

Arquitectura de Redes

Para reducir la complejidad en el diseño de las redes, muchas de ellas están organizadas en capas o niveles, cada una construida sobre la inferior y teniendo en cuenta la superior. El nombre, el número de capas y el contenido de las funciones de cada una de ellas es lo que se denomina una Arquitectura de Red. Sin embargo, en todas las redes, el propósito de cada capa es ofrecer ciertos servicios a la capa superior de modo que esta no tenga que ocuparse del detalle de la implementación real de los servicios. La capa n de una máquina lleva a cabo una conversación con la capa n de la otra. Las reglas y convenciones que se siguen en esta conversación se conoce con el nombre de protocolo de la capa n .

Es así como un conjunto de capas y protocolos recibe el nombre de **Arquitectura de Red**. La especificación de una arquitectura debe contener información suficiente para que un implementador pueda escribir el programa o construir el hardware para cada capa de manera que obedezca en forma correcta al protocolo apropiado.

El modelo más utilizado en la actualidad es el modelo OSI (*Open Systems Interconnect*) basado en una propuesta de la ISO (*Industry Standard Organization*) y que tiene como objetivo lograr una normalización en el tema de protocolos de redes de manera tal de poder interconectar redes de distintos protocolos que respondan a la misma normalización. Esta es la razón por la que se lo denomina **Arquitectura de sistemas abiertos**.

Problemas en el diseño de las capas

En general, hay ciertas hipótesis que se tienen en cuenta para el diseño de las capas que resumiremos a continuación:

- Se precisa un sistema de referencia para identificar emisores y receptores.
- Se debe decidir las reglas de transferencia de datos (duplex, semiduplex, número de canales lógicos, etc.)
- Se debe prestar especial atención al control de los errores, tanto a su detección como a su corrección.
- Se debe establecer un sistema de comunicación tal que el emisor pueda saber que mensajes ha recibido el receptor en forma correcta.
- Se debe establecer una manera de dividir los mensajes largos en partes y luego de transmitidos poder volver a reconstruir el mensaje original.
- Se debe incluir la medición de rutas para poder conocer la trayectoria óptima entre dos puntos.
- Se debe establecer la forma de medir el tráfico de manera de no saturar los canales.

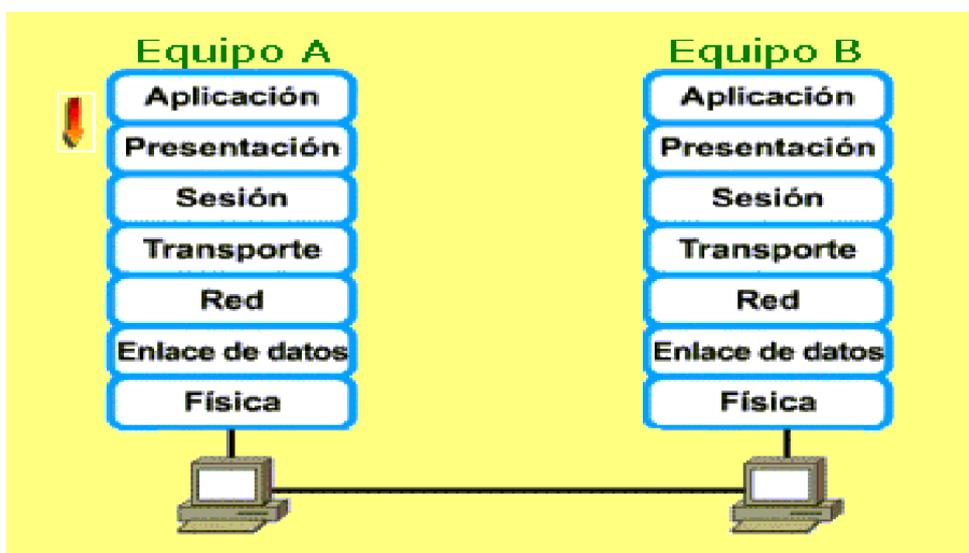
- Se debe incluir la posibilidad de establecer transmisiones coordinadas o abruptas (servicios orientados a conexión o sin conexión).

El modelo OSI

El modelo propuesto por la ISO tiene siete capas. Los principios que se aplicaron para llegar a ellas son los siguientes:

- Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.
- Cada capa debe realizar una función bien definida.
- La función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.
- Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.
- La cantidad de capas debe ser suficiente para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

Es importante hacer notar que el modelo OSI en si no es una arquitectura de red porque no especifica los servicios y protocolos exactos que se han de usar en cada capa; solo dice lo que debe hacer cada capa. Sin embargo, la ISO también ha elaborado estándares para todas las capas, aunque no sean parte del modelo de referencia mismo.



La capa Física

La capa física tiene que ver con la transmisión de bits por un canal de comunicación. Las condiciones de diseño tienen que ver con la acción de asegurarse de que cuando un lado

envíe un bit 1, se reciba del otro lado como bit 1, no como bit 0. Las consideraciones típicas de esta capa tienen que ver con el voltaje que representará un 1 y el que representará a un 0, cuantos milisegundos durará un bit, si la transmisión se puede efectuar en ambas direcciones al mismo tiempo, cuantos conectores tiene el conector del nodo, es decir, tienen que ver con las interfases mecánica, eléctrica y de procedimientos con respecto al medio de transmisión físico.

La capa de enlace de datos

La tarea principal de la capa de enlace es tomar un medio de transmisión en bruto y transformarlo en una línea que parezca libre de errores de transmisión. Puesto que la capa física solamente acepta y transmite una corriente de bits sin preocuparse por su significado o su estructura, corresponde a la capa de enlace dividir el flujo en marcos (de algunos miles de bytes normalmente) y organizar la transmisión de los mismos. También debe prever algún mecanismo de regulación de tráfico para que el transmisor no sature al receptor. En las redes de difusión se requiere una consideración adicional en la capa de enlace, se trata de un método para controlar el acceso al canal compartido; este problema se soluciona introduciendo una subcapa llamada subcapa de acceso al medio.

La capa de red

La capa de red es principalmente la capa encargada de controlar el funcionamiento de la subred, compuesta por las tres capas vistas hasta ahora. Una consideración clave de su diseño es determinar cómo se encaminan los paquetes de la fuente a su destino. Las rutas pueden ser estáticas o dinámicas. El control de la congestión pertenece también a las funciones asignadas a la capa de red. En las redes de difusión, el problema de ruteo es muy simple y por lo tanto tienen una capa de red muy delgada o hasta inexistente.

La capa de transporte

La función básica de la capa de transporte es aceptar datos de la capa de sesión (superior), dividirlos en unidades más pequeñas si es necesario, pasarlos a la capa de red y asegurar que todos los pedazos lleguen correctamente al otro extremo. Además, todo esto se debe hacer de manera eficiente y en forma que aisle a las capas superiores de los cambios inevitables en la tecnología del hardware.

En condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de transporte que requiera la capa de sesión. Sin embargo, si la conexión de transporte requiere un volumen de transmisión alto, la capa de transporte podría crear

múltiples conexiones de red, dividiendo los datos entre las conexiones para aumentar el volumen. Por otro lado, si es costoso crear o mantener una conexión de red, la capa de transporte puede multiplexar varias conexiones de transporte en la misma conexión de red para reducir el costo. En todos los casos, la capa de transporte logra que todo esto sea transparente para la capa de sesión.

La capa de transporte es una verdadera capa de extremo a extremo, es decir, un programa en la máquina fuente sostiene una conversación con un programa similar de la máquina destino. En las capas bajas, los protocolos se usan entre cada máquina y sus vecinas inmediatas, y no entre las máquinas de origen y destino, que pueden estar separadas por muchos enrutadores.

La capa de sesión

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.

Uno de los servicios de la capa de sesión es manejar el control del diálogo, es decir, se ocupa de establecer quién podrá transmitir en cada turno en el caso de las líneas semi duplex.

Otro servicio de sesión es la sincronización que sirve para evitar tener que retransmitir grandes cantidades de información ante un error.

La capa de presentación

La capa de presentación realiza ciertas funciones relacionadas con la sintaxis y la semántica de la información que se transmite. Esta capa maneja las estructuras de datos abstractas y las convierte de la representación que se usa dentro de la computadora a la representación estándar de la red y viceversa. Se ocupa de salvar las diferencias en los tipos de representación que pudieran existir entre computadoras diferentes.

La capa de aplicación

La capa de aplicación contiene varios protocolos que se necesitan con frecuencia. Uno de ellos es el protocolo de terminal virtual, otro es el de transferencia de archivos que elimina incompatibilidades entre distintos sistemas de denominación de archivos y otros como el protocolo de correo electrónico, etc.

Terminología del modelo OSI

Entidades: son los elementos activos de cada capa, puede ser hardware o software que implementa los servicios para la próxima capa.

SAP: (*Service Access Point*) son los puntos de acceso a los servicios proporcionados por cada capa. Son los lugares en los que la capa n puede tener acceso a los servicios ofrecidos por la capa n-1. Cada SAP tiene una dirección que lo identifica de manera única.

Servicio orientado a conexión: encuentra su modelo en el sistema telefónico. Para hacer uso de estos servicios, el usuario debe establecer una conexión, transmitir y luego liberar la misma.

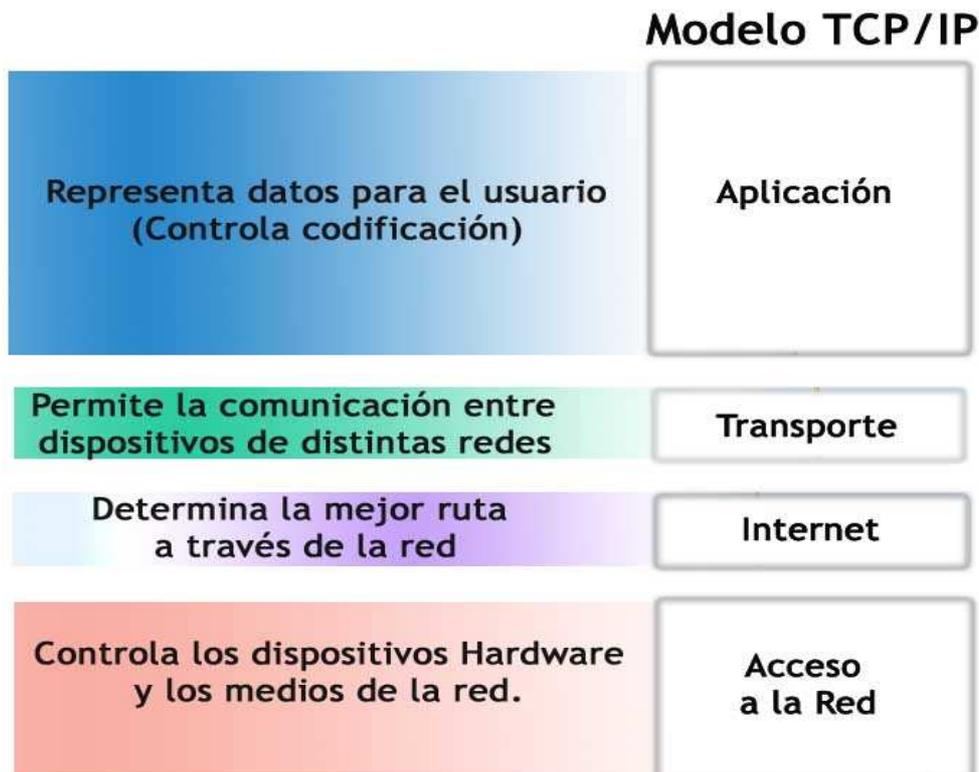
Servicios sin conexión: encuentra su modelo en el sistema postal, en el cual cada mensaje lleva la dirección del destinatario y se encamina en forma independiente.

El modelo de referencia TCP/IP

Tratemos ahora el modelo de referencia usado en la abuela de todas las redes de computadoras de área amplia, ARPANET, y en su sucesora, la Internet mundial. Aunque daremos más adelante una breve historia de ARPANET, es útil mencionar algunos de sus aspectos ahora. ARPANET fue una red de investigación respaldada por el DoD (Departamento de Defensa de Estados Unidos). Con el tiempo, conectó cientos de universidades e instalaciones gubernamentales mediante líneas telefónicas alquiladas. Posteriormente, cuando se agregaron redes satelitales y de radio, los protocolos existentes tuvieron problemas para interactuar con ellas, por lo que se necesitaba una nueva arquitectura de referencia. De este modo, la capacidad para conectar múltiples redes en una manera sólida fue una de las principales metas de diseño desde sus inicios. Más tarde, esta arquitectura se llegó a conocer como el modelo de referencia TCP/IP, de acuerdo con sus dos protocolos primarios. Su primera definición fue en (Cerf y Kahn, 1974). Posteriormente se definió en (Leiner y cols., 1985). La filosofía del diseño que respalda al modelo se explica en (Clark, 1988).

Ante el temor del DoD de que algunos de sus valiosos hosts, enrutadores y puertas de enlace de interredes explotaran en un instante, otro objetivo fue que la red pudiera sobrevivir a la pérdida de hardware de la subred, sin que las conversaciones existentes se interrumpieran. En otras palabras, el DoD quería que las conexiones se mantuvieran intactas en tanto las máquinas de origen y destino estuvieran funcionando, aunque algunas de las máquinas o líneas de transmisión intermedias quedaran fuera de operación

repentinamente. Además, se necesitaba una arquitectura flexible debido a que se preveían aplicaciones con requerimientos divergentes, desde transferencia de archivos a transmisión de palabras en tiempo real.



La capa de interred

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa de interred no orientada a la conexión. Esta capa, llamada capa de interred, es la pieza clave que mantiene unida a la arquitectura. Su trabajo es permitir que los hosts inyecten paquetes dentro de cualquier red y que éstos viajen a su destino de manera independiente (podría ser en una red diferente). Tal vez lleguen en un orden diferente al que fueron enviados, en cuyo caso las capas más altas deberán ordenarlos, si se desea una entrega ordenada. Observe que aquí el concepto “interred” se utiliza en un sentido genérico, aun cuando esta capa se presente en Internet.

Aquí la analogía es con el sistema de correo tradicional. Una persona puede depositar una secuencia de cartas internacionales en un buzón y, con un poco de suerte, la mayoría de

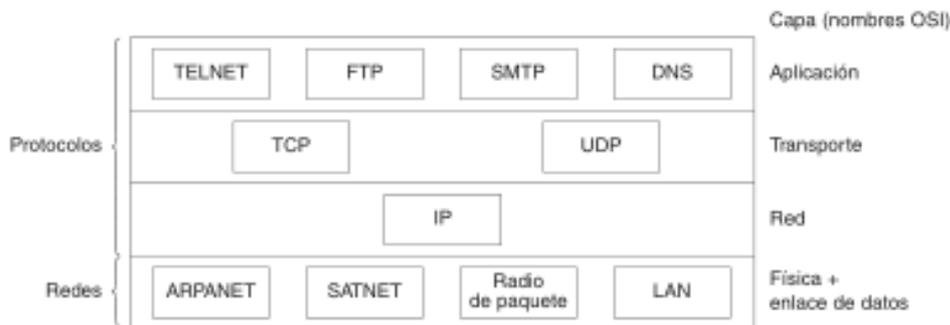
ellas se entregará en la dirección correcta del país de destino. Es probable que durante el trayecto, las cartas viajen a través de una o más puertas de enlace de correo internacional, pero esto es transparente para los usuarios. Además, para los usuarios también es transparente el hecho de que cada país (es decir, cada red) tiene sus propios timbres postales, tamaños preferidos de sobre y reglas de entrega.

La capa de interred define un paquete de formato y protocolo oficial llamado IP (Protocolo de Internet). El trabajo de la capa de interred es entregar paquetes IP al destinatario. Aquí, el enrutamiento de paquetes es claramente el aspecto principal, con el propósito de evitar la congestión. Por estas razones es razonable decir que la capa de interred del modelo TCP/IP es similar en funcionalidad a la capa de red del modelo OSI.

La capa de transporte

La capa que está arriba de la capa de interred en el modelo TCP/IP se llama capa de transporte. Está diseñada para permitir que las entidades iguales en los hosts de origen y destino puedan llevar a cabo una conversación, tal como lo hace la capa de transporte OSI. Aquí se han definido dos protocolos de transporte de extremo a extremo. El primero, TCP (Protocolo de Control de Transmisión), es un protocolo confiable, orientado a la conexión, que permite que un flujo de bytes que se origina en una máquina se entregue sin errores en cualquier otra máquina en la interred. Divide el flujo de bytes entrantes en mensajes discretos y pasa cada uno de ellos a la capa de interred. En el destino, el proceso TCP receptor reensambla en el flujo de salida los mensajes recibidos. TCP también maneja el control de flujo para asegurarse de que un emisor rápido no sature a un receptor lento con más mensajes de los que puede manejar.

El segundo protocolo de esta capa, UDP (Protocolo de Datagrama de Usuario), es un protocolo no confiable y no orientado a la conexión para aplicaciones que no desean la secuenciación o el control de flujo de TCP y que desean proporcionar el suyo. También tiene un amplio uso en consultas únicas de solicitud-respuesta de tipo cliente-servidor en un solo envío, así como aplicaciones en las que la entrega puntual es más importante que la precisa, como en la transmisión de voz o vídeo. La relación de IP, TCP y UDP se muestra en imagen siguiente. Puesto que el modelo se desarrolló, se ha implementado IP en muchas otras redes.



La capa de aplicación

El modelo TCP/IP no tiene capas de sesión ni de presentación. No se han necesitado, por lo que no se incluyen. La experiencia con el modelo OSI ha probado que este punto de vista es correcto: son de poco uso para la mayoría de las aplicaciones.

Arriba de la capa de transporte está la capa de aplicación. Contiene todos los protocolos de nivel más alto. Los primeros incluyeron una terminal virtual (TELNET), transferencia de archivos (FTP) y correo electrónico (SMTP), como se muestra en la imagen anterior. El protocolo de terminal virtual permite que un usuario en una máquina se registre en una máquina remota y trabaje ahí. El protocolo de transferencia de archivos proporciona una manera de mover con eficiencia datos de una máquina a otra. El correo electrónico era originalmente sólo un tipo de transferencia de archivos, pero más tarde se desarrolló un protocolo especializado (SMTP) para él. Con el tiempo, se han agregado muchos otros protocolos: DNS (Sistema de Nombres de Dominio) para la resolución de nombres de host en sus direcciones de red; NNTP, para transportar los artículos de noticias de USENET; HTTP, para las páginas de World Wide Web, y muchos otros.

La capa host a red

Debajo de la capa de interred hay un gran vacío. El modelo de referencia TCP/IP en realidad no dice mucho acerca de lo que pasa aquí, excepto que puntualiza que el host se tiene que conectar a la red mediante el mismo protocolo para que le puedan enviar paquetes IP. Este protocolo no está definido y varía de un host a otro y de una red a otra.

Comparación entre el modelo OSI y el TCP/IP

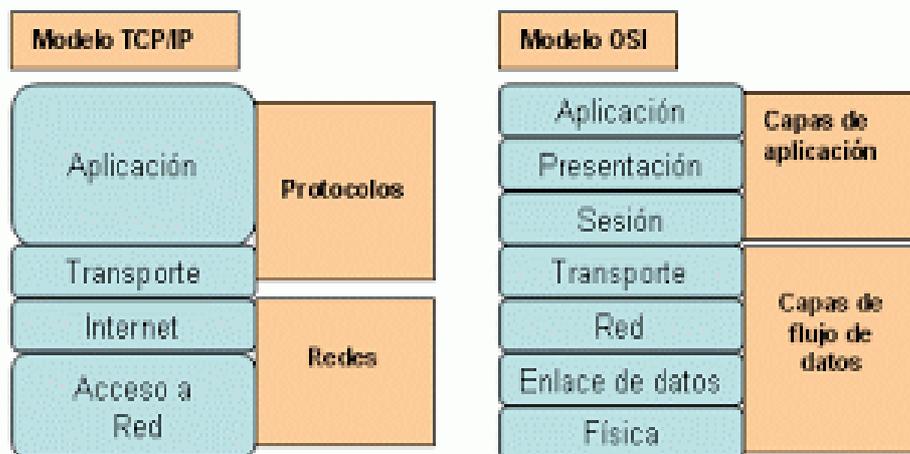
Si comparamos el modelo OSI y el modelo TCP/IP, observamos que ambos presentan similitudes y diferencias.

Similitudes:

- Ambos se dividen en capas
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos
- Ambos tienen capas de transporte y de red similares
- Se supone que la tecnología es de conmutación por paquetes (no de conmutación por circuito)
¡Hay que conocer los dos!

Diferencias:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación
- TCP/IP combina las capas de enlace de datos y la capa física del modelo OSI en una sola capa
- TCP/IP parece ser más simple porque tiene menos capas
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, las redes típicas no se desarrollan normalmente a partir del protocolo OSI, aunque el modelo OSI se usa como guía.



IEEE ESTANDAR 802

Historia

En febrero de 1980 se formó en el IEEE un comité de redes locales (802) se desarrolló paralelamente con el modelo OSI pero es específicamente para el hardware. El proyecto 802 define aspectos relacionados al cableado físico y transmisión de data correspondiente a las capas físicas y enlace de datos. Los estándares OSI y IEEE 802 fueron desarrollados simultáneamente y en cooperación debido a que comparten características e interactúan muy bien. En estas normas también se define el control de acceso al medio (MAC).

Concepto

El Estándar IEEE 802 inicio el proyecto basado en conseguir un modelo para permitir la intercomunicación de ordenadores para la mayoría de los fabricantes. Para ello se enunciaron una serie de normalizaciones que con el tiempo han sido adaptadas como normas internacionales por la ISO. El protocolo 802 está dividido según las funciones necesarias para el funcionamiento de las LAN. Cada división se identifica por un número "802.x"

Características IEEE 802

Los comités 802 del IEEE se concentran principalmente en la interfaz física relacionada con los niveles físicos y de enlace de datos del modelo de referencia OSI de la ISO.

Los productos que siguen las normas 802 incluyen tarjetas de la interfaz de red, bridges, routers y otros componentes utilizados para crear LANs de par trenzado y cable coaxial.

El nivel de enlace se divide en 2 subniveles MAC y LLC.

Son diferentes en la capa física en la subcapa MAC, pero son compatibles en la subcapa de enlace.

Es un módulo de software incorporado a la estación de trabajo o al servidor que proporciona una interfaz entre una tarjeta de interfaz de red NIC y el software redirector que se ejecuta en el ordenador.

El modelo del proyecto 802 - Fundamentos

Cuando comenzaron a aparecer las primeras redes de área local (LAN, Local Área Networks) como herramientas potenciales de empresa a finales de los setenta, el IEEE observó que era necesario definir ciertos estándares para redes de área local. Para conseguir esta tarea, el IEEE emprendió lo que se conoce como proyecto 802, debido al año y al mes de comienzo (febrero de 1980).

Aunque los estándares IEEE 802 publicados realmente son anteriores a los estándares ISO, ambos estaban en desarrollo aproximadamente al mismo tiempo y compartían información que concluyó en la creación de dos modelos compatibles.

El proyecto 802 definió estándares de redes para las componentes físicas de una red (la tarjeta de red y el cableado) que se corresponden con los niveles físico y de enlace de datos del modelo OSI.

Las especificaciones 802 definen estándares para:

- Tarjetas de red (NIC).
- Componentes de redes de área global (WAN, Wide Área Networks).
- Componentes utilizadas para crear redes de cable coaxial y de par trenzado.

Las especificaciones 802 definen la forma en que las tarjetas de red acceden y transfieren datos sobre el medio físico. Éstas incluyen conexión, mantenimiento y desconexión de dispositivos de red.

La selección del protocolo a ejecutar en el nivel de enlace de datos es la decisión más importante que se debe tomar cuando se diseña una red de área local (LAN). Este protocolo define la velocidad de la red, el método utilizado para acceder a la red física, los tipos de cables que se pueden utilizar y las tarjetas de red y dispositivos que se instalan.

Clasificación de los estándares IEEE 802

Los estándares IEEE 802.X se clasifican en 16 categorías que se pueden identificar por su número acompañado del 802.

- IEEE 802.1 Protocolos superiores de redes de área local
- IEEE 802.2 Control de enlace lógico
- IEEE 802.3 Ethernet
- IEEE 802.4 Token Bus
- IEEE 802.5 Token Ring
- IEEE 802.6 Red de área metropolitana
- IEEE 802.7 Grupo de Asesoría Técnica sobre banda ancha
- IEEE 802.8 Grupo de Asesoría Técnica sobre fibra óptica
- IEEE 802.9 RAL de servicios integrados (abandonado)
- IEEE 802.10 Seguridad interoperable en RAL(abandonado)
- IEEE 802.11 Red local inalámbrica, también conocido como Wi-Fi
- IEEE 802.12 Prioridad de demanda
- IEEE 802.13 No usado.
- IEEE 802.14 Cable módems, es decir módems para televisión por Cable
- IEEE 802.15 Red de área personal inalámbrica, que viene a ser Bluetooth
- IEEE 802.16 Acceso inalámbrico de Banda Ancha, también llamada WiMAX, para acceso inalámbrico desde casa

Descripción de los estándares IEEE 802

IEEE 802.1: Protocolos superiores de redes de área local

- Establece los estándares de interconexión relacionados con la gestión de redes.
- La norma 802.1 describe la interrelación entre las partes del documento y su relación con el Modelo de Referencia OSI. También contiene información sobre normas de

gestión de red e interconexión de redes. Establece los estándares de interconexión relacionados con la gestión de redes.

IEEE 802.2: Control de enlace lógico

- IEEE 802.2 es el estándar que define el control de enlace lógico (LLC), que es la parte superior de la capa enlace en las redes de área local. La subcapa LLC presenta una interfaz uniforme al usuario del servicio enlace de datos, normalmente la capa de red. Bajo la subcapa LLC esta la subcapa Medium Access Control (MAC), que depende de la configuración de red usada (Ethernet, token ring, FDDI, 802.11, etc.).

IEEE 802.3: Ethernet

- La norma 802.3 es una especificación estándar sobre la que se monta Ethernet, un método de establecimiento de comunicaciones físicas a través de una red de área local o LAN, creada por el IEEE. 802.3. Especifica el protocolo de transporte de información del nivel físico dentro de una arquitectura de red a capas, tal como TCP/IP, basada a su vez en el modelo OSI.
- Se definió en 1983 y hoy en día el término Ethernet se utiliza para referirnos a las especificaciones Ethernet incluidas en IEEE 802.3. En este tiempo ha sufrido numerosas ampliaciones que han servido para enriquecerlo, notable ha sido el aumento de su velocidad de transferencia de datos dando lugar a los conocidos: Fast Ethernet, Gigabit Ethernet y 10Gigabits Ethernet.
- A continuación mencionaremos todas y cada una de las alternativas, en cuanto a nivel físico se refiere, basadas en este estándar:
 - 10 BASE 2: 10 Mbit/s sobre coaxial fino. Longitud máxima del segmento 185 metros.
 - 10 BASE 5: 10 Mbit/s sobre coaxial grueso. Longitud máxima del segmento 500 metros.
 - 10 BASE T: 10 Mbit/s sobre par trenzado UTP. Longitud máxima del segmento 100 metros.
 - 10 BASE F: 10 Mbit/s sobre fibra óptica. Longitud máxima del segmento 1000 metros.
 - 100 BASE TX/T4/FX: 100Mbit/s, es la considerada Fast Ethernet.
 - 1000 BASE X/T: Gigabit Ethernet.

IEEE 802.4: Token Bus

- Es un protocolo de red que implementa una red lógica en anillo con paso de testigo sobre en una red física de cable coaxial.
- Las redes que siguen este protocolo se han extendido rápidamente, sobre todo por su facilidad de instalación. Sin embargo, tienen un problema que representa un escollo importante en algunas aplicaciones: su carácter probabilístico en la resolución de las colisiones puede provocar retardos importantes en las transmisiones en casos extremos. Algunas aplicaciones no soportan tales retardos, sobre todo las que son críticas en el tiempo, es decir, en aplicaciones en tiempo real, como el control de procesos industriales.

IEEE 802.5: Token Ring

Este estándar define una red con topología de anillo la cual usa token (paquete de datos) para transmitir información a otra. En una estación de trabajo la cual envía un mensaje lo sitúa dentro de un token y lo direcciona específicamente a un destino, la estación destino copia el mensaje y lo envía a un token de regreso a la estación origen la cual borra el mensaje y pasa el token a la siguiente estación.

IEEE 802.6: Red de área metropolitana

Red de área metropolitana (MAN), basada en la topología propuesta por la University of Western Australia, utiliza un bus dual de fibra óptica como medio de transmisión. Ambos buses son unidireccionales, y en contra-sentido. Con esta tecnología el ancho de banda es distribuido entre los usuarios, de acuerdo a la demanda que existe, en proceso conocido como "inserción de ranuras temporales". Puesto que puede llevar transmisión de datos sincrónicos y asincrónicos, soporta aplicaciones de video, voz y datos.

IEEE 802.7: Grupo de Asesoría Técnica sobre banda ancha

Un estándar de IEEE para una red de área local de banda ancha (LAN) que usa el cable coaxial. Este estándar fue desarrollado para las compañías del Internet del cable. Especificaciones de redes con mayores anchos de banda con la posibilidad de transmitir datos, sonido e imágenes.

IEEE 802.8: Grupo de Asesoría Técnica sobre fibra óptica

Especificación para redes de fibra óptica tipo Token Passing /FDDI.

Las redes FDDI (Fiber Distributed Data Interface - Interfaz de Datos Distribuida por Fibra) surgieron a mediados de los años ochenta para dar soporte a las estaciones de

trabajo de alta velocidad, que habían llevado las capacidades de las tecnologías Ethernet y Token Ring existentes hasta el límite de sus posibilidades.

Proporciona asesoría técnica a otros subcomités en redes de fibra óptica como alternativa a las redes actuales basadas en cobre.

IEEE 802.9: Redes integradas para voz, datos y vídeo.

Comité para integración de voz y datos IVD (Integrated Voice and Data) en la red ISDN.

Se define la RDSI (Red Digital de Servicios Integrados, en inglés ISDN) como una evolución de las Redes actuales, que presta conexiones extremo a extremo a nivel digital y capaz de ofertar diferentes servicios.

Decimos Servicios integrados porque utiliza la misma infraestructura para muchos servicios que tradicionalmente requerían interfaces distintas (télex, voz, conmutación de circuitos, conmutación de paquetes...); es digital porque se basa en la transmisión digital.

IEEE 802.10: Seguridad de las redes.

Seguridad de red. Grupo que trabaja en la definición de un modelo normalizado de seguridad que ínter opera sobre distintas redes e incorpore métodos de autenticación y de cifrado.

IEEE 802.11: Red local inalámbrica, también conocido como Wi-Fi (Mejoras y modificaciones)

El protocolo IEEE 802.11 o WI-FI es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico. Por tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet).

Existen diversos tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11 aprobado. Son los siguientes:

Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutaron de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps, 54 Mbps y 300 Mbps, respectivamente.

En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada y, además, no existen otras tecnologías (Bluetooth, microondas, ZigBee, WUSB) que la estén utilizando, por lo tanto existen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2.4 GHz (aproximadamente un 10%), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).

Existe un primer borrador del estándar IEEE 802.11n que trabaja a 2.4 GHz y a una velocidad de 108 Mbps. Sin embargo, el estándar 802.11g es capaz de alcanzar ya transferencias a 108 Mbps, gracias a diversas técnicas de aceleramiento. Actualmente existen ciertos dispositivos que permiten utilizar esta tecnología, denominados Pre-N.

Existen otras tecnologías inalámbricas como Bluetooth que también funcionan a una frecuencia de 2.4 GHz, por lo que puede presentar interferencias con Wi-Fi. Debido a esto, en la versión 1.2 del estándar Bluetooth por ejemplo se actualizó su especificación para que no existieran interferencias con la utilización simultánea de ambas tecnologías, además se necesita tener 40.000 k de velocidad.

IEEE 802.12 y IEEE 802.13: Prioridad de demanda

- Comité que define la norma ethernet a 100 Mbps con el método de acceso de prioridad bajo demanda propuesto por la Hewlett Packard y otros fabricantes.
- El cable especificado es un par trenzado de 4 hilos de cobre utilizándose un concentrador central para controlar el acceso al cable.
- Las prioridades están disponibles para soportar la distribución en tiempo real de aplicaciones multimediales.
- Los concentradores 100VG-AnyLAN controlan el acceso a la red con lo cual eliminan la necesidad de que las estaciones de trabajo detecten una señal portadora, como sucede en el CSMA/CD de la norma ethernet.

IEEE 802.14 Cable módems, es decir módems para televisión por Cable

El Grupo IEEE 802.14 es justamente una parte de la larga serie de estándares 802 de LAN/MAN. Los estándares IEEE 802 para Ethernet y Token Ring, son los mas

extendidos en las redes de comunicación, y productos basados en los estándares sobre 802 dan razón de la mayoría de nodos de comunicación instalados en la industria.

El Grupo de trabajo IEEE 802.14 está caracterizado para crear estándares para transportar información sobre el cable tradicional de redes de TV. La arquitectura especifica un híbrido fibra óptica/coaxial que puede abarcar un radio de 80 kilómetros desde la cabecera. El objetivo primordial del protocolo de red en el diseño es el de transportar diferentes tipos de tráfico del IEEE 802.2 LLC (Control de Enlace Lógico), por ejemplo Ethernet. Sin embargo existe una fuerte opinión dentro del grupo que la red debería soportar redes ATM para llevar varios tipos de tráfico multimedia.

El grupo del estándar de la IEEE 802.14 define el protocolo de Capa Física y Control de Acceso al Medio (MAC) de redes usando cables Híbridos Fibra Óptica/Coaxial (HFC). Varios protocolos MAC han sido propuestos por el grupo de trabajo el cual tiene que comenzar la evaluación de procesos para concebir un sencillo protocolo MAC satisfaciendo todos los requerimientos de HFC.

Actualmente existen organizaciones implicadas en procesos de normalización de las telecomunicaciones en todo el mundo. Pero antes de describir sus trabajos realizados es fundamental explicar qué es el HFC y el protocolo MAC; y de igual forma especificar sus respectivas estructuras.

¿Qué es HFC?

Una red HFC (Híbridas Fibra óptica-Coaxial) es una red de telecomunicaciones por cable que combina la fibra óptica y el cable coaxial como soporte de la transmisión de las señales. Esta se compone básicamente de cuatro partes: la cabecera, la red troncal, la red de distribución y el bucle de abonados.