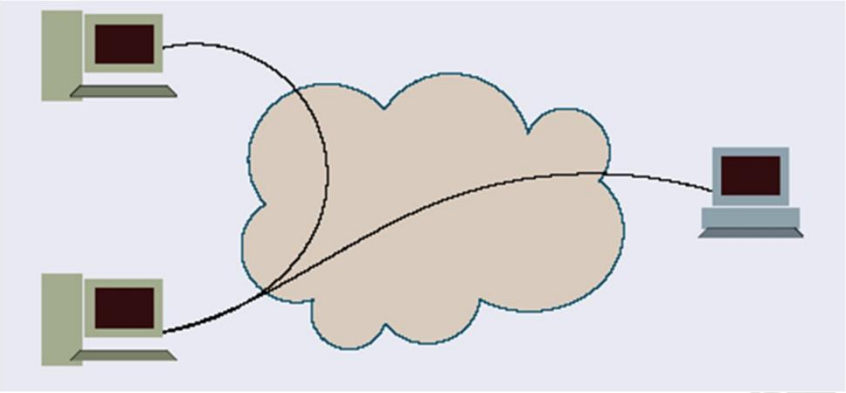
En un esquema de servidor de archivos todo el procesamiento de código, recuperación y manipulación de datos y presentación son ejecutados en una máquina local mientras la aplicación está en uso.

Los archivos (ejecutables y/o de datos) residen, sin embargo, en la máquina remota, mientras la aplicación no está siendo utilizada.

Modelo cliente-servidor

En un esquema cliente servidor típico, el código y los datos se procesan en la máquina remota (servidor) y la presentación y parte de los datos se procesan en la máquina local (cliente). Adicionalmente el cliente es el que comanda al servidor. La distribución entre los elementos de la aplicación puede ser diferente, por ejemplo parte del código puede ejecutarse en el cliente.

Modelo de tres capas

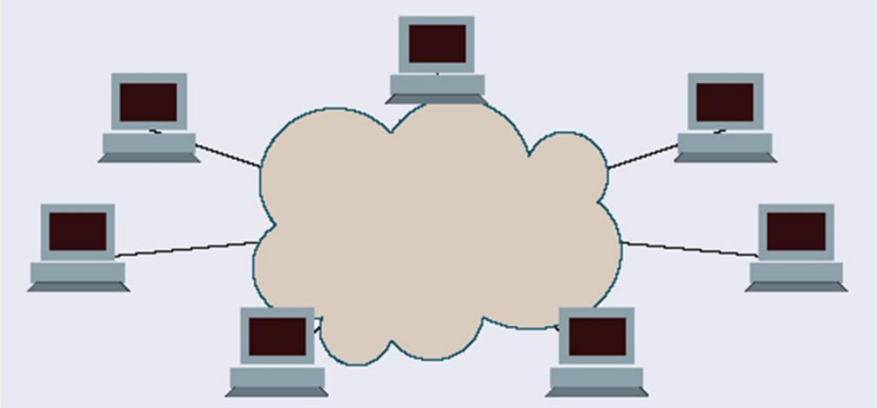


Un modelo de tres capas se compone típicamente de un servidor de aplicaciones, un servidor de base de datos y el cliente, como tres máquinas distintas.

El código de la aplicación y la presentación se distribuye entre el cliente y el servidor de aplicaciones. El cliente no tiene acceso directo a la información que reside en el servidor de base de datos.

El servidor de aplicaciones cumple así como una interfaz de seguridad entre el usuario y la información.

Redes distribuidas



En lugar de concentrar la información y las aplicaciones en un número limitado de servidores, los distintos elementos de la información y las distintas aplicaciones pueden distribuirse entre varias máquinas.

Grupos de trabajo

Los grupos de trabajo son distribuciones de jerarquía plana, sin control central sobre los recursos.

Dominios

Los dominios son distribuciones de jerarquía plana en los cuales el acceso a los recursos está supervisado por un controlador de dominio.

Racimos

Conocidos en inglés como *clusters*, un racimo es un conjunto de máquinas que funcionan como un único servidor.

Extensión de las redes

Dependiendo de la distribución geográfica de los nodos que deben ser interconectados, las redes pueden ser clasificadas en distintos tipos. En esta sección se abordarán estas clases, conocidas como redes WAN, MAN, LAN y Personales.

Redes de distintos alcances

Las redes se pueden distinguir por el tamaño de la distribución geográfica (alcance) de las mismas. La siguiente tabla muestra una clasificación de las redes de acuerdo con este criterio.

distancia	tipo	ejemplo
1 mm		*chip*
1 cm		computador
10 cm		computador
1 m	área personal	puesto de trabajo
10 m	á. pers./á. local	oficina
100 m	área local	edificio
1000 m	área local	campus
10 km	área metropolitana	ciudad
100 km	área amplia	país
10000 km	área amplia	continente

Redes de área amplia

Las redes de área amplia (WAN) se extienden a través de varios kilómetros, conectando nodos que se encuentran en ciudades diferentes. Por extensión se llama también WAN a las redes que unen nodos dentro de una misma ciudad entre edificios que no pertenecen a un mismo campus, principalmente cuando se usan tecnologías similares a las conexiones entre ciudades.

Los enlaces WAN suelen estar basados en tecnologías seriales de bajo ancho de banda entre nodos finales y uso compartido de enlaces de alto ancho de banda a través de la multiplexación.

Redes de área metropolitana

También conocidas como redes de área intermedia (MAN) se extienden a través de unos pocos kilómetros conectando nodos dentro de una misma zona urbana.

Una red de área metropolitana usa tecnologías de amplio ancho de banda, basados en fibra óptica y microondas, entre otros medios.

Redes de área local

Una red de área local (LAN), está restringida a un espacio geográfico limitado a un edificio, un campus, una oficina o una casa.

Utiliza una serie de medios de enlace guiados tales como fibra óptica y cable eléctrico aunque cada vez es más común el uso de medios abiertos en redes inalámbricas.

Suele contar con un ancho de banda alto entre nodos.

Redes de área personal

Las redes de área personal son las que permiten la conexión entre los elementos que se encuentran dentro de un mismo puesto de trabajo, o que son portados por una misma persona.

Protocolos, medios y elementos de red

Introducción

Al igual que una casa bien construida, una red debe edificarse sobre cimientos sólidos. en el modelo de referencia OSI, esta base es la Capa 1 o capa física. Los términos utilizados en este tema describen cómo las funciones de red se relacionan con la capa física del modelo de referencia OSI. La capa física es la capa que define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

En este tópico, aprenderá acerca de las funciones de red que tienen lugar en la capa física del modelo OSI. Aprenderá acerca de los diferentes tipos de medios para networking que se usan en la capa física, incluyendo el cable de par trenzado blindado, el cable de par trenzado no blindado, el cable coaxial y el cable de fibra óptica. Además, aprenderá cómo los dispositivos de red, especificaciones de cables, topologías de red, colisiones y dominios de colisión pueden ayudar a determinar cosas tales como la cantidad de datos que pueden viajar a través de la red y a qué velocidad.

Medios de enlace

Los medios de enlace, son mecanismos de transmisión de energía y/o información en el contexto de un sistema de comunicación, que utiliza diferentes tipos de soporte físico.

Si bien en una teoría general de comunicaciones existe una gama muy variada de medios, nos concentraremos en los medios usados para la comunicación entre máquinas. Particularmente para la comunicación digital entre máquinas.

Tipos de medio por conexión

La primera gran clasificación entre medios está entre guiados y abiertos.

Medios guiados

Los medios guiados son aquellos que conectan dos o medios y existe una conexión clara de cada nodo al medio. Por ejemplo el cable.

Medios abiertos

En los medios abiertos los nodos deben estar al alcance de los otros nodos a través del medio, pero no hay conexión clara del nodo al medio. Por ejemplo la radiodifusión.

Tipos de medios por característica física

Los medios requieren la manipulación de alguna propiedad física para transmitir información. Algunos de los elementos físicos que se pueden manipular incluyen:

El espectro electromagnético de bajo y alto radio

Señales eléctricas como voltaje, corriente o impedancia (eléctrico) Vibraciones mecánicas (audio)

En el caso de los medios oscilantes (medios electromagnéticos, vibraciones mecánicas o corriente alterna), se puede manipular la amplitud, la frecuencia o la fase.

Medios digitales y análogos

Si bien toda manipulación de las propiedades físicas genera una señal análoga, se considerará un medio digital aquel medio diseñado para que los nodos que accedan a éste interpreten la señal como un conjunto discreto de símbolos (usualmente 1 y 0).

Modulación y codificación

Se conoce como codificación a la forma por medio de la cual un conjunto discreto de símbolos, es representado como una señal digital o análoga que modifica el medio.

Se conoce como modulación la forma como una señal (análoga) manipula uno de los parámetros de un medio oscilante.

Algunos parámetros

Tiempo de símbolo (*ts*) es el tiempo que dura la transmisión de un símbolo en una transmisión digital.

Tiempo de bit (*tb*) es el tiempo que dura la trasmisión de un bit, es decir de un elementos primario de información binaria.

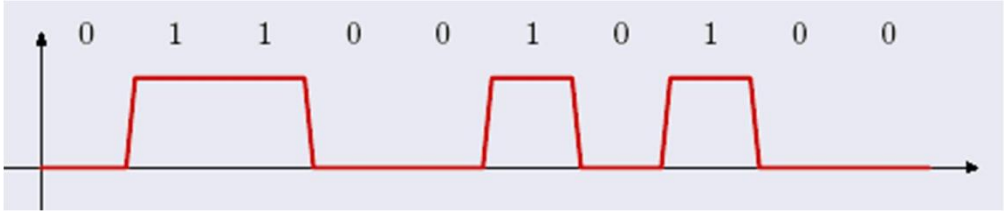
En una comunicación digital binaria, *ts* = *tb*.

Vida útil (δ_m)es la relación entre el tiempo de la existencia de una señal positiva de un símbolo *tm* y el respectivo *ts*.

$$\delta_m = \frac{t_m}{t_s}$$

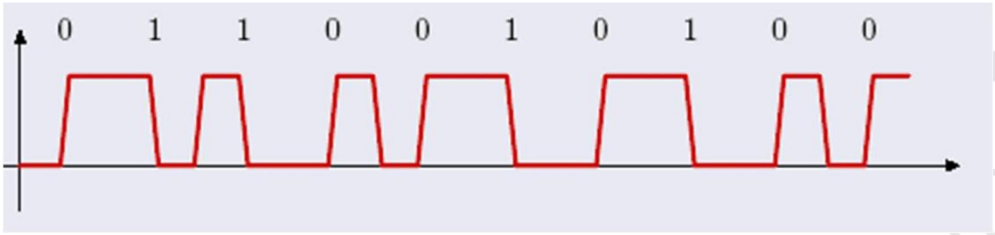
Codificaciones

Codificación por niveles



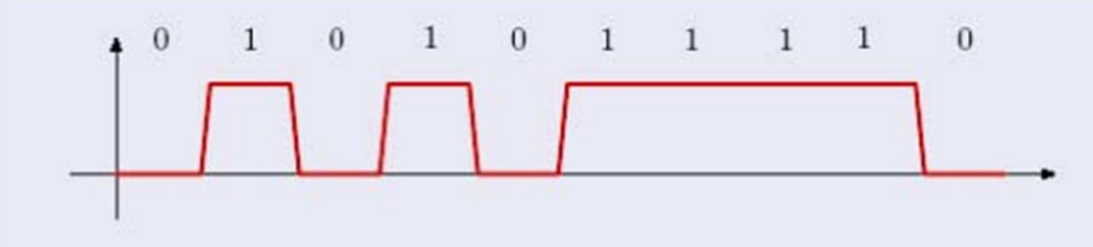
En la codificación por niveles, cada símbolo es representado por un nivel distinto de una propiedad física del medio. Por ejemplo un nivel alto para 1 y un nivel bajo para 0.

Codificación por cambio de nivel



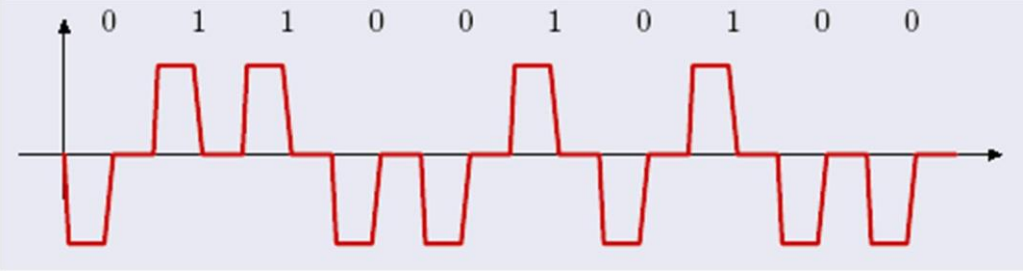
En la codificación por cambio de nivel, cada símbolo es representado por un cambio de nivel de una propiedad física del medio. P. ej de alto a bajo para 1 y de bajo a alto para 0.

Codificación diferencial



En la codificación diferencial, la forma de la señal no indica el símbolo sino el cambio de símbolo a símbolo.

Retorno a cero



En una codificación con retorno a cero, existe un nivel cero o neutro, y el nivel de cada símbolo dura una fracción del tiempo de símbolo *ts*.

Observación: no necesariamente el nivel cero o neutro corresponde al nivel del símbolo cero.

Modulación análoga

Existen diferentes tipos de modulación análoga, esto es, cuando una señal análoga modifica un parámetro de una señal oscilante:

Amplitud modulada (AM)

La amplitud de la señal sigue la forma de la señal modulante.

Frecuencia modulada (FM)

La frecuencia de la señal sigue la forma de la señal modulante.

Fase modulada (PM)

La fase de la señal sigue la forma de la señal modulada. Es poco usada en modulación análoga.

Banda lateral única

Es una modificación de la amplitud modulada que busca reducir la potencia de transmisión y el ancho de banda.

Modulación digital

La forma más sencilla de modular una señal digital, es codificando la señal en banda base y tomar la señal codificada como una señal modulante análoga (y se aplicaría alguna de las técnicas arriba descritas. Se puede modular directamente en forma digital:

Cambio de código en amplitud (ASK)

(Por *Amplitude Shift Keying*.) Con un tiempo de símbolo *ts* igual a un múltiplo del período de la señal *T*

$$t_s = \eta T$$

Cada símbolo es representado por una amplitud distinta.

Cambio de código en frecuencia (FSK)

(Por *Frequence Shift Keying*.) Por cada tiempo de símbolo *ts*, hay dos o más frecuencias *f1*, *f2*,. . . (Tantas como símbolos distintos) tales que *tsfn* es un número entero.

Cambio de código en fase (PSK)

(por *Phase Shift Keying*.) Conservando una frecuencia base tal que el tiempo de símbolo *ts* sea un múltiplo entero del período *T*

$$t_s = nT$$

Cada símbolo se representa por una fase distinta.

Modulaciones combinadas

Es común hacer combinaciones de fase y amplitud, para la codificación de un universo de más de dos símbolos distintos en un solo período.

Control

Un medio puede requerir algún tipo de control para que los nodos puedan determinar si existe o no comunicación, el sentido de la misma, cuando inicia y termina cada módulo de información, etc.

Control de acceso al medio

El control de acceso al medio indica cual de los nodos va a usar el medio y puede hacerlo.

Esto incluye peticiones (*requests*), permisos y notificaciones de estar listo.

Sincronización

La sincronización es el mecanismo por medio del cual se determinan los límites de las unidades de información.

Cuando existe una señal de reloj común para el nodo transmisor y los nodos receptores, se conoce como comunicación sincrónica o síncrona.

Cuando no existe tal reloj común, se conoce como comunicación asíncrona o asincrónica.

En el caso de la comunicación asíncrona es necesario utilizar mecanismos extra de sincronización que remplacen el reloj.

Un reloj es una señal independiente que marca el tiempo de símbolo *ts*.

Ejemplo: RS-232

La norma RS-232 define un sistema de comunicación digital para palabras de 7 bits, (extensible a 8 bits).

RS-232 funciona en banda base en voltaje. Esto es que la señal codificada afecta directamente un nivel de voltaje, sin modulación.

RS-232 está representado por dos niveles. Un nivel se conoce como marca (MARK) y el otro como espacio (SPACE).

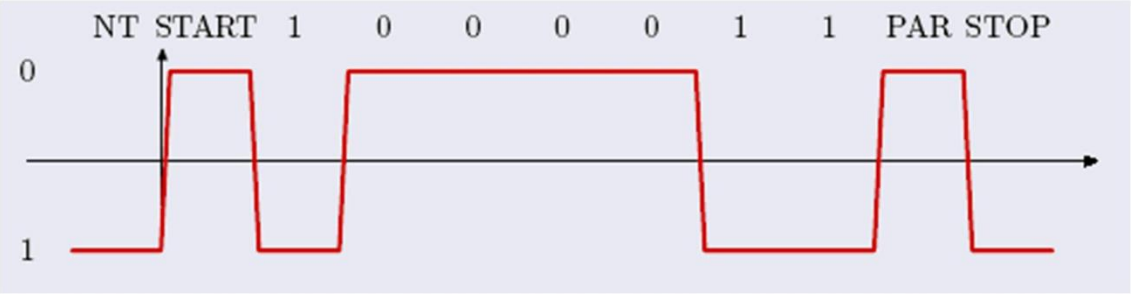
RS-232 es asíncrona. Cada palabra es compuesta de un bit de inicio (STAR), los bits de datos, un bit de paridad y un bit de parada (STOP). El cambio de STOP a STAR indica el inicio de una palabra.

STOP y 1 son representados por una MARK. STAR y 0 son representados por SPACE. MARK usa un voltaje negativo y SPACE usa un voltaje positivo.

La paridad puede ser par (even) o impar (odd). Con paridad par se busca que el número total de marcas (salvo STOP) sea par, y con paridad impar el número total de marcas (salvo STOP) es impar.

Usualmente al transmitir palabras de ocho bits (octetos o *bytes*), no se usa paridad. Si no se está transmitiendo un símbolo, se debe mantener el STOP (MARK).

El STOP más la marca de no transmisión hasta el siguiente STAR debe durar al menos el equivalente a *tb*, 11 2 *tb* o 2 *tb* de acuerdo a lo convenido. Esto se conoce como «un bit», «bit y medio» o «dos bits» de STOP, respectivamente RS-232 transmite en little endian. Esto quiere decir que el bit menos signi ficativo se transmite antes que el bit más significativo.



	MARK	SPACE
Voltaje mínimo	−20 V	3 V
Voltaje máximo	−3 V	20 V
Valor binario	1	0
Otro valor	STOP NT	START

Multiplexación

La multiplexación es el método por el cual varias señales de distintos orígenes y con distintos destinos, comparten un mismo medio de transmisión.

Multiplexación por división en frecuencia

(FDM) Modulando las señales a frecuencias distintas, se pueden combinar las señales moduladas en un mismo medio. Estas señales se pueden después separar mediante filtros y demodularse.

Multiplexación por división en tiempo

(TDM) Propio de la transmisión digital; en un canal de transmisión se asignan porciones de la trama de tiempo para cada uno de las fuentes.

Medios compartidos

Acceso múltiple

El acceso múltiple es similar a la multiplexión: varios mensajes con diferente origen y diferente destino, comparten un mismo medio. Las reglas de compartición no están dadas por un multiplexor sino que son seguidas por las fuentes de los mensajes:

Acceso múltiple con detección de portadora

(CSMA) Cada fuente que va a transmitir espera a que el medio esté libre. La forma más común es el CSMA/CA, utilizado, entre otros, por Ethernet.

Acceso múltiple por división en frecuencia

(FDMA) Cada fuente que va a transmitir se le asigna una frecuencia libre para que con ella module el mensaje.

Acceso múltiple por división de tiempo

(TDMA) Cada fuente que va a transmitir se le asigna una porción libre de la trama de tiempo.

Acceso múltiple con salto en frecuencia

(FHMA) En un esquema FDMA o TDMA modulado, la frecuencia de modulación es cambiada automáticamente cada determinado tiempo.

Acceso múltiple por división de código

(CDMA) En un esquema de espectro ensanchado, a cada fuente que va a transmitir se le asigna un código de dispersión del espectro.

Espectro Ensanchado

Conocido en inglés como *Spread Spectrum*, es una técnica de modulación que dispersa la potencia de una señal en un amplio espectro de frecuencia.

La potencia así dispersa es asimilable a ruido de baja potencia para un sintonizador corriente o para un sintonizador de espectro ensanchado que no comparta la clave de dispersión. Esta característica aumenta la seguridad.

Adicionalmente las fuentes puntuales de ruido (por ejemplo, interferencia electromagnética) son minimizadas por los sintonizadores de espectro ensanchado, lo que permite un mejor desempeño en ambientes con ruido electromagnético.

Puntos de acceso y redes ad hoc

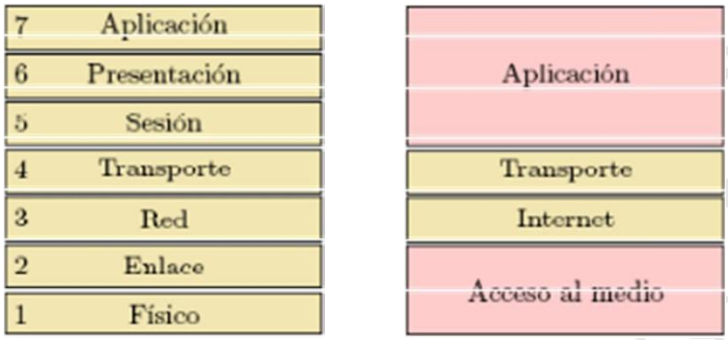
Punto de acceso. Un punto de acceso es una interfaz entre una red alambrada (p. ej Ethernet) y una red inalámbrica (p. ej Wi-Fi). Usualmente sirve como punto de conexión y autenticación para los dispositivos inalámbricos.

Red ad hoc. Una red ad hoc es la red formada por varios dispositivos inalámbricos sin un punto de acceso.

El stack de protocolos TCP/IP

Al igual que OSI, TCP/IP hace referencia tanto a un modelo de referencia, como a una pila de protocolos que trabajan sobre ese modelo.

Modelo OSI y Modelo TCP/IP



TCP/IP, es el protocolo de Internet (en realidad, es una familia de protocolos). En la actualidad es la elección recomendada para casi todas las redes, especialmente si la red tiene salida a Internet.

El modelo de referencia TCP/IP es, al igual que el modelo de referencia OSI, un modelo por capas. Es más simple, sin embargo, reconociendo sólo cuatro capas.

Sus principales protocolos son el protocolo de red IP y los protocolos de transporte TCP y UDP; aunque incluye otros protocolos de capa de red y transporte.

TCP/IP agrupa todo lo que está debajo de la capa de interred como una sola capa: capa de acceso al medio; y todo lo que está por encima de la capa de transporte se agrupa como capa de aplicación.

IP

El protocolo de Internet o IP es un protocolo de red basado en conmutación de paquetes. Funciona bajo el la base del «mejor esfuerzo» para la entrega de paquetes y el principio de «dispare y olvide». Su confiabilidad se reduce a un código de control: no posee confirmaciones ni secuenciación. Una vez enviado un paquete, el nodo que lo envía se desentiende del mismo (*Shoot and forget*).

Cuando un nodo intermedio recibe un paquete, busca la mejor forma de entregarlo al siguiente nodo (*Best Effort*). Sin embargo, si hay congestión o si no encuentra una ruta apropiada, el nodo puede ignorar el paquete (y reciclar los electrones).

Cuando un nodo no encuentra una ruta apropiada para un paquete, debe enviar un datagrama ICMP informando el intento fallido. Esta confirmación es de baja prioridad.

Un nodo intermedio que toma decisiones de envío basado en la dirección de red (v.g. dirección IP) se conoce como enrutador, ruteador o *router*.

Dirección IP

Una dirección IP se compone de 32 bits (4 octetos). Esta se representa convencionalmente escribiendo los octetos en decimal y separada por puntos.

La dirección se compone de tres elementos: red, subred y nodo (*host*). En ocasiones red y subred se consideran simplemente como red.

La "red" corresponde a los primeros 8, 16 o 24 bits de la dirección (dependiendo de la clase). Las unidades de información relevantes a la capa de red son los paquetes (*packets*).

La clase A, la red es de 8 bits y corresponde a las redes 1 a 126, para un total de 126 redes; cada red puede soportar hasta cuatro millones de nodos:

1.Y.Y.Y
126.Y.Y.Y

La clase B, la red es de 16 bits y corresponde a las redes 128.X a 191.X, para un total de 16384 redes, cada una puede soportar hasta sesenta y cinco mil nodos:

128.X.Y.Y
191.X.Y.Y

La clase C, la red es de 24 bits y corresponde a las redes 192.X.X a 223.X.X, para un total de dos millones de redes, cada una soportando un máximo de 254 nodos.

192.X.X.Y
223.X.X.Y

Las redes pueden ser particionadas en subredes, por ejemplo la red 172.16.0.0, con capacidad para 65534 nodos, puede ser particionada en 254 subredes de 254 nodos cada una:

172.16. 1 .Y
172.16. 2 .Y
172.16. 3 .Y
... ...
172.16.254.
Y

Para reconocer qué parte de la dirección corresponde a la *red+subred* y que parte corresponde al *nodo* dentro de la *subred*, se utilizan las máscaras.

La máscara de una red **clase A** sin subredes es 255.0.0.0 , esto indica que los primeros ocho bits (el primer octeto) es la red y los 24 bits restantes son el nodo.

La máscara de una red **clase B** sin subredes es 255.255.0.0

La máscara de una red **clase C** sin subredes es 255.255.255.0

En el ejemplo de subredes, la máscara es 255.255.255.0 , aunque se trate de una red clase B.

Direccionamiento IPv4.

La dirección IPV4, es jerárquica puesto que se divide en dos partes. Una porción de red y una porción de Host.

La porción de red, es aquella que define el espacio de direcciones que tendrá dicha red o subred, es la que tiene el nivel más alto de la jerarquía.

Una porción de Host es la que representa la cantidad de Host que puede tener esa red/subred, es la que tiene el nivel más bajo de la jerarquía.

Ejemplo

192.168.2.7

Entonces 192.168.2 es la porción de red

Y 7 es la porción para Host.

Como está formada una dirección IPv4

Está conformada también por una agrupación de 32 bits es decir 4 octetos.

Para hacer la distribución de red, ya no se basa en las clases A, B, C, ahora se esto se hace en función de la cantidad de Host que queremos tener en una subred. Sin embargo se presentan todas las clases a continuación.

A: Va desde 1.0.0.0 hasta 172.255.255.255

B: Va desde 172.16.0.0 hasta 192.168.0.255

C: Va desde 192.168.1.0 hasta 223.255.255.255

D: Va desde 224.0.0.0 hasta 239.255.255.255 (MULTICAST), Es un tipo de comunicación en que un Host se comunica con un Host o varios host específicos.

E. Va desde 240.0.0.0 hasta 255.255.255.255 (experimentales). Estas son direcciones que no han sido asignadas a ningún propósito.

Mascara de subred

Es una dirección que indica la máxima cantidad de Host que puede llegar a tener en una red.

Ejemplo:

255.255.255.0 hasta 256, Host esta es una máscara de subred de clase C.

El prefijo es un valor que nos indica, la cantidad de bits, usados como porción de red.

Ejemplo:

192.168.1.0/24 el 24 es la porción de red

Esto indica que tenemos una dirección de red de 192.168.1.0 y que podemos utilizar los 8 bits restantes para las direcciones de Host.

La máscara de subred y los prefijos en combinación con el sistema binario van a ser los que nos ofrecen todo el potencial de la división en subredes.

MASCARAS Y PREFIJOS PARA LAS CLASES DE IRECCIONES IPV4

CLASE	MASCARA	PREFIJO
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24

Con esto nos hacemos una idea de la cantidad de bits en cada una de las clases. Esto servirá para cuando se tenga que hacer la división en subredes. Se tienen que conocer los

diferentes bits que conforman las clases. La dirección IPv4 tiene a su vez diferentes tipos de direcciones como son:

DIRECCION DE RED: es aquella que indica la red en la que se encuentra nuestra red/subred, además es la primera dirección de la red.

DIRECCION DE BROADCAST (Difusión): es aquella que envía todo el tráfico hacia esa dirección, ésta va para todos los host, de la red/subred. Es la última dirección de red.

DIRECCION DE LOOPBACK. Es aquella que comienza por 127.0.0.1 y que nos va a permitir comprobar el funcionamiento de la interfaz física (Ethernet, FastEthernet) para comprobar si tiene algún fallo y si nos podemos conectar o no.

DIRECCIONES MULTICAST: Permite enviar paquetes a varios Host específicos siempre y cuando tengan una dirección a partir del 224.0.0.0. Permite enviar paquetes a varios Host específicos como segunda dirección IP, puesto que ya es posible tener más de dos direcciones al mismo tiempo.

DIRECCIONES UTILIZABLES. Las direcciones de red y Broadcast no se pueden asignar a un Host, puesto que son para propósitos específicos. Si se introduce una dirección de red o una dirección de Broadcast, en una dirección de host, se mostrara en pantalla un mensaje de error advirtiendo que esa dirección no se puede utilizar para Host. Entonces las direcciones utilizables son las que empiezan después de la dirección de red, y antes de la dirección de Broadcast. Es decir las que se encuentran entre la dirección de red y la de Broadcast. Esas son las que sí se pueden añadir a los host como se muestra a continuación.

192.168.1.0 **RED**
192.168.1.1
192.168.1.3
192.168.1.4
.
.
.
.
192.168.1.254
192.168.1.255 BROADCAST

Comparación entre IPv4 e IPv6.

Cuando se adoptó TCP/IP en los años 80, la versión 4 PB (IPv4) ofrecia una estrategia de direccionamiento que, aunque resulto escalable durante algún tiempo, produjo una asignación poco eficiente de las direcciones.

A mediados de los años 90 se comenzaron a detectar las siguientes dificultades sobre IPv4:

Agotamiento de las restantes direcciones de red IPv4 no asignadas. En ese entonces, el espacio de clase B estaba a punto de agotarse. Se produjo un gran y rápido aumento en el tamaño de las tablas de enrutamiento de Internet a medida que las redes Clase C se conectaban en línea. La inundación resultante de nueva información en la red amenazaba la capacidad de los Routers de Internet para ejercer una efectiva administración.

Durante las últimas dos décadas, se desarrollaron numerosas extensiones al IPv4. Estas extensiones se diseñaron específicamente para mejorar la eficiencia con la cual es posible utilizar un espacio de direccionamiento de 32 bits como VLSM y CIDR.

Mientras tanto, se ha definido y desarrollado una versión más extensible y escalable del IP, la versión 6 de IP (IPv6). Esta utiliza 128 bits en lugar de los 32 bits que en la actualidad utiliza IPv4. IPv6 utiliza números hexadecimales para representar los 128 bits. Proporciona 640 sextillones de direcciones. Esta versión del IP proporciona un número de direcciones. Esta versión del IP proporciona un número de direcciones suficientes para futuras necesidades de comunicación.

Este direccionamiento IPv6 también es conocido como IPng o IP de nueva generación. Formato de una dirección IPv6

Las direcciones IPv6 miden 128 bits y son identificadores de interfaces individuales y conjuntos de interfaces. Las direcciones IPv6 se asignan a interfaces, no a nodos. Como cada interfaz pertenece a un solo nodo, cualquiera de las direcciones unicast asignada a las interfaces del nodo se pueden usar como identificadores del nodo. Las direcciones IPv6 se escriben en hexadecimal, separadas por dos puntos. Los campos IPv6 tienen una longitud de 16 bits.

Ejemplo de una dirección IPv6:

24ae:0000:f2f3:0000:0000:0687:a2ff:6184

Para que las direcciones sean más fáciles de leer, es posible omitir los ceros iniciales de cada campo.

Enrutamiento

IP es un protocolo enrutado: esto quiere decir que si un nodo IP no alcanza a un destino determinado dentro de los segmentos de red propio, debe entregar el paquete a otro nodo que conozca al posible destino.

Para cumplir esta labor cada nodo posee una tabla de enrutamiento, que debe indicar la mejor ruta para llegar a un destino apropiado.

Los elementos de una tabla de enrutamiento se conocen como rutas. (Respectivamente route table y route en inglés.). Cuando un administrador de la red introduce manualmente las entradas de una tabla, esto se conoce como enrutamiento estático.

Para muchos enrutadores el número de rutas puede ser muy grande para utilizar rutas estáticas, adicionalmente si la red cambia, esto implicaría cambiar las rutas en muchos enrutadores. Para resolver este problema se requiere que los enrutadores intercambien información sobre sus rutas para armar sus propias tablas. Para este intercambio de información existen los protocolos de enrutamiento (routing protocols).

Algunos protocolos de enrutamiento incluyen RIP, OSPF, IGRP, EIGRP, BGP, etc.

ICMP

El protocolo de gestión de conexión de Internet, ICMP es un protocolo de red anexo a IP, y comparte varias de sus características. Su principal labor es realizar diagnósticos del estado de la red. Este es el protocolo usado por PING para enviar cargas y recibir respuesta del estado.

TCP

El protocolo de control de transmisión TCP (*Transmission Control Protocol*) es un protocolo de capa de transporte, destinado a encapsular mensajes y protocolos de capas superiores. Este protocolo es el más utilizado, tiene control de flujo, re ensamblado de paquetes y acuses de recibo. Es un protocolo orientado a conexión muy seguro que utiliza un saludo de tres vías antes del envío de los datos. En párrafos anteriores se hace una descripción más en detalle del funcionamiento TCP.

TCP es un protocolo confiable orientado a la conexión. Utiliza secuenciación y acuses de recibo periódicos para garantizar la confiabilidad.

TCP está basado en el uso de puertos lógicos para la conexión entre los nodos finales. Una sesión de TCP está unívocamente marcada en un espacio de tiempo por la dirección IP y el puerto TCP del destino y el origen.

Un puerto es un código de 16 bits. El puerto en el servidor, suele ser un indicativo del servicio (aplicación). El cliente utiliza un puerto que no esté definido en alguna norma como perteneciente a un servicio.

UDP

El protocolo de datagrama de usuario UDP (*User Datagram Protocol*) es un protocolo de capa de transporte, destinado a encapsular mensajes y protocolos de capas superiores.

UDP no es un protocolo confiable, no tiene corrección de errores y es del tipo no orientado a conexión, los datos se envían sin verificar previamente el destino y no es orientado a la conexión. Sirve como complemento a TCP para aplicaciones donde prima la velocidad y la simplicidad de la conexión sobre la confiabilidad de la misma. UDP utiliza el mismo concepto de puertos que TCP. A pesar de todo esto es muy utilizado por el bajo consumo de recurso de red. Si un puerto es TCP o UDP está determinado por el servicio.

Protocolos de aplicación

Algunos protocolos de aplicación del conjunto de protocolos TCP/IP incluyen:

Telnet

El protocolo de emulación de terminal permite intercambiar información con un servidor. Está diseñado para crear una sesión de trabajo que simula una terminal bruta; pero es la base de otros protocolos. El puerto por defecto es el 23 y trabaja con TCP.

FTP

Es protocolo de transferencia de archivos permite el intercambio de archivos, así como la consulta de archivos remotos y algunas labores de mantenimiento en el sistema de archivos del servidor remoto. Trabaja sobre TCP y utiliza los puertos 20 y 21 del servidor; para control y transferencia, respectivamente.

TFTP

El protocolo trivial de transferencia de archivos es una versión simplificada de FTP que no permite hacer mantenimiento o consultas del sistema de archivos del servidor. Trabaja con UDP en el puerto 69 del servidor.

HTTP

El protocolo de transferencia de hipertexto es el usado comúnmente por la World Wide Web para el intercambio de información. Trabaja con TCP y suele usar el puerto 80 en el servidor.

Otros protocolos

Otros protocolos de aplicación de TCP/IP incluyen: SMTP, POP3, SNMP, RADIUS, etc.

Medios LAN más comunes

En esta sesión se presentará un inventario de los medios de transmisión más utilizados desde los inicios de la implementación de redes telemáticas hasta los últimos avances en transmisión de datos tales como los de las redes inalámbricas.

STP

El cable de par trenzado blindado (STP por *Shielded Twisted Pair*) combina las técnicas de blindaje, cancelación y trenzado de cables. Cada par de hilos está envuelto en un papel metálico. Los 4 pares de hilos están envueltos a su vez en una trenza o papel metálico. Generalmente es un cable de 150.

Tal como se especifica en las instalaciones de redes *Ethernet*, el STP reduce el ruido eléctrico, tanto dentro del cable (acoplamiento par a par o diafonía) como fuera del cable (interferencia electromagnética [EMI] e interferencia de radiofrecuencia [RFI]. El cable de par trenzado blindado comparte muchas de las ventajas y desventajas del cable de par trenzado no blindado (UTP). El cable STP brinda mayor protección ante toda clase de interferencias externas, pero es más caro y es de instalación más difícil que el UTP.

Un nuevo híbrido de UTP con STP tradicional se denomina UTP blindado (ScTP), conocido también como par trenzado de papel metálico (FTP). ScTP consiste, básicamente, en cable UTP envuelto en un blindaje de papel metálico. Generalmente el cable es de 100 ó 120.

Los materiales metálicos de blindaje utilizados en STP y ScTP deben estar conectados a tierra en ambos extremos. Si no están debidamente conectados a tierra (o si existe cualquier discontinuidad en toda la extensión del material de blindaje, debido, por ejemplo, a una terminación o instalación inadecuadas), el STP y el ScTP se vuelven susceptibles a problemas de ruido, ya que permiten que el blindaje funcione como una antena que recibe señales no deseadas. (Urueña, 2007).

Sin embargo, este efecto funciona en ambos sentidos. El papel metálico (blindaje) no sólo impide que las ondas electromagnéticas entrantes produzcan ruido en los cables de datos, sino que mantiene en un mínimo la radiación de ondas electromagnéticas salientes, que de otra manera pueden producir ruido en otros dispositivos. Los cables

STP y ScTP no pueden tenderse sobre distancias tan largas como las de otros medios para networking (tales como cable coaxial y fibra óptica) sin que se repita la señal. El uso de aislamiento y blindaje adicionales aumenta de manera considerable el tamaño, peso y costo del cable.

Además, los materiales de blindaje hacen que las terminaciones sean más difíciles y aumentan la probabilidad de que se produzcan defectos de mano de obra.

El cable par trenzado se maneja por categorías de cable y ésta ha sido su evolución:

Categoría 1: Cable de par trenzado sin apantallar, se adapta para los servicios de voz, pero no a los datos.

Categoría 2: Cable de par trenzado sin apantallar, este cable tiene cuatro pares trenzados y está certificado para transmisión de 4 Mbps.

Categoría 3: Cable de par trenzado que soporta velocidades de transmisión de 10 Mbps de Ethernet 10Base-T, la transmisión en una red Token Ring es de 4 Mbps. Este cable tiene cuatro pares.

Categoría 4: Cable par trenzado certificado para velocidades de 16 Mbps. Este cable tiene cuatro pares.

Categoría 5: Es un cable de cobre par trenzado de cuatro hilos de 100 OHMIOS. La transmisión de este cable puede ser a 100 Mbps para soportar tecnologías como ATM (Asynchronous Transfer Mode).

Existen varias opciones para el estándar 802,3 que se diferencian por velocidad, tipo de cable y distancia de transmisión.

10Base-T: Cable de par trenzado con una longitud aproximada de 500 mts, a una velocidad de 10 Mbps.

1Base-5: Cable de par trenzado con una longitud extrema de 500 mts, a una velocidad de 1 Mbps.

100Base-T: (Ethernet Rápida) Cable de par trenzado, nuevo estándar que soporta velocidades de 100 Mbps que utiliza el método de acceso CSMA/CD.

100VG AnyLan: Nuevo estándar Ethernet que soporta velocidades de 100 Mbps utilizando un nuevo método de acceso por prioridad de demandas sobre configuraciones de cableado par trenzado. (Urueña, 2007).

UTP

El cable de par trenzado no blindado (UTP por *Unshielded Twisted Pair*) es un medio compuesto por cuatro pares de hilos, que se usa en diversos tipos de redes. Cada uno de los 8 hilos de cobre individuales del cable UTP está revestido de un material aislador. Además, cada par de hilos está trenzado. Este tipo de cable se basa sólo en el efecto de cancelación que producen los pares trenzados de hilos para limitar la degradación de la señal que causan la EMI y la RFI. Para reducir aún más la diafonía entre los pares en el cable UTP, la cantidad de trenzados en los pares de hilos varía. Al igual que el cable STP, el cable UTP debe seguir especificaciones precisas con respecto a cuanto trenzado se permite por unidad de longitud del cable.

Cuando se usa como medio de networking, el cable UTP tiene cuatro pares de hilos de cobre de calibre 22 ó 24. El UTP que se usa como medio de networking tiene una impedancia de 100. Esto lo diferencia de los otros tipos de cables de par trenzado como, por ejemplo, los que se utilizan para el cableado telefónico. El hecho de que el cable UTP tiene un diámetro externo pequeño (aproximadamente 0,43 cm), puede ser ventajoso durante la instalación. Como el UTP se puede usar con la mayoría de las principales arquitecturas de networking, su popularidad va en aumento.

El cable de par trenzado no blindado presenta muchas ventajas. Es de fácil instalación y es más económico que los demás tipos de medios para networking. De hecho, el cable UTP cuesta menos por metro que cualquier otro tipo de cableado de LAN, sin embargo, la ventaja real es su tamaño. Debido a que su diámetro externo es tan pequeño, el cable UTP no llena los conductos para el cableado tan rápidamente como sucede con otros tipos de cables. Este puede ser un factor sumamente importante para tener en cuenta, en especial si se está instalando una red en un edificio antiguo. Además, si se

está instalando el cable UTP con un conector RJ, las fuentes potenciales de ruido de la red se reducen enormemente y prácticamente se garantiza una conexión sólida y de buena calidad.

El cableado de par trenzado presenta ciertas desventajas. El cable UTP es más susceptible al ruido eléctrico y a la interferencia que otros tipos de medios para networking y la distancia que puede abarcar la señal sin el uso de repetidores es menos para UTP que para los cables coaxiales y de fibra óptica. En una época el cable UTP era considerado más lento para transmitir datos que otros tipos de cables. Sin embargo, hoy en día ya no es así. De hecho, en la actualidad, se considera que el cable UTP es el más rápido entre los medios basados en cobre.

Cable coaxial

El cable coaxial está compuesto por dos elementos conductores. Uno de estos elementos (ubicado en el centro del cable) es un conductor de cobre, el cual está rodeado por una capa de aislamiento flexible. Sobre este material aislador hay una malla de cobre tejida o una hoja metálica que actúa como segundo alambre del circuito, y como blindaje del conductor interno. Esta segunda capa, o blindaje, ayuda a reducir la cantidad de interferencia externa. Este blindaje está recubierto por la envoltura del cable.

Para las LAN, el cable coaxial ofrece varias ventajas. Se pueden realizar tendidos entre nodos de red a mayores distancias que con los cables STP o UTP, sin que sea necesario utilizar tantos repetidores. Los repetidores reamplifican las señales de la red de modo que puedan abarcar mayores distancias. El cable coaxial es más económico que el cable de fibra óptica y la tecnología es sumamente conocida. Se ha usado durante muchos años para todo tipo de comunicaciones de datos. ¿Se le ocurre algún otro tipo de comunicación que utilice cable coaxial?

Al trabajar con cables, es importante tener en cuenta su tamaño. A medida que aumenta el grosor, o diámetro, del cable, resulta más difícil trabajar con él. Debe tener en cuenta que el cable debe pasar por conductos y cajas existentes cuyo tamaño es limitado. El cable coaxial viene en distintos tamaños. El cable de mayor diámetro se especificó para su uso como cable de backbone de Ethernet porque históricamente siempre poseyó mejores características de longitud de transmisión y limitación del ruido.

Este tipo de cable coaxial frecuentemente se denomina *thicknet* o red gruesa. Como su apodo lo indica, debido a su diámetro, este tipo de cable puede ser demasiado rígido como para poder instalarse con facilidad en algunas situaciones. La regla práctica es: "cuanto más difícil es instalar los medios de red, más cara resulta la instalación." El cable coaxial resulta más costoso de instalar que el cable de par trenzado. Hoy en día el cable thicknet casi nunca se usa, salvo en instalaciones especiales.

En el pasado, un cable coaxial con un diámetro externo de solamente 0,35 cm (a veces denominado thinnet (red fina)) se usaba para las redes Ethernet. Era particularmente útil para instalaciones de cable en las que era necesario que el cableado tuviera que hacer muchas vueltas. Como la instalación era más sencilla, también resultaba más económica. Por este motivo algunas personas lo llamaban cheapernet (red barata). Sin embargo, como el cobre exterior o trenzado metálico del cable coaxial comprende la mitad del circuito eléctrico, se debe tener un cuidado especial para garantizar su correcta conexión a tierra. Esto se hace asegurándose de que haya una sólida conexión eléctrica en ambos extremos del cable. Sin embargo, a menudo, los instaladores omiten hacer esto. Como resultado, la conexión incorrecta del material de blindaje constituye uno de los problemas principales relacionados con la instalación del cable coaxial. Los problemas de conexión resultan en ruido eléctrico que interfiere con la transmisión de señales sobre los medios de red. Es por este motivo que, a pesar de su diámetro pequeño, thinnet ya no se utiliza con tanta frecuencia en las redes Ethernet.

Fibra óptica

El cable de fibra óptica es un medio de networking que puede conducir transmisiones de luz moduladas. Si se compara con otros medios para networking, es más caro, sin embargo, no es susceptible a la interferencia electromagnética y ofrece velocidades de datos más altas que cualquiera de los demás tipos de medios para networking descritos aquí. El cable de fibra óptica no transporta impulsos eléctricos, como lo hacen otros tipos de medios para networking que usan cables de cobre. Más bien, las señales que representan a los bits se convierten en haces de luz. Aunque la luz es una onda electromagnética, la luz en las fibras no se considera inalámbrica ya que las ondas electromagnéticas son guiadas por la fibra óptica. El término " inalámbrico" se reserva para las ondas electromagnéticas irradiadas, o no guiadas.

La comunicación por medio de fibra óptica tiene su origen en varias invenciones del siglo XIX. Sin embargo, el uso de la fibra óptica para comunicaciones no era factible hasta la década de 1960, cuando se introdujeron por primera vez fuentes de luz láser de estado sólido y materiales de vidrio de alta calidad sin impurezas. Las promotoras del uso generalizado de la fibra óptica fueron las empresas telefónicas, quienes se dieron cuenta de los beneficios que ofrecía para las comunicaciones de larga distancia.

El cable de fibra óptica que se usa en networking está compuesto por dos fibras envueltas en revestimientos separados. Si se observa una sección transversal de este cable, veremos que cada fibra óptica se encuentra rodeada por capas de material amortiguador protector, normalmente un material plástico como Kevlar, y un revestimiento externo. El revestimiento exterior protege a todo el cable. Generalmente es de plástico y cumple con los códigos aplicables de incendio y construcción. El propósito del Kevlar es brindar una mayor amortiguación y protección para las frágiles fibras de vidrio que tienen el diámetro de un cabello. Siempre que los códigos requieran que los cables de fibra óptica deban estar bajo tierra, a veces se incluye un alambre de acero inoxidable como refuerzo.

Las partes que guían la luz en una fibra óptica se denominan núcleo y revestimiento. El núcleo es generalmente un vidrio de alta pureza con un alto índice de refracción.

Cuando el vidrio del núcleo está recubierto por una capa de revestimiento de vidrio o de plástico con un índice de refracción bajo, la luz se captura en el núcleo de la fibra. Este proceso se denomina reflexión interna total y permite que la fibra óptica actúe como un "tubo de luz", guiando la luz a través de enormes distancias, incluso dando vuelta en codos.

Comunicación inalámbrica

Las señales inalámbricas son ondas electromagnéticas que pueden recorrer el vacío del espacio exterior y medios tales como el aire. Por lo tanto, no es necesario un medio físico para las señales inalámbricas, lo que hace que sean un medio muy versátil para el desarrollo de redes.

Puede resultarle sorprendente el hecho de que, a pesar de que todas las ondas (ondas de potencia, ondas de radio, microondas, ondas de luz infrarroja, ondas de luz visible, ondas de luz ultravioleta, rayos X y rayos gamma) parecen ser muy distintas, todas comparten algunas características muy importantes:

1. Todas estas ondas tienen un patrón energético similar.

2. Todas estas ondas viajan a la velocidad de la luz, c = 2990792,458 metros por segundo, en el vacío. Para ser más precisos, esta velocidad podría denominarse velocidad de las ondas electromagnéticas.

3. Todas estas ondas cumplen con la ecuación f = λ c. Donde f es la frecuencia y λ la longitud de onda.

4. Todas estas ondas viajan por el vacío. Sin embargo, interactúan de manera muy diferente con los distintos materiales.

La diferencia principal entre las distintas ondas electromagnéticas es la frecuencia. Las ondas electromagnéticas de baja frecuencia tienen una longitud de onda larga (la distancia entre un pico de la onda sinusoidal y el siguiente pico), mientras que las ondas electromagnéticas de alta frecuencia tienen una longitud de onda corta.

Una aplicación común de la comunicación inalámbrica de datos es la que corresponde a los usuarios móviles. Algunos ejemplos de usuarios móviles incluyen:

- Los pasajeros de automóviles o aviones
- Los satélites
- Las sondas espaciales remotas
- Los transbordadores espaciales y las estaciones espaciales
- Cualquier persona/cualquier cosa/cualquier lugar/cualquier momento que requiera comunicaciones de datos de red.
- Comunicaciones independientes del uso de cables de cobre o la fibra óptica

Otra aplicación común de las comunicaciones de datos inalámbricas son las LAN inalámbricas (WLAN), que se desarrollan según los estándares IEEE 802.11. Las WLAN normalmente utilizan ondas de radio (por ejemplo, 902MHz), microondas (por ejemplo, 2,4 GHz) y ondas infrarrojas (por ejemplo, 820nm) para las comunicaciones. Las tecnologías inalámbricas son cada vez más una parte fundamental de las redes.

Especificaciones y terminación de cables

Con el vertiginoso crecimiento del campo de networking, especialmente en el ámbito empresarial, se tornó cada vez más difícil la comunicación entre redes que usaban distintas especificaciones e implementaciones. Una organización llamada Organización Internacional de normalización (ISO), realizó una investigación de diversos tipos de redes y creó un modelo de red, denominado modelo OSI.

El modelo se creó con el fin de ayudar a los fabricantes a desarrollar redes que funcionaran de forma compatible e interoperable. Al crear el modelo de referencia OSI, la ISO proporcionó a los fabricantes una serie de estándares que permite a los fabricantes ofrecer elementos de red que no causen inconvenientes al momento de su instalación.

Propósito de las especificaciones de los medios LAN

A mediados de la década de 1980, comenzaron a surgir los primeros problemas causados por la expansión en el campo de networking, especialmente en el caso de las empresas que habían implementado varias tecnologías de red distintas. Se tornó cada vez más difícil la comunicación entre redes que usaban distintas especificaciones e implementaciones. Una organización llamada Organización internacional de normalización (ISO), realizó una investigación de diversos tipos de redes y creó un modelo de red, denominado modelo de referencia OSI. (Nota: No se debe confundir el nombre del modelo (OSI) con el nombre de la organización (ISO). El modelo se creó para ayudar a los fabricantes a desarrollar redes que funcionaran de forma compatible e interoperable. Al crear el modelo OSI, la ISO proporcionó a los fabricantes un conjunto de estándares.

Los estándares son conjuntos de normas o procedimientos de uso generalizado, o que se especifican oficialmente, y que sirven como medida o modelo de excelencia. Los estándares del modelo OSI aseguraban la compatibilidad e interoperabilidad entre los distintos tipos de tecnologías de red producidas por diversas empresas a nivel mundial. En su mayoría los primeros estándares que se desarrollaron para los medios de networking eran propietarios. Se desarrollaron para que los utilizaran diversas empresas. Con el tiempo, muchas otras organizaciones y entidades gubernamentales se unieron al movimiento para regular y especificar cuáles eran los tipos de cables que se podían usar para fines o funciones específicos. Hasta hace poco tiempo, ha existido una mezcla algo confusa de estándares que regían los medios para networking. Dichos estándares variaban desde los códigos de construcción e incendios hasta especificaciones eléctricas detalladas. Otros estándares han especificado pruebas para garantizar la seguridad y el rendimiento.

Cuando empiece a diseñar y desarrollar redes, debe asegurarse de que cumplan todos los códigos contra incendios, de construcción y de seguridad aplicables. Debe seguir cualquier estándar de rendimiento establecido para asegurar el funcionamiento óptimo de la red y para asegurar la compatibilidad y la interoperabilidad de los diversos medios para networking disponibles en la actualidad. En este currículum sus esfuerzos se enfocarán en las normas desarrolladas y publicadas por los siguientes grupos para regir los medios de red:

- IEEE: Instituto de ingenieros eléctricos y electrónicos
- (IEEE) UL: Underwriters Laboratories
- nEIA - Asociación de Industrias Electrónicas
- TIA - Asociación de la Industria de las Telecomunicaciones

Las dos últimas organizaciones, de forma conjunta, publican una lista de estándares que frecuentemente se denominan estándares TIA/EIA. Además de estos grupos y organizaciones, las entidades gubernamentales locales, estatales, de distrito y nacionales publican especificaciones y requisitos que pueden tener efecto sobre el tipo de cableado que se puede usar en una red de área local.

El IEEE ha descrito los requisitos de cableado para los sistemas Ethernet y Token Ring en las especificaciones 802.3 y 802.5 y los estándares para FDDI. Underwriters Laboratories publica especificaciones de cableado que se ocupan principalmente de las normas de seguridad, sin embargo, también evalúan el rendimiento de los medios para networking de par trenzado. Underwriters Laboratories estableció un programa de identificación que enumera los requisitos para los medios de networking de par trenzado blindado y no blindado cuyo objetivo es simplificar la tarea de asegurar que los materiales que se usan en la instalación de una LAN cumplan con las especificaciones.

Normas TIA/EIA

De todas las organizaciones mencionadas aquí, TIA/EIA es la que ha causado el mayor impacto sobre los estándares de los medios para networking. Específicamente, TIA/EIA- 568-A y TIA/EIA-569-A, han sido y continúan siendo los estándares más ampliamente utilizados para determinar el rendimiento de los medios para networking.

Las normas TIA/EIA especifican los requisitos mínimos para los entornos compuestos por varios productos diferentes, producidos por diversos fabricantes. Estas normas tienen en cuenta la planificación e instalación de sistemas de LAN sin imponer el uso de equipo específico, y, de ese modo, ofrecen a los diseñadores de las LAN la libertad de crear opciones con fines de perfeccionamiento y expansión.

Explicación de los detalles de los estándares TIA/EIA-568-

Los estándares TIA/EIA se refieren a seis elementos del proceso de cableado de LAN. Ellos son:

- Cableado horizontal
- Centros de telecomunicaciones
- Cableado backbone
- Salas de trabajo

- Facilidades de acceso.

Esta lección se concentra en los estándares TIA/EIA-568-A para el cableado horizontal, que definen el cableado horizontal como el cableado tendido entre una toma de telecomunicaciones y una conexión cruzada horizontal. TIA/EIA- 568-A incluye los medios para networking que están tendidos a lo largo de una ruta horizontal, la toma o conector de telecomunicaciones, las terminaciones mecánicas de centro de cableado y los cables de conexión o jumpers del centro de cableado. En resumen, el cableado horizontal incluye los medios para networking que se usan en el área que se extiende desde el centro de cableado hasta una estación de trabajo.

Los medios para networking reconocidos para estas categorías son los que ya se han estudiado:

- Par trenzado blindado
- Par trenzado no blindado
- Cable de fibra óptica
- Cable coaxial

Para el cable de par trenzado blindado, el estándar TIA/EIA-568-A establece el uso de cable de dos pares de 150 ohmios. Para cables de par trenzado no blindado, el estándar establece cables de cuatro pares de 100 ohmios. Para fibra óptica, el estándar establece dos fibras de cable multimodo 62.5/125µm. Aunque el cable coaxial de 50 es un tipo de medio para networking reconocido en TIA/EIA-568B, su uso no se recomienda para instalaciones nuevas. Es más, se prevé que este tipo de cable coaxial sea eliminado de la lista de medios para networking reconocidos durante la próxima revisión del estándar.

Para el componente de cableado horizontal, TIA/EIA-568A requiere un mínimo de dos tomas o conectores de telecomunicaciones en cada área de trabajo. Esta toma o conector de telecomunicaciones admite dos cables. El primero es un cable UTP de cuatro pares de 100 ohmios CAT 3 o superior, junto con su conector apropiado. El segundo puede ser cualquiera de los siguientes:

- Cable de par trenzado no blindado de cuatro pares de 100 ohmios y su conector apropiado.

- Cable de par tranzado blindado de 150 ohmios y su conector apropiado
- Cable coaxial y su conector apropiado
- Cable de fibra óptica de dos fibras de (62,5))µ y su conector apropiado.

Según TIA/EIA-568-A, la distancia máxima para los tendidos de cable en el cableado horizontal es 90 metros (m). Esto es aplicable para todos los tipos de medio de networking de UTP CAT 5 reconocidos. El estándar también específica que los cables de conexión o jumpers de conexión cruzada (cross-connect) ubicados en la conexión cruzada horizontal no deben superar los 6 metros de longitud. TIA/EIA-568-A también permite 3 m de cables de conexión utilizados para conectar los equipos en el área de trabajo. La longitud total de los cables de conexión y de los jumpers de conexión cruzada utilizados en el cableado horizontal no puede superar los 10 m. Una especificación final mencionada por TIA/EIA-568-A para el cableado horizontal establece que todas las uniones y conexiones a tierra deben adecuarse a TIA/EIA-607 así como a cualquier otro código aplicable.

Los últimos estándares industriales, actualmente, son el cableado Cat 5e, Cat 6 y Cat 7, todos los cuales son perfeccionamientos de Cat 5.

Se recomiendan los siguientes links para ampliar temática, y actualizar conceptos:

- http://fmc.axarnet.es/redes/tema_02.htm.
- http://materias.fi.uba.ar/6679/apuntes/CABLEADO_ESTRUC.pdf.
- http://multimedia.mmm.com/mws/mediawebserver.dyn?TTTTTTB_LdgTmwUTfwUTTtC88DPssss r- Consultados 23/09/11.

Medios para networking y terminaciones

Eventualmente los cables deben terminarse para proporcionar la conectividad. Este proceso involucra una gran transición e innovación en lo que respecta al networking informático. Esto representa un gran desafío para los estudiantes, que deben aprender una amplia variedad de estándares, propiedades y terminaciones de medios para networking.

Componentes y dispositivos de capa física

Ethernet 10Base-T

En este currículum, se presentarán tres tecnologías LAN: Ethernet, Token Ring y FDDI. Las tres tienen una amplia variedad de componentes y dispositivos de Capa 1. Se hará referencia a las tecnologías Ethernet 10BASE-T.

El diseño original de Ethernet representaba un punto medio entre las redes de larga distancia y baja velocidad y las redes especializadas de las salas de computadores, que transportaban datos a altas velocidades a distancias muy limitadas. Ethernet se adecua bien a las aplicaciones en las que un medio de comunicación local debe transportar tráfico esporádico y ocasionalmente pesado, a velocidades de datos muy elevadas.

Las tecnologías Ethernet 10BASE-T transportan tramas Ethernet en cableado de par trenzado de bajo costo. Usted estudiará cuatro componentes y tres dispositivos que se relacionan con estas tecnologías. Los primeros cuatro componentes son pasivos, lo que significa que no requieren energía para funcionar.

Son las siguientes:

- Paneles de conexión
- Conectores
- Cableado
- Jacks

Los últimos tres son activos. Necesitan energía para ejecutar sus tareas. Son las siguientes:

- Transceivers
- Repetidores
- Hubs

Para más información sobre evolución de Ethernet en general puedes consultar: http://www.alfinal.com/Temas/ethernetevo.php. Consultado el 23/9/11.

Otros componentes y dispositivos Ethernet, Token Ring y FDDI, recomendamos al sitio Web: http://www.lcc.uma.es/~eat/services/fddi/fddi.htm. Consultado 23/9/11

Conectores

La terminación estándar de 10BASE-T (punto de terminación) es el conector "Registered Jack-45" (RJ-45). Este conector reduce el ruido, la reflexión y los problemas de estabilidad mecánica y se asemeja al conector telefónico, con la diferencia de que tiene ocho conductores en lugar de cuatro. Se considera como un componente de networking pasivo ya que sólo sirve como un camino conductor entre los cuatro pares del cable trenzado de Categoría 5 y las patas de la toma RJ-45. Se considera como un componente de Capa 1, más que un dispositivo, dado que sirve sólo como camino conductor para bits.

Cableado

El cableado podemos definirlo como una serie de circuitos interconectados de forma permanente para llevar a cabo una función específica. Suele hacer referencia al conjunto de cables utilizados para formar una red de área local. (Urueña 2007).

La necesidad de redes locales de alta velocidad son resultado directo de la adopción universal de las mismas como elemento clave para el incremento de la productividad y la comunicación en todos los campos de la vida actual, y de la disponibilidad de nuevas aplicaciones que generan cada vez más tráfico en dichas redes.

El incremento de prestaciones y de capacidad de los ordenadores personales, así como la disponibilidad de periféricos exequibles de alta resolución, han propulsado el desarrollo de aplicaciones muy exigentes en cuanto al tráfico de datos, como entornos IGU, CAD, proceso de imágenes, gestión documental, multimedia, videoconferencia, etc.

La tecnología Ethernet, desde su invención en el año 1973, ha evolucionado continuamente para adaptarse a los nuevos requerimientos del mercado. Como respuesta a dicha evolución, en el año 1992, Grand Junction Networks anuncio la disponibilidad de los primeros productos "Fast Ethernet" (denominados en su momento 100 base-X), esto es Ethernet adaptada a una velocidad de 100Mbps.

Desde ese momento, ha ido aumentando el soporte de dicha especificación por un numeroso grupo de fabricantes que han comercializado una cantidad de dispositivos interoperables.

Esta tecnología fue normalizada en el año 1994, por un grupo de estudio de IEEE 802.3, creado inicialmente en torno a 100Base-X, siendo bautizada formalmente como 100-BaseT

100Base-T permite multiplicar por 10 veces la velocidad de las redes Ethernet, y al igual que en el caso de 10Base-T, puede emplear cableado de par trenzado no apantallado (UTP), puede emplear cableados de par trenzado no apantallado (UTP), y apantallado (STP), con longitudes de hasta 100 mts, en topología de estrella, partiendo de un concentrado o repetidor central.

Al igual que las diferentes versiones de la tecnología Ethernet, 100Base-T cumple la especificación clave que define las mismas: CSMA/CD.

El comité 802.3 cuidó los detalles de definición de la norma, especificando la capa MAC de un modo independiente a la velocidad. Exceptuando el tramo entre paquetes, todos los parámetros de la capa MAC fueron definidos en bits respecto del tiempo. Ello permite la variación de la velocidad sin alterar los parámetros MAC, por lo que CSMA/CD funciona a 1 Mbps. (1Base5), 10 Mbps (redes Ethernet actuales y 100 Mbps. (Fast Ethernet o 100Base-T).

La segunda parte del protocolo Ethernet es la capa física (Thy O Phisical Layer), que se ocupa de la comunicación entre la capa MAC y el cableado. En el caso de Ethernet existen diferentes implementaciones de la capa física, dadas las diferentes posibilidades de cableado (10Base5, 10Base2, 10Broad36, 10Base-F, 10Base-T y 1Base5), pero en todos los casos se emplea el mismo MAC CSMA/CD.

La capa física es responsable tanto de obtener los datos (bits) del medio como de situarlos en el mismo, incluyendo las funciones de codificación y descodificación, detección de la portadora, detección de colisiones e interfaz eléctrica y mecánica con el medio.

Por otra parte el cable 10BASE-T estándar es un cable CAT 5 de par trenzado, que está formado por cuatro pares trenzados que reducen los problemas de ruido. El cable CAT 5 es delgado, económico y de fácil instalación. La función del cable CAT 5 es transportar bits, por lo tanto, es un componente de Capa 1.

Dado que la velocidad de 100Mbps empleada en 100Base –T era la misma que la empleada en las redes FDDI, se hizo necesario intentar el uso de la capa física, del mismo modo que se había empleado en las redes FDDI con cableado UTP (categoria5) o STP (tipo 1).

Para la codificación, en lugar de seguir el esquema Manchester, como en el caso de Ethernet, en FDDI se optó por MLT-3 (multilevel threshold empleando niveles lógicos de +1, 0 y -1 voltios). Sin embargo, para 100Base-T se ha optado por seguir NRZI, al igual que en el caso de ATM.

Tanto en FDDI como en 100Base-Tx y 100Base-FX, se emplea una codificación 4B/5B para la compresión de los datos.

El sistema de señalización que permite alcanzar altas velocidades a través de cableados UTP, fuer normalizado en 1992, como NSI X3T.5 y se denomina TP-PMD (Twisted Pair Physical Medium Dependent).

Como en el caso de CSMA/CD, la capa ANSI PMD es un estándar bien conocido y soporta tanto cableado UTP de categoría 5, como fibra óptica y cable apantallado de tipo 1.

Jacks

Los conectores RJ-45 se insertan en jacks o receptáculos RJ-45. Los jacks RJ- 45 tienen 8 conductores, que se ajustan a los del conector RJ-45. En el otro lado del jack RJ-45 hay un bloque de inserción donde los hilos individuales se separan y se introducen en ranuras mediante una herramienta similar a un tenedor denominada herramienta de

punción. Esto suministra un camino conductor de cobre para los bits. El jack RJ-45 es un componente de Capa 1.

Paneles de conexión

Los paneles de conexión son jacks RJ-45 agrupados de forma conveniente. Vienen provistos de 12, 24 ó 48 puertos y normalmente están montados en un bastidor. Las partes delanteras son jacks RJ-45, y las partes traseras son bloques de punción que proporcionan conectividad o caminos conductores. Se clasifican como dispositivos de Capa 1.

Transceivers (transceptores).

Un transceiver es una combinación de transmisor y receptor. En las aplicaciones de networking, esto significa que convierten una forma de señal en otra. Por ejemplo, varios dispositivos de networking traen una interfaz de unidad auxiliar y un transceiver para permitir que 10Base2, 10Base5, 10BaseT o 10/100Base-FX se conecten con el puerto. Una aplicación común es la conversión de puertos AUI en puertos RJ-45. Estos son dispositivos de Capa 1. Transmiten de una configuración de pin y/o medio a otra. Los Transceivers a menudo se incorporan a las NIC, que se consideran normalmente como dispositivos de Capa 2. Los Transceivers de las NIC se denominan componentes de señalización, lo que significa que codifican señales en un medio físico. (Daza, 2009).

Los Transceivers son utilizados para conectar nodos a varios medios Ethernet. La mayoría de las computadoras y placas de interfaz de red poseen un transceiver 10BASE-T o 10BASE2 incorporado ("built-in"), permitiéndoles conectarse directamente al medio Ethernet sin la necesidad de un transceiver externo.

Muchos dispositivos Ethernet compatibles proveen un conector AUI, el cual permite al usuario conectarse a cualquier tipo de medio vía un transceiver externo.

El conector AUI consiste en un conector (hembra del lado de la PC y macho del lado del transceiver) de 15 pines tipo D-shell.

Cables Thickwire o ThickEthernet (10BASE5) también utilizan Transceivers para permitir conexiones.Para redes fast Ethernet, una nueva interfaz llamada MII (Interfaz Medio Independiente o "Media Independent Interface") fue desarrollada para ofrecer un modo flexible de soportar conexiones de 100 Mbps. La MII es un modo bastante difundido de conectar vínculos 100BASE-FX a dispositivos Fast Ethernet basados en cobre. Entre los componentes de un cableado con cable grueso se incluyen:

Transceivers

Se trata de dispositivos que pueden enviar y recibir, proporcionar comunicación entre el equipo y el cable principal de la LAN, y están situados en las conexiones de los vampiros sobre el cable.

- Cables de transceiver. El cable que conecta el transceiver a la NIC.
- Conectores DIX (o AUI). Estos son los conectores del cable del transceiver.
- Conectores serie, incluyendo N conectores de barril y N terminales serie.

Los componentes del cable grueso funcionan de la misma forma que los componentes del cable fino.

AUI son unas siglas que significan Interfaz de conexión de unidad y es un conector de 15 pines (DB-15) que se suele utilizar para conectar una tarjeta de red a un cable Ethernet.

Multitransceivers

Son Transceivers que permiten la conexión de más de un equipo a la red en el mismo sitio, es decir, tienen varias salidas para equipos.

Multiport-transceivers

Son equipos que van conectados a un transceiver y que tienen varias puertas de salida para equipos. La única limitación que tienen es que mediante estos equipos no se pueden interconectar equipos que conecten redes entre sí.

Repetidores

Los repetidores regeneran y retemporizan las señales, lo que permite entonces que los cables se extiendan a mayor distancia. Solamente se encargan de los paquetes a nivel de los bits, por lo tanto, son dispositivos de Capa 1.

Los repetidores son dispositivos de internetworking que existen en la capa física (la Capa 1) del modelo OSI. Pueden aumentar la cantidad de nodos que se pueden conectar a una red y, como consecuencia, la distancia a la cual se puede extender una red. Los repetidores modifican la forma, regeneran y retemporizan las señales antes de enviarlas por la red.

La desventaja del uso de repetidores es que no pueden filtrar el tráfico de red. Los datos (bits) que llegan a uno de los puertos del repetidor se envían a todos los demás puertos. Los datos se transfieren a todos los demás segmentos de la LAN sin considerar si deben dirigirse hacia allí o no. (Dazq, 2007).

Repetidores multipuerto (hubs)

Los repetidores multipuerto combinan las propiedades de amplificación y de retemporización de los repetidores con la conectividad. Es normal que existan 4, 8, 12 y hasta 24 puertos en los repetidores multipuerto. Esto permite que varios dispositivos se interconecten de forma económica y sencilla. Los repetidores multipuerto a menudo se llaman hubs, en lugar de repetidores, cuando se hace referencia a los dispositivos que sirven como centro de una red de topología en estrella. Los hubs son dispositivos de internetworking muy comunes.

Dado que el hub típico “no administrado” simplemente requiere alimentación y jacks RJ-45 conectados, son excelentes para configurar una red con rapidez. Al igual que los repetidores en los que se basan, sólo manejan bits y son dispositivos de Capa 1.

Componentes y dispositivos de Capa 1 del modelo OSI

Todos estos dispositivos (pasivos y activos) crean o actúan sobre bits. No reconocen patrones de información en los bits, ni direcciones, ni datos. Su función es simplemente transportar los bits. La Capa 1 es fundamental en el diagnóstico de fallas de las redes y su importancia no debe subestimarse. Muchos de los problemas de la red pueden deberse a malas inserciones o terminaciones RJ-45, o a jacks, repetidores, hubs o transceivers dañados o que funcionan mal.

Recomendamos consultar el siguiente link para complementar:

http://fmc.axarnet.es/redes/tema_03.htm (consultado el 25 de sept/2011).

Consultar el siguiente link: http://www.telepieza.com/wordpress/2008/03/09/los-diferentes-dispositivos-de-conexion-en-redes-repetidor-hub-bridge-switch-router-y-gateway/