Universidad Nacional Autónoma de México

Facultad de Estudios Superiores "Aragón"

"Evolución de la tecnología de acceso a Internet"

T E S I S

Que presenta para obtener el grado de:
LICENCIATURA EN INGENIERÍA MECÁNICA ELÉCTRICA CON ESPECIALIDAD EN TELECOMUNICACIONES

Conde Mora Israel
098238329

Asesor:
Ing. Ramírez Mora José Manuel

México, D.F. **2006**

A Dios: Gracias por ser mi maestro, mi confidente y mi amigo; por guiar mis pasos e iluminar mi camino, en esta gran aventura de mi realización profesional.

A mi mamá: Quien me ha brindado todo su amor, apoyo y confianza; contribuyendo a mi formación profesional.

A mis abuelos: Quienes han representado un gran pilar en mi familia, y han sido la máxima motivación en mi realización profesional.

A mi familia: Gracias por su paciencia y confianza que han hecho esto posible.

A mis maestros: Un especial agradecimiento, quienes me guiaron durante mi formación profesional.

INDICE

INTRODUCCIÓN		1
JUSTIFICACIÓN		5
OBJETIVO		6
NOCIONES TEORICAS PREELIMINARES		7

CAPITULO 1

BANDA ANCHA: ACCESO Y SERVICIO

1	BANDA ANCHA: ACCESO Y SERVICIO	12
1.1	ADSL	13
1.2	DSLAM	14
1.3	DSLAM ATM	16

CAPITULO 2

BANDA ANCHA INALAMBRICA

2	BANDA ANCHA INALAMBRICA	19
2.1	CREACION DEL MODELO OSI	19
2.2	ESTRUCTURA DEL MODELO OSI	21
2.3	TRANSMISION DE DATOS EN EL MODELO OSI	30
2.4	EQUIPO DE COMUNICACION DE NIVEL RED	40
2.5	RIP	45
2.6	LMDS	48
2.7	CARACTERISTICAS DEL LMDS	49
2.8	WI-FI	51
2.9	HIPERLAN	52
2.10	IPsec	56
2.11	HIPERLAN/2	63
2.12	WIMAX	67

CAPITULO 3

HOGAR Y ENTRETENIMIENTO DIGITAL

3	HOGAR Y ENTRETENIMIENTO DIGITAL	69
3.1	PROLIFERACION DE COMUNICACIONES INALAMBRICAS	71

CONCLUSIONES 80

GLOSARIO 82

REFERENCIAS ELECTRONICAS Y BIBLIOGRAFICAS 84

INTRODUCCION

Tanto como a usuarios o empresas el futuro nos deparara una red mucho más amplia, de un alcance real trascendiendo los límites de conectividad, uso y aplicación. Ver todo este futuro logra hacernos realmente vivir de cerca la rápida maduración de la red de redes con la fuerza de su crecimiento.

La apuesta por Internet ya se ve grande y la competencia de los actores del mercado incluye a representantes de todos los sectores. Lo único que resta es estar preparados para los nuevos tiempos en donde la movilidad y la convergencia reinaran.

Ciertamente mucho ha cambiado desde la caída de las punto com. (dominios de regiones que agrupa organizaciones comerciales), cuando la burbuja (fiebre especulativa vinculada a Internet) creada en Wall Street hacia fluir los capitales hacia las empresas de Internet. En aquel momento las empresas preveían ingresos en base a un mercado futuro potencial, hoy la mirada es más pragmática y los números son los que mandan a la hora de adoptar uno u otro estándar.

La palabra que resume sus ponencias es la convergencia de cualquier tipo de tecnología a Internet. Si de telefonía móvil se trata GPRS, 3G, UMTS, MMS todos confluyen a este objetivo. Un tanto igual sucede con las tecnologías inalámbricas como Bluetooth, Wi-fi, WMAX, entre otras. Por lo que ciertamente habrá un periodo de convivencia obligado.

Móviles, Televisores, Cámaras, Reproductores de audio, DVDs, cualquiera sea el dispositivo digital la conclusión es siempre la misma:” Todo se conectará a Internet “. El estándar Ipv6 es el encargado de ampliar las cantidades de IP disponibles a tal punto que no haya persona en el planeta capaz de no tener como mínimo tres dispositivos digitales "online".

La telefonía IP (VoIP) es otro gran actor que se abre paso entre los servicios de voz en Internet. Con la venia de los mismos proveedores de Internet, las llamadas por el sistema tradicional podrán o no convivir con la digital en el futuro. Su proliferación sin embargo se descarta a tal punto que quizás solo paguemos una tarifa plana por su uso en el futuro mediato.

Las redes dejaran de ser algo profesional para convertirse en algo domestico, mas de un ordenador es habitual en algunos usuarios hogareños pero lo será aun más en el futuro así como el hecho de la existencia de una conexión permanente. Los Hotspots (zonas) móviles en vehículos no serán asimismo un sueño, las tecnologías inalámbricas se encargaran de hacerlo realidad.

En materia de seguridad y privacidad los usuarios se enfrentaran lamentablemente en forma permanente al riesgo. La tecnología esta mas preocupada en crecer y desarrollarse que cuidar a los usuarios. Evaluar cada nuevo dispositivo será una tarea indispensable. Las prestaciones los integraran con tanta facilidad mimetizándose unos con otros.

China y los países asiáticos influirán aún más en la red con su presencia. Su crecimiento se enmarca globalmente en una dimensión hasta ahora desconocida. La sorpresa del gigante rojo la da su potencial aunque aún debe salvar el excesivo control sobre sus habitantes. Con sólo decir que la cantidad de teléfonos móviles igualan a la población norteamericana tenemos una idea de la dimensión del fenómeno.

Así el Congreso Mundial de Internet, nos muestra una red a donde todos los dispositivos convergen, a tal punto de confundirnos con tantos usos posibles. No sabremos en esencia como un sólo dispositivo lo hace todo pero con toda seguridad nos adaptaremos. En cuanto a la movilidad, además de ser un hecho se transformara en vital.

El acceso de banda ancha es un desafío que se viene logrando desde la década pasada. El problema fundamental está en desarrollar tecnologías que permitan altas velocidades en la última milla, a través de medios de transmisión convencionales como el par trenzado telefónico, el cable coaxial de las redes de cable o el espacio

radioeléctrico. Otro hecho es, lograr que sobre este acceso se pueda brindar al usuario garantías de QoS (calidad y servicio), donde el ATM juega un papel fundamental.

En este trabajo se realiza un estudio de algunas tecnologías de acceso de banda ancha que permiten brindar al usuario una gama de servicios integrados que incluyen, servicio de Internet de alta velocidad, e interconexión de redes LAN, entre otros.

***Capitulo "1"*:** Se aborda la necesidad de ancho de banda esto ha hecho nacer varias tecnologías de acceso de banda ancha: DSL (Línea de Abonado Digital) en todas sus formas simétricas y asimétricas, utiliza la infraestructura de cobre para dar servicios a velocidades de hasta algunos megabits por segundo.

C***apitulo "2"*:** Se tratan las redes inalámbricas las cuales proveen portabilidad, escalabilidad, flexibilidad y, sobre todo, simplicidad para el usuario común. En las redes modernas existen diversos protocolos y tecnologías, desde tecnologías que nacieron como simple reemplazo de cables, como ejemplo tenemos el LMDS (Sistema de Distribución Local de Servicio Multipunto) los servicios locales de distribución multipunto ofrecen velocidades de banda ancha a usuarios residenciales y a profesionales independientes. La libertad que permiten las tecnologías inalámbricas, libertad de movimiento, acción, conectividad, son precisamente la razón de su aceptación, y también el motivo por el que las compañías se esfuerzan cada vez más por mejorarlas y ganar un nicho en el mercado.

***Capitulo "3"*:** Se finaliza viendo como estos servicios son integrados en el en las viviendas de hoy en día las cuales disponen de un gran número de equipos y sistemas, principalmente autónomos, y redes no conectados entre ellos como la telefonía, los sistemas de acceso, la televisión, las redes de datos (cableados e inalámbricos), electrodomésticos, equipamiento de audio y video, calefacción, aire-condicionado, seguridad, riego, iluminación, etc., el proceso de integración de estos equipos, sistemas autónomos, en redes y sistemas integrados se denominó inicialmente Integración de Sistemas y a las mismas viviendas, Viviendas Inteligentes. Todo ello en combinación con el servicio de Banda Ancha, ha hecho sustituir el concepto original por el de Hogar Digital. Además de los sectores de la domótica, electrodomésticos y seguridad, un gran número de fabricantes también ha llegado a utilizar el concepto

“Hogar Digital” para sus productos o familias de productos principalmente relacionados con redes de datos o productos multimedia de entretenimiento.

JUSTIFICACION

En ocasiones las tecnologías podrían parecer competencia directa entre sí, dependiendo del nicho de mercado en el cual se sobrepusieran, y en otros casos parecerán completamente indiferentes; sin embargo, parte de lo que hace interesante al mundo de las comunicaciones inalámbricas es precisamente como todas estas diferentes tecnologías e iniciativas interactúan y se impactan mutuamente ya que, en su mayoría, todas lo hacen. Sin embargo la tendencia siempre se inclinará a buscar la libertad de movimiento, la libertad de esas marañas de cables que pueden, desde complicar el tránsito en una oficina, hasta provocar accidentes por los mismos cables.

Las redes inalámbricas proveen portabilidad, escalabilidad, flexibilidad y, sobre todo, simplicidad para el usuario común. En las redes modernas existen diversos protocolos y tecnologías, desde tecnologías que nacieron como simple reemplazo de cables hasta protocolos completos para comunicación y acceso a redes más grandes.

OBJETIVO

Explorar las tecnologías en los equipos y protocolos principales con el fin de modelar aplicaciones para acceso, recuperación y transmisión de información multimedia para poder determinar puntos de interferencia e interoperabilidad.

NOCIONES TEORICAS PREELIMINARES.

La historia de Internet se remonta al temprano desarrollo de las redes de comunicación. La idea de una red entre ordenadores diseñada para permitir la comunicación general entre usuarios de varias computadoras se ha desarrollado en un gran número de pasos. La unión de todos estos desarrollos culminó con la red de redes que conocemos como Internet. Esto incluía tanto desarrollos tecnológicos como la fusión de la infraestructura de la red ya existente y los sistemas de telecomunicaciones.

Las más antiguas versiones de estas ideas aparecieron a finales de los años 50. Implementaciones prácticas de estos conceptos empezaron a finales de los 60 y a lo largo de los 70. En la década de 1980, tecnologías que reconoceríamos como las bases de la moderna Internet, empezaron a expandirse por todo el mundo. En los 90 se introdujo la World Wide Web, que se hizo común.

La infraestructura de Internet se esparció por el mundo, para crear la moderna red mundial de ordenadores que hoy conocemos. Atravesó los países occidentales e intentó una penetración en los países en desarrollo, creando un acceso mundial a información y comunicación sin precedentes, pero también una brecha digital en el acceso a esta nueva infraestructura. Internet también alteró la economía del mundo entero, incluyendo las implicaciones económicas de las burbujas de los punto com.

Antes de la red que originó Internet, la mayoría de las redes de comunicación estaban limitadas por su idiosincrasia de solo permitir las comunicaciones entre las diferentes estaciones de la red. Algunas redes contenían gateways o puentes entre ellos, pero estos puentes se limitaban a un solo usuario.

Un método de conectar computadoras, prevalente sobre los demás, se basaba en el método del ordenador central o unidad principal, que simplemente consistía en permitir a sus terminales conectarse a través de largas línea alquilada. Este método se usaba en los años 50's por el Proyecto RAND para apoyar a investigadores como Herbert Simon, en Pittsburgh (Pensilvania), cuando colaboraba a través de todo el continente con otros investigadores de Santa Monica (California) trabajando en demostraciones de teoremas automatizadas e inteligencia artificial.

Un pionero fundamental en en lo que se refiere a una red mundial, J.C.R. Licklider, comprendió la necesidad de una red mundial, según consta en su documento de Enero, 1960, Man-Computer Symbiosis (Simbiosis Hombre-Computadora).

En Octubre de 1962, Licklider fue nombrado jefe de la oficina de procesado de información DARPA, y empezó a formar un grupo informal dentro del DARPA del Departamento de Defensa de los Estados Unidos para investigaciones sobre ordenadores más avanzadas. Como parte del papel de la oficina de procesado de información, se instalaron tres terminales de redes: una para la System Development Corporation en Santa Mónica, otra para el Proyecto Genie en la Universidad de California (Berkeley) y otra para el proyecto Multics en el Instituto Massachusetts de Tecnología. La necesidad de Licklider de redes se haría evidente por los problemas que esto causó.

Como principal problema en lo que se refiere a las inter-conexiones está el conectar diferentes conexiones físicas para formar una sóla conexión lógica. Durante los años 60, varios grupos trabajaron en el concepto de la conmutación de paquetes. Normalmente se considera que Donald Davies (National Physical Laboratory), Paul Baran (Rand Corporation) y Leonard Kleinrock (MIT) lo han inventado simultáneamente. El común mito que dice que Internet se hizo para sobrevivir a un ataque nuclear tiene sus raíces en las tempranas teorías desarrolladas por RAND. La investigación de Baran nos ha traído el concepto de conmutación de paquetes desde el estudio de la descentralización de Internet para evitar ponerla en manos de enemigos en caso de guerra.

Leonard Kleinrock ascendido a jefe de la oficina de procesamiento de información en el ARPA, Robert Taylor intentó hacer reales las ideas de Licklider sobre un sistema de redes interconectadas. Junto con Larry Roberts del MIT, inició un proyecto para empezar con una red por el estilo. La primera conexión de ARPANET se estableció el 21 de noviembre de 1969, entre la Universidad de California, Los Angeles y el Instituto de Investigaciones de Stanford. Antes del 5 de diciembre de 1969, se había formado una red de 4 nodosm añadiendo la Universidad de Utah y la Universdad de California, Santa Barbara. Usando ideas desarrolladas en la ALOHAnet, la ARPANET se inauguró en 1972 y creció rápidamente hasta el 1981. El número de hosts creció a 213, con uno nuevo añadiéndose aproximadamente cada 20 días.

ARPANET se convirtió en el núcleo de lo que posteriormente sería Internet, y también en una herramienta primaria en el desarrollo de la tecnología del momento. ARPANET evolucionó usando estándares del proceso RFC, aún usado actualmente para proponer y distribuir protocolos y sistemas de Internet. El RFC1, titulado "Host Software", fue escrito por Steve Crocker desde la Universidad de California, Los Angeles, y publicado el 7 de abril de 1969.

Las colaboraciones internacionales en ARPANET eran escasas; por varias razones políticas los desarrolladores europeos estaban preocupados en desarrollar las redes X.25, con la notable excepción del Norwegian Seismic Array en 1972 seguidos en 1973 por enlaces de los satélites a la estación terrestre de Tanum en Suecia y en la University College de Londres.

A partir de la investigación del DARPA, las redes de conmutación de paquetes fueron desarrolladas por la Unión Internacional de Telecomunicaciones (UIT) en forma de redes X.25. X.25 formó la base de la red entre la academia británica y otros sitios de investigación en SERCnet, en 1974, que más tarde pasaría a llamarse JANET. El Estándar inicial de X.25 según la UIT se aprobó en Marzo de 1976.

En 1978, la Oficina de Correos británica, Western Union International y Tymnet colaboraron para crear la primera red de paquetes conmutados internacional; refiriéndose a ella como "International Packet Switched Service" (IPSS). Esta red creció desde Europa y Estados Unidos hasta Canadá, Hong Kong y Australia antes del 1981, y pocos años después, creó una infraestructura de conexiones mundial. [7]

Al contrario que ARPAnet, X.25 estaba diseñado para poderse utilizar en oficina. Se usó para las primeras redes de teléfono de acceso público, tales como Compuserve y Tymnet. En 1979, CompuServe fue el primero en ofrecer posibilidades para el correo electrónico y soporte técnico a usuarios de PCs. La compañía fue nuevamente pionera en 1980, como la primera en ofrecer chat con su CB Simulator. También estaban las redes de teléfono de America Online (AOL) y Prodigy, y varias redes BBS como The WELL y FidoNet. FidoNet era popular entre usuarios por hobby, parte de ellos hackers y radioaficionados.

En 1979, dos estudiantes de la Universidad de Duke, Tom Truscott y Jim Ellis, propusieron la idea de usar scripts simples en Bourne Shell para transefir noticias y mensajes entre su universidad y la cercana Universidad de Carolina del Norte, Chapel Hill. Después de la salida del software al dominio público, la red de hosts UUCP usada para noticias Usenet se expandió rápidamente. UUCPnet, nombre que acabaría recibiendo, también crearía portales y vínculos entre Fidonet y los hosts de marcaje telefónico BBS. Las redes UUCP se distribuyeron rápidamente debido a su bajo coste y a su capacidad de usar las líneas alquiladas ya existentes, los vínculos X.25 o incluso las conexiones de ARPANET. Antes de 1983 el número de hosts UUCP ya había aumentado a 550, casi duplicándose hasta los 940 en 1984.

Por esta época había muchos métodos diferentes de conexionado, hacía falta algo para unificarlos. Robert E. Kahn del ARPA y ARPANET contrató a Vint Cerf de la Universidad de Stanford para trabajar con él en el problema. Antes del 1973, habían pensado en una reformulación fundamental, donde las diferencias entre los protocolos de red se escondían usando un protocolo de red común, y donde eran los hosts los encargados de ser fiables, y no la red. Cerf atribuye a Hubert Zimmerman y a Louis Pouzin (diseñador de la red CYCLADES) un importante trabajo en este diseño. [8]

Con el rol de la red reducido al mínimo, se hizo posible juntar prácticamente todas las redes, sin importar sus características, resolviendo el problema inicial de Kahn. DARPA aceptó patrocinar el desarrollo del software prototipo, y tras muchos años de trabajo, la primera demostración (algo básica) de en cómo se había convertido al protocolo TCP/IP (en Julio de 1977). Este nuevo método se expandió rápidamente por las redes, y el 1 de Enero de 1983, los protocolos TCP/IP se hicieron los únicos protocolos aprobados en ARPANET, sustitiyendo al anterior protocolo NCP. [9]

Después que [ARPANET]] estuviera funcionando por varios, ARPA buscó otra agencia para ceder la red de ordenadores; la tarea primaria de ARPA era impulsar investigaciones y desarrollos de avanzada, no manejar un servicio público de comunicaciones. Eventualmente, en julio de 1975, la red se cedió a la "Defense Communications Agency" que también era parte del Departamento de Defensa. En 1984, la porción militar de ARPANet se dividió como una red separada, la MILNET.

Las redes basadas alrededor de ARPANET eran pagadas por el gobierno y por tanto restringidas a usos no comerciales tales como investigación; el uso comercial estaba estrictamente prohibido. Las conexiones se restringieron a sitios militares y universidades. Durante los 80s, las conexiones se expandieron a más instituciones educacionales, e incluso a un creciente número de compañías tales como Digital Equipment Corporation y Hewlett-Packard, que estaban participando en proyectos de investigación y suministrando servicios.

Otra rama del gobierno, la National Science Foundation (NSF), se volvió fuertemente involucrada en investigación en Internet y empezó un desarrollo como sucesor de ARPANET. En 1984 esto resultó en la primera red de banda ancha diseñada específicamente para usar TCP/IP. Esto creció como NSFNet, establecida en 1986, para conectar y proveer acceso a una cantidad de supercomputadores establecidos por la NSF.

En la actualidad Proveer acceso a Internet de alta velocidad, es de esencial valor para los usuarios residenciales, negocios medianos, etc. Tecnologías DSL como ADSL y G.Lite, pueden satisfacer los requerimientos de las actuales aplicaciones de Internet

1 “BANDA ANCHA: ACCESO Y SERVICIO"

El primero propone como tema: “Buscar un modelo de hogar digital analizando las claves estratégicas de su desarrollo: automatización, control y teleservicios, ¿cuál es el por qué de la evolución del concepto de domótica tradicional al de conectividad en el hogar?”

En estos temas opino que las principales barreras para un gran despliegue son el interés y conocimiento de los instaladores y la falta de interés y desconocimiento por parte de los usuarios. Considero que existe un gran potencial para los servicios del hogar digital y sobre todo con la banda ancha.

Las nuevas tecnologías de interacción que el usuario puede utilizar para disfrutar de los servicios digitales en el hogar. El desarrollo del ambiente artificial alrededor del hogar digital, las nuevas formas de interfaces como voz, gestos, etc. que el usuario podrá utilizar para interactuar con su vivienda sin barreras en el futuro.

En telefónica I+D, el tema del ambiente digital personal, y el objetivo de que los clientes de banda ancha dispusiesen de servicios interoperables de gestión remota y siendo uno de los principales requisitos la movilidad para poder acceder a ellos desde cualquier lugar. También de la seguridad, la diversidad multimedia, la facilidad de uso y el Home Gateway (El punto de entrada es el dispositivo que ofrece conectividad de banda ancha al hogar y que entrega servicios a la ambiente familiar y a los diversos dispositivos y interfaces que la componen.), como elemento de interconexión entre el hogar y el mundo exterior.

En este apartado tuve en cuenta temas como que no se puede hablar de “un” hogar digital sino de “varios”; Un concepto con fuerte auge es el del ocio y entretenimiento.

1.1 ADSL (“ASYMMETRIC DIGITAL SUBSCRIBER LINE, LÍNEA DE ABONADO DIGITAL ASIMÉTRICA”)

Es una tecnología de acceso a Internet para la transmisión de datos a gran velocidad sobre el par de cobre. La primera diferencia entre esta modulación y las usadas por los módem en banda vocal (V.32 a V.90) es que éstos últimos sólo transmiten en la banda de frecuencias usada en telefonía (300 Hz a 3400 Hz), mientras que los módem ADSL operan en un margen de frecuencias mucho más amplio que va desde los 24 KHz hasta los 1104 KHz, aproximadamente, por lo que, para disponer de ADSL, es necesaria la instalación de un filtro (llamado splitter o discriminador) que se encarga de separar la señal telefónica convencional de la que usaremos para conectarnos con ADSL.

Esta línea se denomina asimétrica debido a que la velocidad de bajada y de subida de datos (entendiéndose por bajada la llegada de datos al usuario, y subida el envío de datos del usuario hacia la Red) no coinciden. Normalmente, la velocidad de bajada es mayor que la de subida.

En una línea ADSL se establecen tres canales de comunicación, que son el de envío de datos, el de recepción de datos y el de servicio telefónico normal.

Al tratarse de una modulación en la que se transmiten diferentes caudales en los sentidos Usuario -> Red y Red -> Usuario, el módem ADSL situado en el extremo del usuario es distinto del ubicado al otro lado del bucle, en la central local. En una primera etapa coexistieron dos técnicas de modulación para el ADSL: CAP ("Carrierless Amplitude/Phase") y DMT ("Discrete MultiTone"). Finalmente los organismos de estandarización (ANSI American National Standards Institute, ETSI The European Telecommunications Standards Institute e ITU, con sede en Ginebra (Suiza), es una organización internacional del sistema de las Naciones Unidas en la cual los gobiernos y el sector privado coordinan los servicios y redes mundiales de telecomunicaciones.) se han decantado por la solución DMT. Básicamente consiste en el empleo de múltiples portadoras y no sólo una, que es lo que se hace en los módems de banda vocal. Cada una de estas portadoras (denominadas subportadoras) es modulada en cuadratura (modulación QAM) por una parte del flujo total de datos que se van a transmitir. Estas

subportadoras están separadas entre sí 43125 KHz, y el ancho de banda que ocupa cada subportadora modulada es de 4 KHz.

El reparto del flujo de datos entre subportadoras se hace en función de la estimación de la relación Señal/Ruido en la banda asignada a cada una de ellas.

1.2 DSLAM ("DIGITAL SUBSCRIBER LINE ACCESS MULTIPLEXER, MULTIPLEXOR DE ACCESO A LA LÍNEA DE ABONADO DIGITAL")

Como antes se ha explicado, el ADSL necesita una pareja de módems por cada usuario: uno en el domicilio del usuario (ATU-R) y otro (ATU-C) en la central local a la que llega el bucle de ese usuario.

Esto complica el despliegue de esta tecnología de acceso en las centrales. Para solucionar esto surgió el DSLAM ("Digital Subscriber Line Access Multiplexer"): un chasis que agrupa gran número de tarjetas, cada una de las cuales consta de varios módem es ATU-C, y que además concentra el tráfico de todos los enlaces ADSL hacia una red WAN (WAN, Wide Area Network o redes de área amplia.) Las WAN conectan entre sí ordenadores separados por distancias mayores, situados en distintos lugares de un país o en diferentes países; emplean equipo físico especializado y costoso y arriendan los servicios de comunicaciones.

La integración de varios ATU-Cs en un equipo, el DSLAM, es un factor fundamental que ha hecho posible el despliegue masivo del ADSL. ATM sobre ADSL.

Estas son las ventajas del acceso ADSL:

Gran ancho de banda en el acceso: permite el intercambio de información en formato digital a gran velocidad entre un usuario y la central local a la que se conecta mediante un par de cobre.

Este ancho de banda está disponible de forma permanente.

Se aprovecha una infraestructura ya desplegada, por lo que los tiempos de implantación de los servicios sobre la nueva modalidad de acceso se acortan.

El acceso es sobre un medio no compartido, y por tanto intrínsecamente seguro.

Ahora bien, ¿cómo se puede sacar provecho de esta gran velocidad de acceso? Las redes de comunicaciones de banda ancha emplean el ATM ("Asynchronous Transfer Mode") para la conmutación en banda ancha. Desde un primer momento, dado que el ADSL se concibió como una solución de acceso de banda ancha, se pensó en el envío de la información en forma de células ATM sobre los enlaces ADSL.

En los estándares sobre el ADSL, desde el primer momento se ha contemplado la posibilidad de transmitir la información sobre el enlace ADSL mediante células ATM. La información, ya sean tramas de vídeo MPEG2 o paquetes IP, se distribuye en células ATM, y el conjunto de células ATM así obtenido constituye el flujo de datos que modulan las subportadoras del ADSL DMT.

Si en un enlace ADSL se usa ATM como protocolo de enlace, se pueden definir varios circuitos virtuales permanentes (CVPs) ATM sobre el enlace ADSL entre el ATU-R y el ATU-C. De este modo, sobre un enlace físico se pueden definir múltiples conexiones lógicas cada una de ellas dedicadas a un servicio diferente. Por ello, ATM sobre un enlace ADSL aumenta la potencialidad permitiendo flexibilidad para múltiples servicios a un gran ancho de banda.

1.3 DSLAM ATM ("DIGITAL SUBSCRIBER LINE ACCESS MULTIPLEXER ASYNCHRONOUS TRANSFER MODE, MULTIPLEXOR DE ACCESO A LA LÍNEA DE ABONADO DIGITAL MODO DE TRANSFERENCIA ASÍNCRONA")

En los módems ADSL se pueden definir dos canales, uno el canal "fast" y otro el "interleaved". El primero agrupa los CVPs ATM dedicados a aplicaciones que pueden ser sensibles al retardo, como puede ser la transmisión de voz. El canal "interleaved", llamado así porque en el se aplican técnicas de entrelazado para evitar pérdidas de información por interferencias, agrupa los CVPs ATM asignados a aplicaciones que no son sensibles a retardos, como puede ser la transmisión de datos como se muestra en la figura 1.3.1.

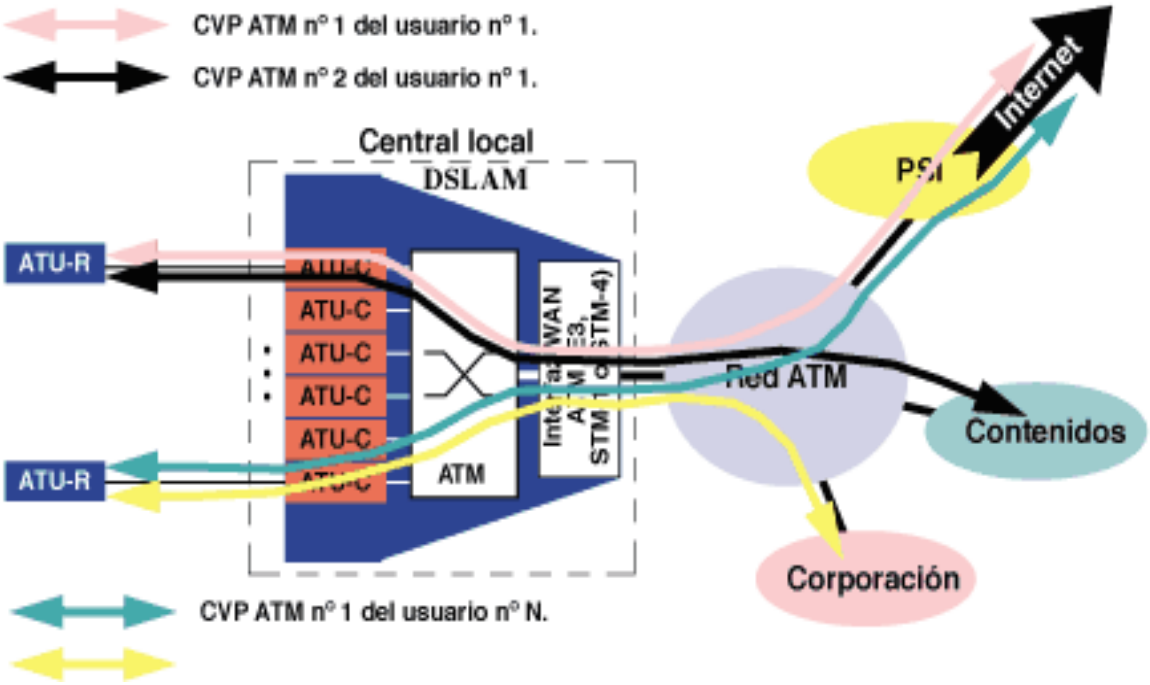


Figura 1.3.1. CVPs ATM

A nivel de enlace, algunos suministradores de equipos de central para ADSL han planteado otras alternativas al ATM, como PPP sobre ADSL y frame-relay sobre ADSL, pero finalmente no han tenido mucho predicamento.

Los estándares y la industria han impuesto el modelo de ATM sobre ADSL. En ese contexto, el DSLAM pasa a ser un conmutador ATM con múltiples interfaces, una de ellas sobre STM-1, STM-4 ó E3, y el resto ADSL-DMT, y el núcleo del DSLAM es una matriz de conmutación ATM sin bloqueo. De este modo, el DSLAM puede ejercer funciones de policía y conformado sobre el tráfico de los usuarios con acceso ADSL. En Torre de protocolos con ATM sobre ADSL se muestra la torre de protocolos con ATM sobre ADSL. Figura 1.3.2.

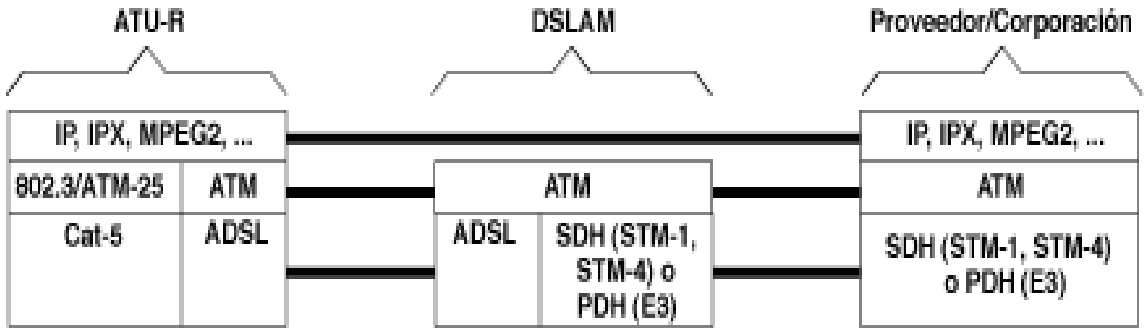


Figura 1.3.2 Torre de protocolos con ATM sobre ADSL

Modelos para ofrecer servicios

Los modelos para ofrecer servicios propuestos por el ADSL son los que se muestran en la figura 1.4.3:

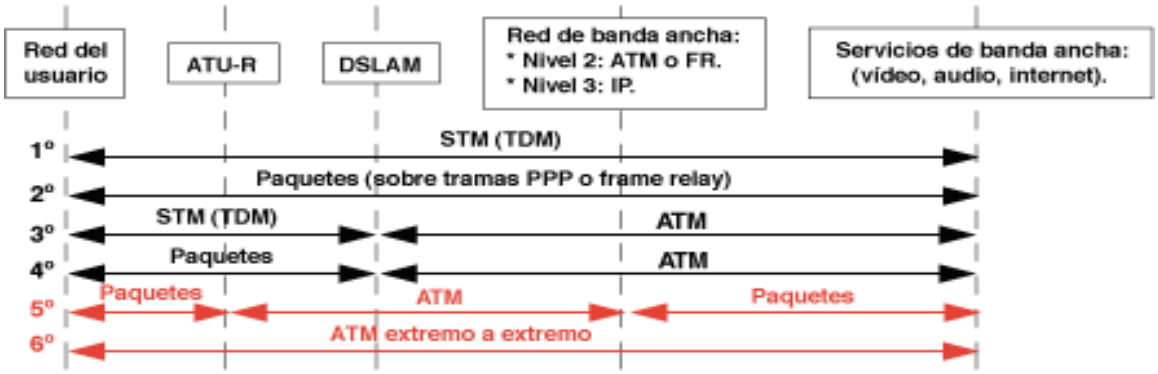


Figura 1.3.3 Modelos propuestos por el ADSL para la prestación de servicios con acceso ADSL

De acuerdo con lo que ya explicamos, la solución que se ha impuesto pasa por el envío de células ATM sobre el enlace ADSL (entre el ATU-R y el ATU-C situado en el

DSLAM). Por lo tanto, de los seis modelos que propone el ADSL sólo son válidos los dos últimos.

2 “BANDA ANCHA INALAMBRICA”

Las tecnologías inalámbricas del Hogar Digital, con descripciones y comparaciones de Bluetooth, ZigBee, UWB, WiFi y otras tecnologías. Disponemos de muchos dispositivos en casa y queremos interconectar estos para compartir la información. Para ello necesitamos un estándar y existen varias alternativas. La elección dependerá de los tipos de necesidades de volumen de datos, la conectividad, estabilidad de información, la seguridad, etc.

La estandarización del Hogar Digital para permitir que todos los usuarios tengan acceso a los servicios. Para el Hogar Digital es distinto, no se va a imponer a algún agente la instalación de todo esto sino que el desarrollo va a ser coordinado mediante una normalización que permita escala y que también se preocupe del derecho del usuario.

2.1 CREACION DEL MODELO OSI

En 1979, la Organización Internacional de Estándares (ISO), integrada por industrias representativas del medio, creó un subcomité para desarrollar estándares de comunicación de datos que promovieran la accesibilidad universal y una interoperabilidad entre productos de diferentes fabricantes.

El resultado de estos esfuerzos es el Modelo de Referencia Interconexión de Sistemas Abiertos (OSI).

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI.

Como se mencionó anteriormente, OSI nace de la necesidad de uniformizar los elementos que participan en la solución del problema de comunicación entre equipos de cómputo de diferentes fabricantes.

Estos equipos presentan diferencias en:

- Procesador Central.
- Velocidad.
- Memoria.
- Dispositivos de Almacenamiento.
- Interfaces para Comunicaciones.
- Códigos de caracteres.
- Sistemas Operativos.

Estas diferencias propician que el problema de comunicación entre computadoras no tenga una solución simple.

Dividiendo el problema general de la comunicación, en problemas específicos, facilitamos la obtención de una solución a dicho problema.

Esta estrategia establece importantes beneficios, como una mayor comprensión del problema y la solución de cada problema específico que puede ser optimizada individualmente. Este modelo persigue un objetivo claro y bien definido. Formalizar los diferentes niveles de interacción para la conexión de computadoras habilitando así la comunicación del sistema de cómputo independientemente del:

- Fabricante.
- Arquitectura.
- Localización.

Sistema Operativo.

Este objetivo tiene las siguientes aplicaciones:

Obtener un modelo de referencia estructurado en varios niveles en los que se contemple desde el concepto BIT hasta el concepto APILACION.

Desarrollar un modelo en el cual cada nivel define un protocolo que realiza funciones específicas diseñadas para atender el protocolo de la capa superior.

No especificar detalles de cada protocolo.

Especificar la forma de diseñar familias de protocolos, esto es, definir las funciones que debe realizar cada capa.

2.2 ESTRUCTURA DEL MODELO OSI:

El objetivo perseguido por OSI establece una estructura que presenta las siguientes particularidades:

Estructura multinivel: Se diseñó una estructura multinivel con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación. Esto es, cada nivel ejecuta funciones específicas.

El nivel superior utiliza los servicios de los niveles inferiores: Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora. La comunicación internivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1. Ver Figura 2.2.1.

Puntos de acceso: Entre los diferentes niveles existen interfaces llamadas "puntos de acceso" a los servicios.

Dependencias de Niveles: Cada nivel es dependiente del nivel inferior y también del superior.

Encabezados: En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información. Cualquier nivel dado, puede incorporar un encabezado al mensaje. Por esta razón, se considera que un

mensaje esta constituido de dos partes: Encabezado e Información. Entonces, la incorporación de encabezados es necesaria aunque representa un lote extra de información, lo que implica que un mensaje corto pueda ser voluminoso. Sin embargo, como la computadora destino retira los encabezados en orden inverso a como fueron incorporados en la computadora origen, finalmente el usuario sólo recibe el mensaje original.

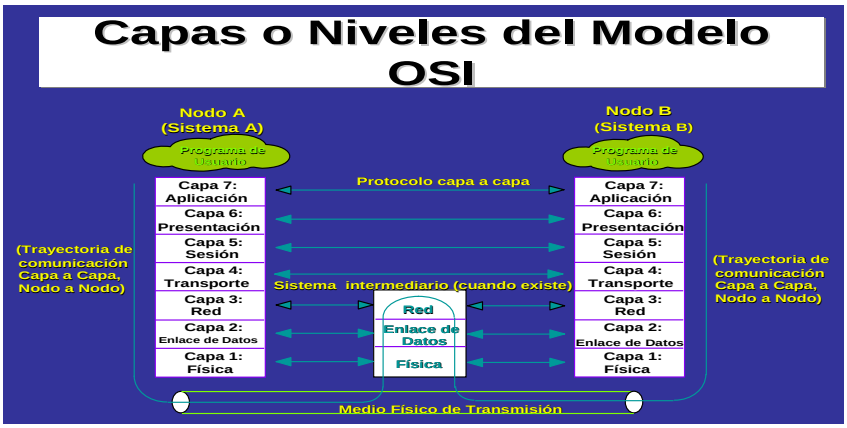


Figura 2.2.1 Capas o Niveles del Modelo OSI

Unidades de información: En cada nivel, la unidad de información tiene diferente nombre y estructura. :

La descripción de los 7 niveles es la siguiente:

Nivel Físico: Define el medio de comunicación utilizado para la transferencia de información, dispone del control de este medio en el caso de las comunicaciones inalámbricas nuestro medio de transmisión es el aire y especifica bits de control (Figura 2.3.2.), mediante:

- Definir conexiones físicas entre computadoras.
- Describir el aspecto mecánico de la interfase física.
- Describir el aspecto eléctrico de la interfase física.
- Describir el aspecto funcional de la interfase física.
- Definir la Técnica de Transmisión.
- Definir el Tipo de Transmisión.
- Definir la Codificación de Línea.

- Definir la Velocidad de Transmisión.
- Definir el Modo de Operación de la Línea de Datos.

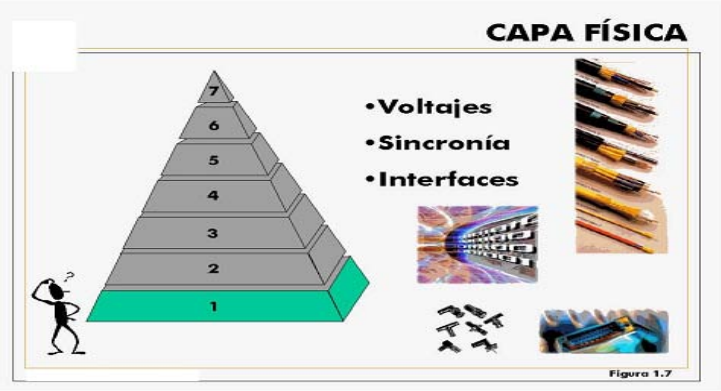


Figura 2.2.2 Capa Física

Nivel Enlace de Datos: Este nivel proporciona facilidades para la transmisión de bloques de datos entre dos estaciones de red. (Figura 2.2.3). Esto es, organiza los 1's y los 0's del Nivel Físico en formatos o grupos lógicos de información. Para:

- Detectar errores en el nivel físico.
- Establecer esquema de detección de errores para las retransmisiones o reconfiguraciones de la red.
- Establecer el método de acceso que la computadora debe seguir para transmitir y recibir mensajes.
- Realizar la transferencia de datos a través del enlace físico.
- Enviar bloques de datos con el control necesario para la sincronía.
- En general controla el nivel y es la interfaces con el nivel de red, al comunicarle a este una transmisión libre de errores.

Figura 2.2.3 Capa de Enlace

Nivel de Red: Este nivel define el enrutamiento y el envío de paquetes entre redes. (Figura 2.2.4.)

- Es responsabilidad de este nivel establecer, mantener y terminar las conexiones.
- Este nivel proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Nivel de Transporte) o bien al nivel 2 (Enlace de datos).
- Este nivel conmuta, enruta y controla la congestión de los paquetes de información en una sub-red.
- Define el estado de los mensajes que se envían a nodos de la red.

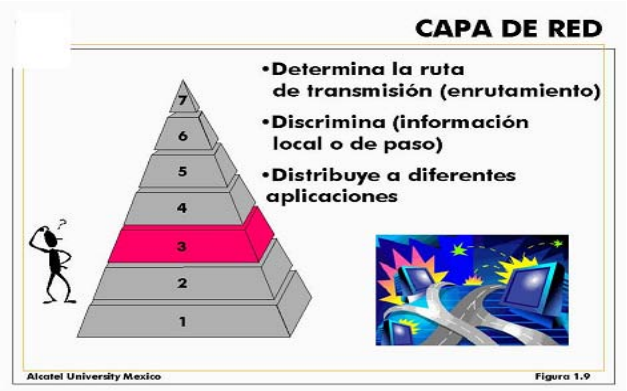


Figura 2.2.4 Capa de Red

Nivel de Transporte: Este nivel actúa como un puente entre los tres niveles inferiores totalmente orientados a las comunicaciones y los tres niveles superiores totalmente orientados a él procesamiento. Además, garantiza una entrega confiable de la información. Como se muestra en la Figura 2.2.5.

- Asegura que la llegada de datos del nivel de red encuentra las características de transmisión y calidad de servicio requerido por el nivel 5 (Sesión).
- Este nivel define como direccionar la localidad física de los dispositivos de la red.
- Asigna una dirección única de transporte a cada usuario.

- Define una posible multicanalización. Esto es, puede soportar múltiples conexiones.
- Define la manera de habilitar y deshabilitar las conexiones entre los nodos.
- Determina el protocolo que garantiza el envío del mensaje.
- Establece la transparencia de datos así como la confiabilidad en la transferencia de información entre dos sistemas.

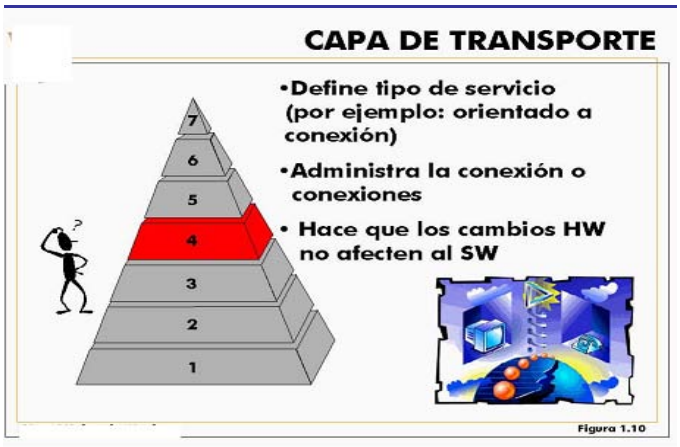


Figura 2.2.5 Capa de Transporte

Nivel Sesión: proveer los servicios utilizados para la organización y sincronización del diálogo entre usuarios y el manejo e intercambio de datos. (Figura 2.2.6.)

- Establece el inicio y termino de la sesión.
- Recuperación de la sesión.
- Control del diálogo; establece el orden en que los mensajes deben fluir entre usuarios finales.
- Referencia a los dispositivos por nombre y no por dirección.
- Permite escribir programas que correrán en cualquier instalación de red.

Figura 2.2.6 Capa de Sesión

Nivel Presentación: Traduce el formato y asignan una sintaxis a los datos para su transmisión en la red. (Figura 2.2.7).

- Determina la forma de presentación de los datos sin preocuparse de su significado o semántica.
- Establece independencia a los procesos de aplicación considerando las diferencias en la representación de datos.
- Proporciona servicios para el nivel de aplicaciones al interpretar el significado de los datos intercambiados.
- Opera el intercambio.
- Opera la visualización.

Figura 2.2.7 Capa de Presentación

Nivel Aplicación: Proporciona servicios al usuario del Modelo OSI. (Ver Figura 2.2.8.)

- Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.
- Proporciona aspectos de comunicaciones para aplicaciones específicas entre usuarios de redes: manejo de la red, protocolos de transferencias de archivos (ftp), etc.

Figura 2.2.8 Capa de Aplicación

Ventajas de la división en siete capas

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí de una forma totalmente definida.
- Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.

Características de las capas del modelo OSI

Las 7 capas del modelo OSI pueden ser divididas en 2 categorías: De aplicación y De transporte de datos. Las primeras usualmente son implementadas únicamente

como software, mientras que las segundas, usualmente cuentan con implementaciones en hardware y software.

Las primeras 3 capas, Aplicación, Presentación y Sesión usualmente están implementadas en software e interactúan de alguna forma con el usuario.

Las capas de Transporte y red no interactúan directamente con el usuario y únicamente se encargan de preparar la información para las siguientes dos capas, que primordialmente están concretadas en hardware. Como se muestra en la Figura 2.2.9.

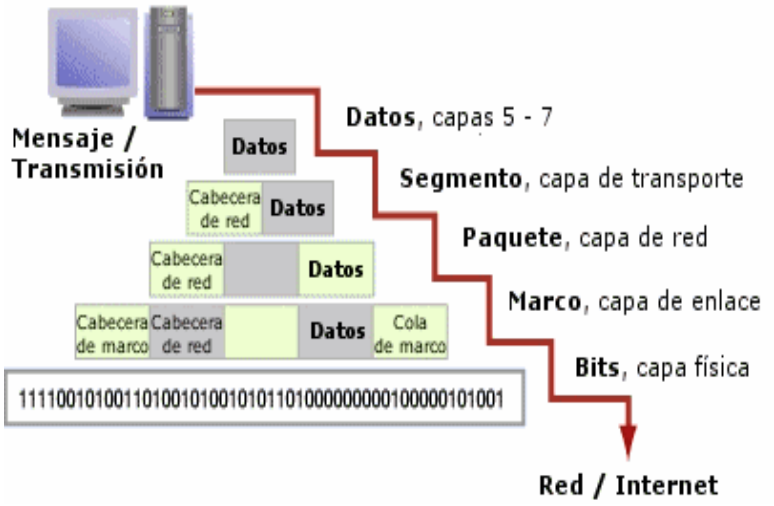


Figura 2.2.9 ejemplo de interacción entre las capas de transporte y red

2.3 TRANSMISIÓN DE DATOS EN EL MODELO OSI

La capa “n” de un computador se comunica con la capa “n” de otro computador, utilizando protocolos de la capa “n”.

Por otra parte, cada capa de protocolos le pasa datos a la siguiente capa, ésta les añade datos propios de control y se los pasa a la siguiente capa, formando así una cadena. De esta forma, cada capa forma unidades de datos, que contienen los datos tomados de la capa anterior y los propios que les ha añadido ella, denominándose al conjunto obtenido PDU (unidades de datos del protocolo).

La idea clave en todo este proceso es que aunque la transmisión real de los datos es vertical, cada capa se programa como si fuera horizontal.

Ejemplo de cómo trabaja el modelo OSI

El modelo de referencia consiste en 7 capas. Estas capas se visualizan generalmente como un montón de bloques apilados o en ingles como un "stack of blocks", por lo que en ingles, a esto se le conoce como el "OSI Protocol Stack".

En este modelo, sólo las capas que tengan otra capa equivalente en el nodo remoto podrán comunicarse, esto es, sólo las capas que son iguales entre si se comunican entre si. El protocolo de cada capa sólo se interesa por la información de su capa y no por la de las demás, por ejemplo: El e-mail es un protocolo de aplicación que se comunica sólo con otros protocolos de la información se pasa a las capas de abajo hasta que la información llega a la red. En el nodo remoto, la información es entonces pasada hacia arriba hasta que llega a la aplicación correspondiente. Cada capa confía en que las demás harán su trabajo, una capa no se interesa por el funcionamiento de las demás, lo único que es de interés es la forma en como los datos serán pasados hacia arriba o hacia abajo. Figura 2.3.1.

La forma de lograr esto es empacando y desempacando información en los mensajes que se van a enviar, así el e-mail le da una información a la capa de TCP, la cual agrega información y se la pasa a la capa de IP, la cual agrega mas información y se la pasa a la de ethernet, la cual agrega más información y la transmite a la red como se puede apreciar en la figura 2.3.2.

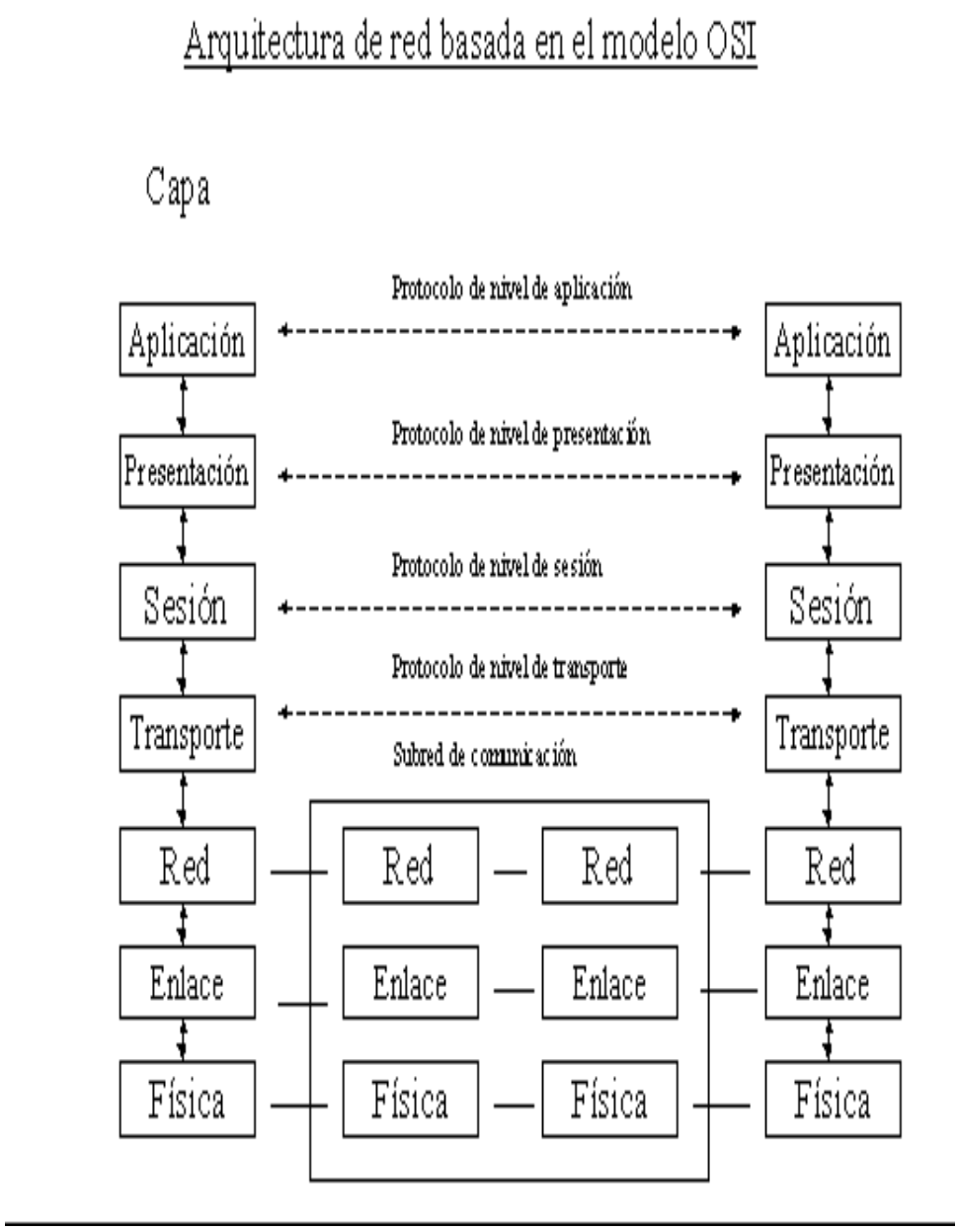


Figura 2.3.1 modelo de arquitectura de red en el modelo OSI

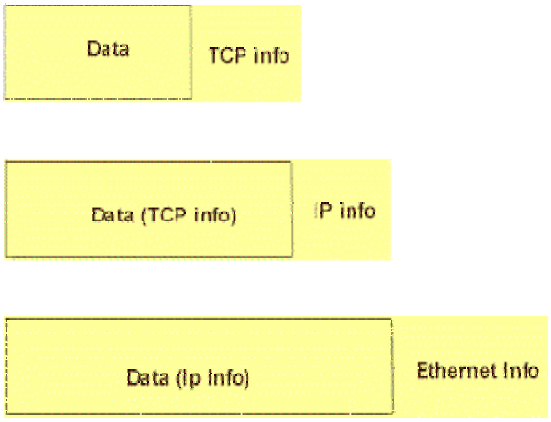


Figura 2.3.2. Si seguimos este método de empacar y desempacar llegará un momento en que a las capas mas altas casi no llegue información, este es uno de los aspectos que la capa de transporte y sesión tienen que resolver.

Capa Física

La Capa física de el modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, en este nivel están, por ejemplo, los estándares de cable de par trenzado que se deben de usar para conectar una red, la forma en que las antenas de microondas deben de estar orientadas para comunicarse, y las características de propagación de ondas radiales.

Capa de enlace de datos

La capa de enlace de datos, provee la transmisión de los Bits en "frames" de información, es quien checa que los bits lleguen libres de errores a su destino y controla las secuencias de transmisión y los "acuses de recibo" de los mensajes recibidos. También se encarga de retransmitir los paquetes o frames que no han sido "acusados" por el otro extremo. Este nivel controla el flujo de información entre dos nodos de la red.

Por lo que este nivel sólo se encarga de la transmisión y recepción de datos entre dos nodos colindantes, y no es quién redirige o re-enruta paquetes (ese es el siguiente

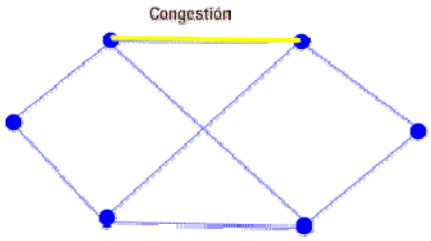
nivel, el nivel de red). Un ejemplo de el nivel de enlace de datos es el Standard de ETHERNET o el de ATM.

Capa de red y de transporte

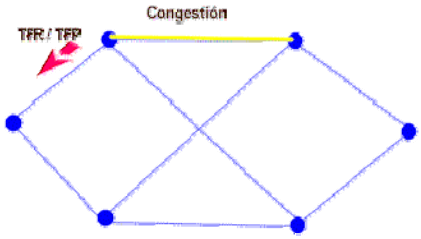
Las capas tres y cuatro manejan lo que comúnmente conocemos como "Networking" o manejo de red. Es aquí donde se definen las rutas, destinos y caminos de llegada de un punto a otro de la red. Esto es comúnmente lo que manejan las capas de TCP/IP. Todo lo referente a los ROUTERS, BRIDGES IP ADDRESS, IP MASK, ETC pertenece a este nivel.

La capa 3

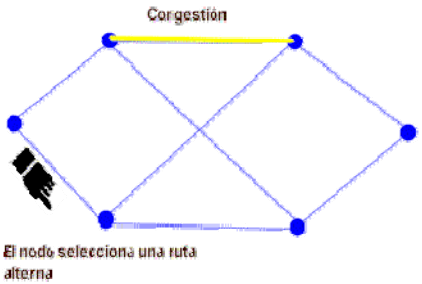
Un destino es un punto valido en la red donde los mensajes pueden llegar y ser enviados. Para llegar a un destino, debe de existir una ruta de comunicación, por lo general los puntos aislados de la red sólo apuntan a una dirección default (que se llama el default gateway). En una redecita esto significa el ROUTER más cercano. Este router tiene las direcciones más conocidas de la red y el enlace que conduce a ellas. Si la dirección que se le manda no es conocida por el router, éste también tiene un Default Gateway que es un Router en la una red más grande, así se va pasando de router a router mayor. Hasta llegar al Internet backbone, que es una red de SUPER ROUTERS que tienen todas las direcciones de Internet y el Super router más cercano a ellas.



Un nodo de la red se da cuenta de que existe congestión en uno de sus enlaces (esto es informado por la capa dos, una forma en que se puede determinar es monitoreando el tamaño de el buffer de retransmisión).



El nodo congestionado manda un mensaje de transferencia restringida (TFR), a los nodos vecinos, los que al recibirlo escogen una ruta alterna para mandar sus mensajes.



Si la congestión es severa o el enlace se pierde, entonces se manda un mensaje de transferencia prohibida (TFP), en este mensaje se envía el último FSK recibido. Los nodos vecinos, al recibir este mensaje, retransmiten todos los mensajes de él buffer de retransmisión que no hayan sido acusados de recibo en la ruta alterna. (para esto usan la información recibida en el TFP).

Una vez que la comunicación se restablece, el nodo afectado manda un mensaje de transferencia aceptada (TFA) a los nodos vecinos, los cuales usan esta ruta otra vez.

Las funciones de esta capa también pueden ser capaces de reconfigurar la red para que los datos fluyan por un camino u otro si es que un enlace se cae. Enseguida se presenta un ejemplo de como es posible esto (Ejemplo basado en un sistema telefónico CCs No.7).

La capa 4

Ahora, si mandamos un archivo grande, este archivo deberá de ser dividido en pedazos que puedan ser transmitidos por la red, estos pedazos viajan por la red y al llegar al destino deben de ser acomodados de la manera en que fueron enviados (pueden

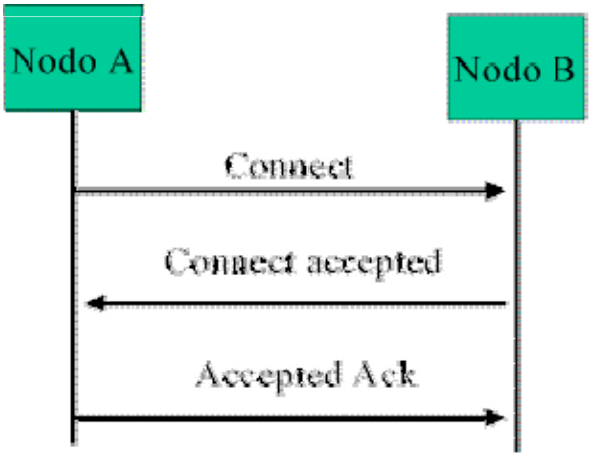
llegar desacomodados por que pueden tomar diferente ruta si acaso una se congestiona o se cae). La forma de reacomodar los paquetes, cuanto tiempo y como esperar por ellos son las funciones de la capa 4.

Capas de sesión y presentación

Capa de sesión

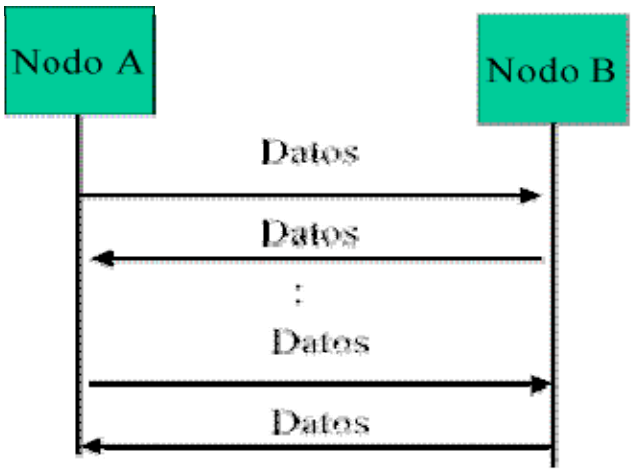
Ya vimos como el sistema de telecomunicaciones transporta los datos y mantiene la red confiablemente. Pero ¿quien ordena o decide a donde deben de ir los datos?, además ¿quien indica cuantos datos se habrá de enviar o recibir en cierto destino de la red?. Estas son las operaciones de la capa de sesión.

Una comunicación en la red tiene dos tipos. Con conexión lógica (conection oriented, como el TCP) o sin conexión lógica entre los nodos (conection less como el UDP).



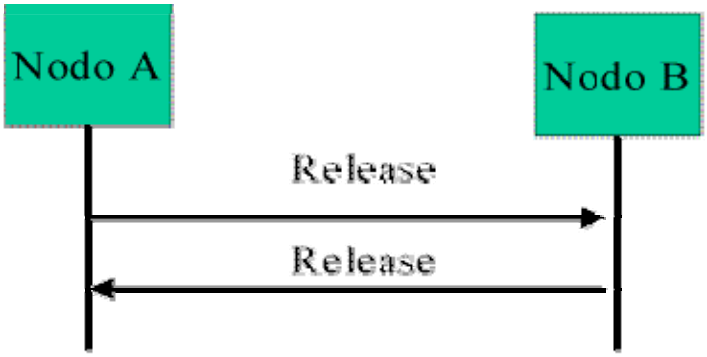
Establecimiento de una conexión lógica

En la comunicación con conexión primero se establece un conexión lógica (una serie de mensajes se envían para saber primero si es que podemos establecer la comunicación entre los nodos).



Intercambio de datos en comunicación

Una vez que la comunicación ha sido establecida, entonces los datos fluyen entre los dos destinos de la red.



Liberación de la conexión

Cuando la comunicación ya no es necesaria entonces la conexión se libera.

Este tipo de comunicación nos da la certidumbre de que el nodo remoto nos esta oyendo, aunque se pierde un tiempo y procesamiento en establece y liberar la conexión entre dos nodos.

Noten que en las gráficas sólo se ven dos nodos adyacentes, los nodos pueden ser parte de una red y tener muchos nodos entre ellos, sin embargo en este nivel esos nodos son irrelevantes. Esta es una de las características del modelo de referencia OSI, a cierto nivel sólo se ve lo relevante, lo que esta abajo se toma por hecho que existe y no es necesario ni siquiera el mencionarlo.

En la comunicación sin conexión solamente enviamos los datos al nodo remoto y no sabemos a ciencia cierta si el nodo nos escucha o no, sin embargo se ahorra tiempo y

procesamiento por que no necesitamos establecer ni liberar conexiones. este tipo de comunicaciones es muy usado en las redes que son muy confiables (Como la red de señalización telefónica C7).

Capa de presentación

Un protocolo de telecomunicaciones debe de ser diseñado para que diferentes versiones y sistema lo puedan usar, de modo que los datos se deben de tener en un formato definido y documentado. Por ejemplo una página de HTML debe de tener campos como el puerto, la dirección de URL, y el texto del mensaje. Esos campos serán transmitidos como bits y bytes y hay un documento (el estándar de HTML) que me indica en que parte del mensaje va cada pedazo de la página.

Precisamente de esto es lo que se encarga la capa de presentación, recibe bits y bytes de las aplicaciones y las formatea de modo que sean octetos entendibles en una red. Recibe un mensaje con octetos de una red y los decodifica para que se conviertan en bits y bytes de una aplicación.

Capa de aplicación

Todas las capas anteriores en este modelo sirven de mera infraestructura de telecomunicaciones. Por si solas no hacen nada más que mantener en buen estado el camino para que fluyan los datos, la capa que hace posible que una red se pueda usar es la capa de aplicación.

Es aquí donde lo visible y lo más orientado al usuario se genera. A esta capa pertenecen por ejemplo los Web Browsrs, El FTP, el e-mail, el telnet, las presentaciones de shockwave, los java applets y demás.

Una aplicación en Java sólo tiene que saber en que dirección y en que puerto se localiza el nodo remoto y ordenar a las demás capas (por medio de un TCP API) que vayan a ese nodo remoto y le envíen información.

Hasta aquí hemos explicado de qué consiste cada una de las capas del modelo de referencia OSI observe la imagen 2.3.2 en la cual se resume las capas del modelo OSI. En estos campos se han hecho ya muchas investigaciones, sin embargo existe aun mucho por explorar e investigar en las capas superiores de este modelo. Los temas de transmisión, de red y de transporte llevan alrededor de 30 años de estudios, sin embargo las aplicaciones en Internet son relativamente jóvenes, es ahí donde hay oportunidad de desarrollo y de ganancia.

Capa de aplicación	Es el nivel último de la capa, el que aloja el programa de red que interactúa con el usuario.
Capa de presentación	Maneja los datos de la aplicación y los acomoda en un formato que pueda ser transmitido en una red.
Capa de sesión	Establece conexiones lógicas entre puntos de la red.
Capa de transporte	Maneja la entrega entre un punto y otro de la red de los mensajes de una sesión.

Capa de red	Maneja destinos, rutas, congestión en rutas, alternativas de enrutamiento, etc.
Capa de enlace de datos	Entrega los datos entre un nodo y otro en un enlace de red
Capa Física	Define la conexión física de la red

Figura 2.3.2 capas del modelo OSI

2.4 EQUIPO DE COMUNICACIÓN DE NIVEL RED.

Ruteadores (Routers)

Son dispositivos inteligentes que trabajan en el Nivel de Red del modelo de referencia OSI, por lo que son dependientes del protocolo particular de cada red. Envían paquetes de datos de un protocolo común, desde una red a otra.

Convierten los paquetes de información de la red de área local, en paquetes capaces de ser enviados mediante redes de área extensa. Durante el envío, el ruteador examina el paquete buscando la dirección de destino y consultando su propia tabla de direcciones, la cual mantiene actualizada intercambiando direcciones con los demás ruteadores para establecer rutas de enlace a través de las redes que los interconectan. Este intercambio de información entre ruteadores se realiza mediante protocolos de gestión propietarios.

Fig. 2.4.1Representación física de un ruteador

Aplicaciones

Por su posibilidad de segregar tráfico administrativo y determinar las rutas más eficientes para evitar congestión de red, son una excelente solución para una gran interconexión de redes con múltiples tipos de LANs, MANs, WANs y diferentes protocolos un ejemplo de ello es mostrado en la figura 2.4.2. Es una buena solución en redes de complejidad media, para separar diferentes redes lógicas, por razones de seguridad y optimización de las rutas.

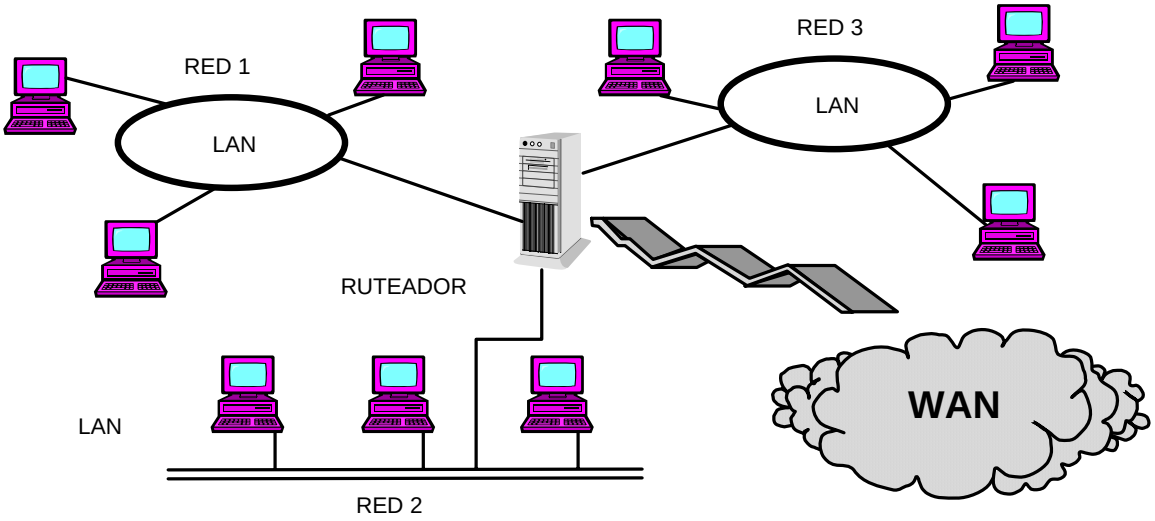


Fig. 2.4.2 Interconexión de redes utilizando ruteadores

Principales funciones de un ruteador

Los ruteadores a diferencia de los puentes, trabajan en el nivel 3 (capa de red) de OSI y toman decisiones de encaminamiento.

Las principales funciones que ha de realizar un ruteador son:

- Establecer un enlace entre LAN's. Como mínimo se necesita un control de la conexión a nivel físico y de enlace.
- Establecer procedimientos de encaminamiento entre diferentes máquinas de diferentes LAN's.
- Controlar la existencia y la disponibilidad de las redes de interconexión que permiten comunicar dos LAN's.

- Proporcionar las siguientes funciones sin la necesidad de modificar la arquitectura de las LAN's conectadas, es decir de una manera transparente:
- Gestión de diferentes esquemas de direccionamiento empleados por las redes de interconexión.
- Uso de diferentes longitudes de paquetes, por lo que necesita de recursos para la segmentación.
- Diferentes interfaces de red.
- Gestión de diferentes time-out.
- Capacidad de recuperar errores en las comunicaciones internas.
- Control del estado de las redes de interconexión.
- Técnicas de encaminamiento que permiten evitar situaciones de congestión, y minimizar de alguna manera el costo en tiempo o en utilización de recursos.
- Control de acceso, ya que cada red tiene sus propias técnicas de control de acceso a los usuarios.
- Proporcionar servicios orientados a conexión o a modo datagrama.

Ventajas

Algunas ventajas de la utilización de ruteadores, se describen a continuación:

- Seguridad. Permiten el aislamiento de tráfico, y los mecanismos de encaminamiento facilitan el proceso de localización de fallos en la red.
- Flexibilidad. Las redes interconectadas con ruteador no están limitadas en su topología, siendo estas redes de mayor extensión y más complejas que las redes enlazadas con puente.
- Soporte de Protocolos. Son dependientes de los protocolos utilizados, aprovechando de una forma eficiente la información de cabecera de los paquetes de red.
- Relación Precio / Eficiencia. El costo es superior al de otros dispositivos, en términos de precio de compra, pero no en términos de explotación y mantenimiento para redes de una complejidad mayor.

- Control de Flujo y Encaminamiento. Utilizan algoritmos de encaminamiento adaptativos (RIP, OSPF, etc. Ver capítulo 3), que gestionan la congestión del tráfico con un control de flujo que redirige hacia rutas alternativas menos congestionadas.

Desventajas

Algunas desventajas que se presentan al utilizar ruteadores se listan a continuación:

- Lentitud de proceso de paquetes respecto a los puentes.
- Necesidad de gestionar el subdireccionamiento en el Nivel de Enlace.
- Precio superior a los puentes.

Enrutamiento.

La función principal del nivel de red en Internet es hacer llegar los paquetes de un computador a otro dando igual cual sea el medio físico que utilicen y los datos que estén transmitiendo, el enrutamiento es justamente eso. Una computador tiene que conocer que computador están en su red, y también debe conocer el computador o computadores a la que debe enviar los paquetes aunque estas que no estén en su red (router, gateway). Así sabrá que debe hacer con cada paquete que quiera enviar observe la figura 2.4.3. Existen varias formas de enrutar paquetes por Internet, el uso de una no excluye de otra, seria muy raro que un paquete que recorre una distancia larga no pasara por todas ellas o por lo menos por las más conocidas.

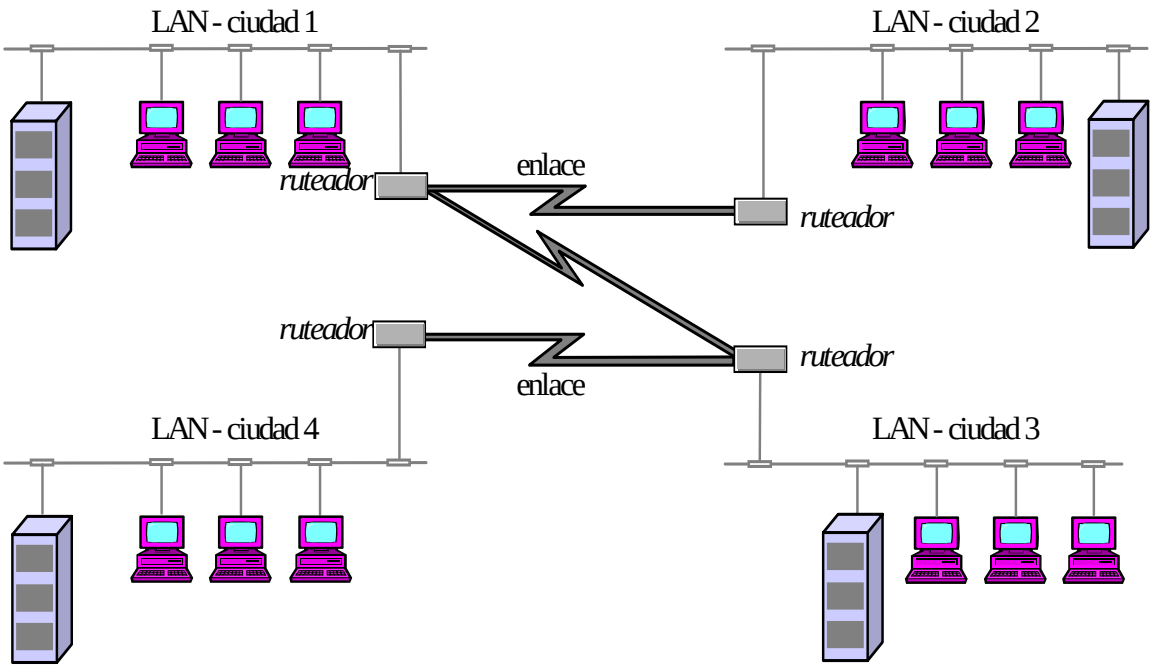


Fig. 2.4.3 Ejemplo del uso de ruteadores

Entrega directa.

La entrega directa se realiza cuando dos hosts (un host es todo aquel dispositivo que se le pueda asignar una LAN o una configuración IP) que se comunican están en la misma red física, por lo que los paquetes se entregan de forma directa, sin pasar por routers.

Salto al siguiente.

Es la forma más sencilla de enrutamiento, es usado en redes pequeñas que saben que todo lo que no esté en su red se lo va a tener que pasar a otro router mejor conectado. Por ejemplo si tenemos dos redes (A y B), A tiene un router hacia Internet y otro hacia la otra red. B sólo tiene un router hacia la otra red (el router que conecta A y B es uno sólo). El router A-B conoce las máquinas de la red de A y las de la red de B,

por lo que si le piden que enrute una dirección que no está ni en A ni en B lo tendrá que pasar al router A-Internet.

2.5 RIP (ROUTING INFORMATION PROTOCOL, PROTOCOLO DE INFORMACIÓN DE ENRUTADO).

RIP es un protocolo de enrutado interno, es decir para la parte interna de la red, la que no está conectada al backbone de Internet. Es muy usado en sistemas de conexión a internet como infovia, en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos.

Cuando un usuario se conecta el servidor de terminales (equipo en el que finaliza la llamada) avisa con un mensaje RIP al router más cercano advirtiendo de la dirección IP que ahora le pertenece.

Así podemos ver que RIP es un protocolo usado por distintos routers para intercambiar información y así conocer por donde deberían enrutar un paquete para hacer que éste llegue a su destino.

OSPF (Open shortest path first, el camino más corto primero).

OSPF se usa, como RIP, en la parte interna de las redes, su forma de funcionar es bastante sencilla. Cada router conoce los routers cercanos y las direcciones que posee cada router de los cercanos. Además de esto cada router sabe a que distancia (medida en routers) está cada router. Así cuando tiene que enviar un paquete lo envía por la ruta por la que tenga que dar menos saltos.

Así por ejemplo un router que tenga tres conexiones a red, una a una red local en la que hay puesto de trabajo, otra (A) una red rápida frame relay de 48Mbps y una línea (B) RDSI de 64Kbps. Desde la red local va un paquete a W que esta por A a tres saltos y por B a dos saltos. El paquete iría por B sin tener en cuenta la saturación de la línea o el ancho de banda de la línea.

La O de OSPF viene de abierto, en este caso significa que los algoritmos que usa son de disposición pública.

BGP (Border gateway protocol, protocolo de la pasarela externa).

BGP es un protocolo muy complejo que se usa en la interconexión de redes conectadas por un backbone de internet. Este protocolo usa parámetros como ancho de banda, precio de la conexión, saturación de la red, denegación de paso de paquetes, etc. para enviar un paquete por una ruta o por otra. Un router BGP da a conocer sus direcciones IP a los routers BGP y esta información se difunde por los routers BGP cercanos y no tan cercanos. BGP tiene sus propios mensajes entre routers, no utiliza RIP.

Dispositivos de interconexión

Para superar las limitaciones físicas de los elementos básicos de una red tales como: omputadoras personales, minicomputadoras, terminales interactivas, elementos de memoria, impresoras, dispositivos de telecomunicaciones, etc., conectados entre sí, que permite a los usuarios tener transferencia de datos y compartir recursos de hardware y de software, existen dispositivos de interconexión cuyas, funciones son las de extender las topologías de red. Estos elementos son: servidores, concentradores o hubs, repetidores, puentes o bridges, encaminadores o routers y pasarelas o gateways.

La principal diferencia entre ellos está en el nivel del modelo de referencia OSI en el que operan, por ejemplo, los repetidores operan en el nivel de la capa física, los puentes operan en el nivel de la capa de enlace de datos, y los ruteadores que operan en el nivel de la capa de red. Ver Figura 2.5.1.

Funciones básicas de los dispositivos de interconexión

Los dispositivos de interconexión de redes proporcionan algunas (o todas) de las siguientes funciones básicas:

Extensión de la red. Permiten ampliar el rango de distancia que puede alcanzar una red.

Definición de segmentos dentro de la red. Al dividir la red en segmentos se consigue aumentar las prestaciones de la red ya que cada tramo soporta sólo su propio tráfico y no los de los otros segmentos.

Separación entre redes. Mediante estos dispositivos las grandes redes se pueden componer de otras más pequeñas interconectadas entre sí, de forma transparente para el usuario. Varias redes físicas pueden combinarse para formar una única red lógica.

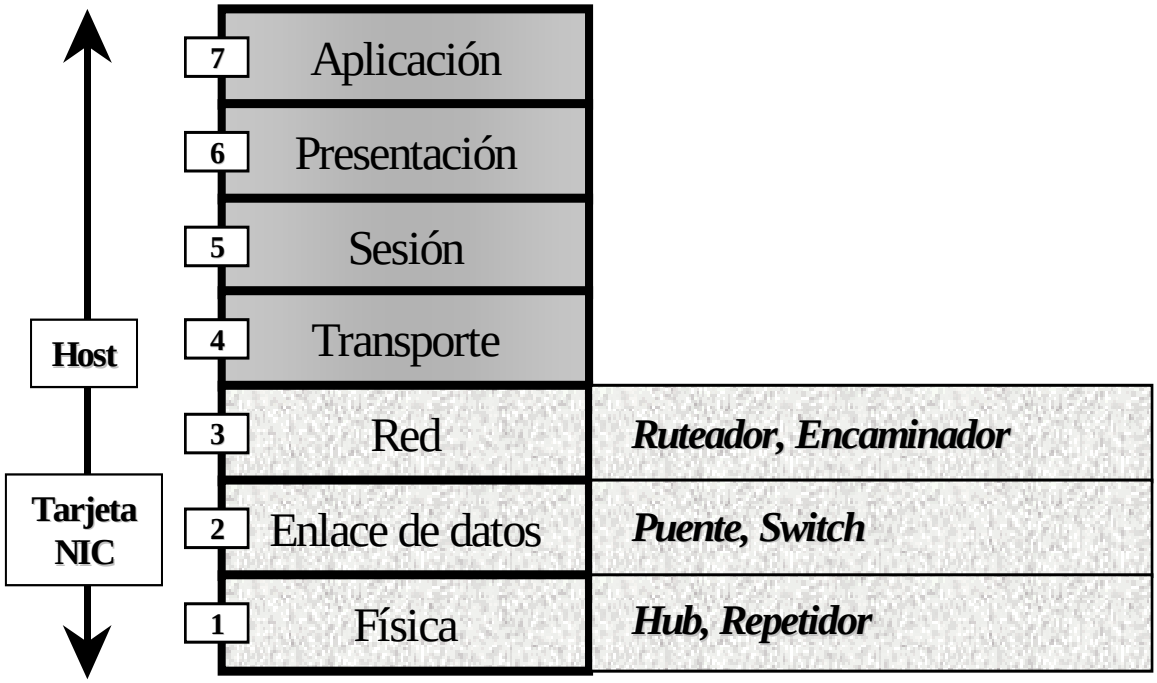


Figura 2.5.1 Dispositivos de interconexión en el modelo de referencia OSI

2.6 “LMDS” (“LOCAL MULTIPOINT DISTRIBUTION SERVICE, SISTEMA DE DISTRIBUCIÓN LOCAL DE SERVICIO MULTIPUNTO”)

LMDS ó Local Multipoint Distribution Service (Sistema de Distribución Local de Servicio Multipunto) es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a Internet, comunicaciones de datos en redes privadas, y video bajo demanda.

Del nombre de la tecnología se dice que es "Multipunto", que quiere decir que se hace una transmisión vía radio hacia múltiples instalaciones de abonado desde un sólo punto, la estación base, mientras que desde los abonados a la base se hace de manera punto a punto. Una base puede tener varios sectores, y cada sector, un área de cobertura del sistema multipunto.

Está concebida de una manera celular, esto es, existen una serie de antenas fijas (no móviles) en cada estación base, que son los sectores que prestan servicio a determinados núcleos poblacionales (usuarios agrupados geográficamente dentro de una determinada zona de cobertura), lo cual resulta muy apetecible para las operadoras, puesto que se evitan los costosos cableados de fibra óptica o de pares de cobre necesarios para dar cobertura a zonas residenciales/empresariales. Así por ello, es muy fácil y rápido desplegar esta tecnología por la zona, ya que sólo requiere de una o varias estación base, de antenas colocadas estratégicamente en los emplazamientos de las estaciones base, y de circuitos troncales punto a punto para interconectar las bases entre sí, asegurando la escalabilidad de la red montada según demanda geográfica o de mercado.

No obstante, cada vez está siendo más utilizada la tecnología portátil WiMAX, que no necesita teléfono móvil y funciona con LMDS.

2.7 CARACTERÍSTICAS DEL LMDS (“LOCAL MULTIPOINT DISTRIBUTION SERVICE, SISTEMA DE DISTRIBUCIÓN LOCAL DE SERVICIO MULTIPUNTO”)

LMDS usa señales en la banda de las microondas, en concreto la banda Ka (en torno a los 28 Ghz y además dependiente de las licencias de uso de espectro radioeléctrico del país), por lo que las distancias de transmisión son cortas (a esto se debe la palabra "Local" en el nombre de la tecnología), debido a que a tan altas frecuencias la reflexión de las señales es considerable (nótese que la banda Ka, es la banda del espectro usado para las comunicaciones satelitales). Pero también en muchos países europeos, se trabaja en 3,4 - 3,5GHz

A continuación, una tabla con las bandas de frecuencia (van separados en dos bloques, ya que usan unas N "rebanadas" de frecuencia para usar en total un ancho banda X) que son las asignadas por la FCC (Federal Communications Commision), y que se pretenden que sea el Standard:

Bloque A

Frecuencias	->	Ancho de Banda usado		
27,500	-	28,350 GHz	->	850 MHz
29,100	-	29,250 GHz	->	150 MHz
31,075	-	31,225 GHz	->	150 Mhz
Total Ancho de Banda del Bloque A:				1150 Mhz

Bloque B

Frecuencias	->	Ancho de Banda usado		
31,000	-	31,075 GHz	->	75 MHz
31,225	-	31,300 GHz	->	75 MHz
Total Ancho de Banda del Bloque B:				150 Mhz

Como se comentó antes, la reflexión en las señales de alta frecuencia es enorme, ya que son incapaces de atravesar obstáculos, cosa que si es posible con las señales de baja frecuencia; debido a esto, desde la estación base hasta la antena de abonado ha de estar totalmente libre de obstáculos o no habrá servicio. Puesto que es lógico pensar, la orografía/geografía de la zona a la que hay que desplegar la tecnología LMDS juega un papel muy importante a tener en cuenta. En general, pueden formarse unas zonas de sombra (zonas "imposibles" de ofrecer servicio), pero éstas se pueden paliar con la

colocación estratégica de las estaciones base/antenas para que una misma zona tenga acceso a varias células y también mediante el uso de amplificadores y reflectores.

Otro problema a tener en cuenta es la derivación de la energía de la señal transmitida en la molécula de agua (recordemos que estamos hablando de microondas), por lo que la potencia de la señal se reduce. Este efecto se palia mediante la subida de la potencia entregada y/o la reducción del tamaño de la célula.

Esta interactuación con la molécula de agua, invita a pensar que en condiciones lluviosas el servicio LDMS se cae, y es cierto; es lo que se le denomina en inglés "rainfall" y para conseguir que el usuario reciba señal en estas condiciones se usa la corrección de errores hacia adelante, la adaptación dinámica de potencia y la adaptación dinámica de la modulación usada.

2.8 Wi-Fi (WIRELESS FIDELITY, FIDELIDAD INALAMBRICA)

Wi-Fi acrónimo de Wireless Fidelity, es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11. 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. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todas los mismos protocolos. El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. En la actualidad no se fabrican productos sobre este estándar. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11legacy." La siguiente modificación apareció en 1999 y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabajaba en la frecuencia de 2,4 GHz. También se realizo una especificación sobre una frecuencia de 5 Ghz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la b y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporo un

estándar a esa velocidad y compatible con el b que recibiría el nombre de 802.11g. En la actualidad la mayoría de productos son de la especificación b y de la g (Actualmente se está desarrollando la 802.11n, que se espera que alcance los 500 Mbps). La seguridad forma parte del protocolo desde el principio y fue mejorada en la revisión 802.11i. Otros estándares de esta familia (c–f, h–j, n) son mejoras de servicio y extensiones o correcciones a especificaciones anteriores. El primer estándar de esta familia que tuvo una amplia aceptación fue el 802.11b. En 2005, la mayoría de los productos que se comercializan siguen el estándar 802.11g con compatibilidad hacia el 802.11b.

Los estándares 802.11b y 802.11g utilizan bandas de 2,4 gigahercios (Ghz) que no necesitan de permiso para su uso. El estándar 802.11a utiliza la banda de 5 GHz. Las redes que trabajan bajo los estándares 802.11b y 802.11g pueden sufrir interferencias por parte de hornos microondas, teléfonos inalámbricos y otros equipos que utilicen la misma banda de 2,4 Ghz.

Wi-Fi se creó para ser utilizada en redes locales inalámbricas, pero es frecuente que en la actualidad también se utilice para acceder a Internet.

Normalización

Hay, al menos, dos tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11.

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

En los Estados Unidos y Japón, IEEE 802.11a, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. En otras zonas, como la Unión Europea, 802.11a no está aprobado todavía para operar en la banda de 5 GHz, y los reguladores europeos están todavía considerando el uso del estándar europeo.

2.9 HIPERLAN.

HIPERLAN es un estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54 Mbps en la frecuencia de banda de 5 GHz. HIPERLAN/2 es una solución estándar para un rango de comunicación corto que permite una alta transferencia de datos y Calidad de Servicio del tráfico entre estaciones base WLAN y terminales de usuarios. La seguridad esta provista por lo último en técnicas de encriptación y protocolos de autenticación.

HIPERLAN es similar a 802.11a (5 GHz) y es diferente de 802.11b/g (2,4 GHz). HIPERLAN/1, HIgh Performance Radio LAN version 1 es un estándar del ETSI (European Telecomunications Standards Institute , Instituto Europeo Estándar de Telecomunicaciones).

El plan empezó en 1991. El objetivo de HIPERLAN era la alta velocidad de transmisión, más alta que la del 802.11. El estándar se aprobó en 1996.

El estándar cubre las capas física y MAC como el 802.11. Hay una nueva subcapa llamada “channel access and control sublayer, canal de acceso y control de subcapa” (CAC). Esta subcapa maneja las peticiones de acceso a los canales. La aceptación de la petición depende del uso del canal y de la prioridad de la petición. La capa CAC proporciona independencia jerárquica con un mecanismo de “elimination-yield non-preemptive multiple access , eliminación no preventiva de acceso multiple” (EY-NPMA). EY-NPMA codifica las prioridades y demás funciones en un pulso de radio de longitud variable que precede a los datos.

EY-NPMA permite trabajar a la red con pocas colisiones aunque halla un gran número de usuarios. Las aplicaciones multimedia funcionan en HIPERLAN gracias al mecanismo de prioridades del EY-NPMA. La capa MAC define protocolos para enrutado, seguridad y ahorro de energía y proporciona una transferencia de datos natural a las capas superiores.

En la capa física se usan modulaciones FSK y GMSK.

Características de HIPERLAN:

- rango 50 m
- baja movilidad (1.4 m/s)

- soporta tráfico asíncrono y síncrono.
- sonido 32 Kbps, latencia de 10 ns
- vídeo 2 Mbit/s, latencia de 100 ns
- datos a 10 Mbps

HIPERLAN no interfiere con hornos microondas y otros aparatos del hogar, que trabajan a 2.4 GHz.

Wi-Fi y las tecnologías de consumo relacionadas tienen la llave para reemplazar a las redes de telefonía móvil como GSM. Algunos obstáculos para que esto ocurra en el futuro próximo son la pérdida del roaming y de la autenticación y la estrechez del espectro disponible.

Seguridad

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes se han instalado por administradores de sistemas o de redes por su simplicidad de implementación, sin tener en consideración la seguridad y por tanto han convertido sus redes en redes abiertas, sin proteger el acceso a la información que por ellas circulan. Existen varias alternativas para garantizar la seguridad de estas redes, las más comunes son la utilización de protocolos de encriptación de datos como el WEP y el WPA, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) y 802.1x, proporcionados por o mediando otros dispositivos de la red de datos.

WEP, acrónimo de Wired Equivalency Privacy

Es sistema de cifrado incluido en el estándar 802.11 como protocolo para redes Wireless que permite encriptar la información que se transmite. Proporciona encriptación a nivel 2. Está basado en el algoritmo de encriptación RC4, y utiliza claves de 64bits, de 128bits o de 256 bits.

Actualmente hay un sistema de cifrado mejor para redes WiFi, con las siglas WPA, surgido para solucionar los problemas de seguridad encontrados en WEP.

WPA (Wi-Fi Protected Access - Acceso Protegido Wi-Fi)

Es un sistema para asegurar redes inalámbricas (Wi-Fi), creado para corregir la seguridad del sistema previo, WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado); investigadores han encontrado varias debilidades en WEP (tal como un ataque estadístico que permite recuperar la llave WEP). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era preparado. WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).

WPA fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x); sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (PSK - Pre-Shared Key). La información es cifrada utilizando el algoritmo RC4, con una llave de 128 bits y un vector de inicialización de 48 bits.

Una de las mejoras sobre WEP es dado por el Protocolo de Integridad de Clave Temporal (TKIP - Temporal Key Integrity Protocol), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con una vector de inicialización (IV) mucho mas grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

Adicional a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. El chequeo de redundancia cíclica (CRC - Cyclic Redundancy Check) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la llave WEP. WPA implementa un chequeo de integridad del mensaje (MIC - Message Integrity Check) llamado "Michael". Adicionalmente WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.

Al incrementar el tamaño de las llaves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el mas fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas mas viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, las redes WPA se desconectan por 30 segundos cada vez que se detecta un intento de ataque.

WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no soporta todas las características, WPA2 ya implementa el estándar completo. Particularmente WPA no se puede utilizar en redes Ad-Hoc (IBSS), solo en redes BSS; WPA2 ya puede utilizar tanto en IBSS (Ad-Hoc) como en BSS.

El estándar 802.11i fue ratificado en Junio de 2004.

La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x WPA-Enterprise y WPA2-Enterprise

2.10 IPSEC

IPsec es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a IPv4. La arquitectura IPsec se describe en el RFC2401. Los siguientes párrafos dan una pequeña introducción a IPsec.

IPsec emplea dos protocolos diferentes - AH y ESP - para asegurarla autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. Estos modos se denominan, respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec. En modo transporte IPsec sólo maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores. Como se muestra a continuación en la Figura 2.11.1.

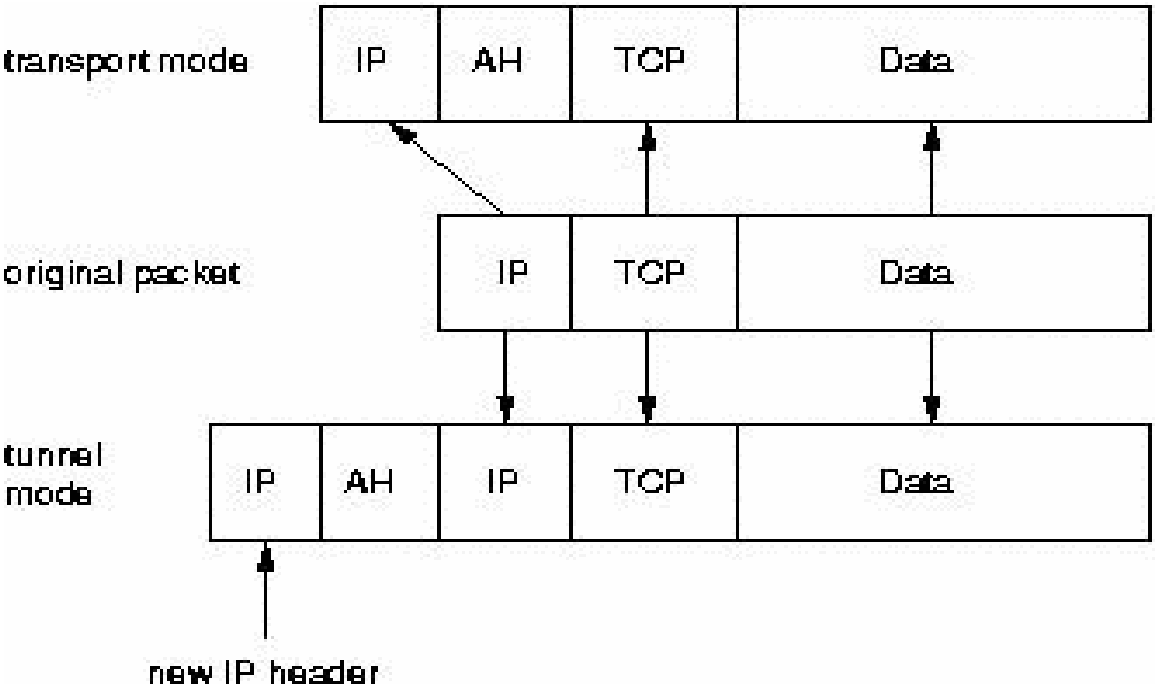


Figura 2.10.1. IPsec: modos túnel y transporte

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC - Hash Message Authentication Codes). Para el cálculo de estos HMAC los protocolos HMAC emplean algoritmos de resumen como MD5 y SHA para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPsec y el receptor del paquete puede comprobar el HMAC si tiene acceso a la clave secreta.

Para proteger la confidencialidad de lo datagramas IP, los protocolos IPsec emplean algoritmos estándar de cifrado simétrico. El estándar IPsec exige la implementación de NULL y DES. En la actualidad se suelen emplear algoritmos más fuertes: 3DES, AES y Blowfish.

Para protegerse contra ataques por denegación de servicio, los protocolos IPsec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

Para que los participantes de una comunicación puedan encapsular y desencapsular los paquetes IPsec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en asociaciones de seguridad (SA - Security Associations). Las asociaciones de seguridad, a su vez, se almacenan en bases de datos de asociaciones de seguridad (SAD - Security Asocciation Databases).

Cada asociación de seguridad define los siguientes parámetros:

- Dirección IP origen y destino de la cabecera IPsec resultante. Estas son las direcciones IP de los participantes de la comunicación IPsec que protegen los paquetes.
- Protocolo IPsec (AH o ESP). A veces, se permite compresión (IPCOMP).
- El algoritmo y clave secreta empleados por el protocolo IPsec.
- Índice de parámetro de seguridad (SPI - Security Parameter Index). Es un número de 32 bits que identifica la asociación de seguridad.

Algunas implementaciones de la base de datos de asociaciones de seguridad permiten almacenar más parámetros:

- Modo IPsec (túnel o transporte)
- Tamaño de la ventana deslizante para protegerse de ataques por repetición.
- Tiempo de vida de una asociación de seguridad.

En una asociación de seguridad se definen las direcciones IP de origen y destino de la comunicación. Por ello, mediante una única SA sólo se puede proteger un sentido del tráfico en una comunicación IPsec full duplex. Para proteger ambos sentidos de la comunicación, IPsec necesita de dos asociaciones de seguridad unidireccionales.

Las asociaciones de seguridad sólo especifican cómo se supone que IPsec protegerá el tráfico. Para definir qué tráfico proteger, y cuándo hacerlo, se necesita información adicional. Esta información se almacena en la política de seguridad (SP - Security Policy), que a su vez se almacena en la base de datos de políticas de seguridad (SPD - Security Policy Database).

Una política de seguridad suele especificar los siguientes parámetros:

- Direcciones de origen y destino de los paquetes por proteger. En modo transportes estas serán las mismas direcciones que en la SA. En modo túnel pueden ser distintas.
- Protocolos y puertos a proteger. Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege todo el tráfico entre las direcciones IP indicadas.
- La asociación de seguridad a emplear para proteger los paquetes.

La configuración manual de la asociación de seguridad es proclive a errores, y no es muy segura. Las claves secretas y algoritmos de cifrado deben compartirse entre todos los participantes de la VPN. Uno de los problemas críticos a los que se enfrenta el administrador de sistemas es el intercambio de claves: ¿cómo intercambiar claves simétricas cuando aún no se ha establecido ningún tipo de cifrado?

Para resolver este problema se desarrolló el protocolo de intercambio de claves por Internet (IKE - Internet Key Exchange Protocol). Este protocolo autentica a los participantes en una primera fase. En una segunda fase se negocian las asociaciones de seguridad y se escogen las claves secretas simétricas a través de un intercambio de claves Diffie Hellmann. El protocolo IKE se ocupa incluso de renovar periódicamente las claves para asegurar su confidencialidad.

Los protocolos IPsec

La familia de protocolos IPsec está formada por dos protocolos: el AH (Authentication Header - Cabecera de autenticación) y el ESP (Encapsulated Security Payload - Carga de seguridad encapsulada). Ambos son protocolos IP independientes. AH es el protocolo IP 51 y ESP el protocolo IP 50. Las siguientes secciones tratarán brevemente sobre sus propiedades:

AH - Cabecera de autenticación

El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y

las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete. La cabecera AH se muestra en la Figura 2.11.2.

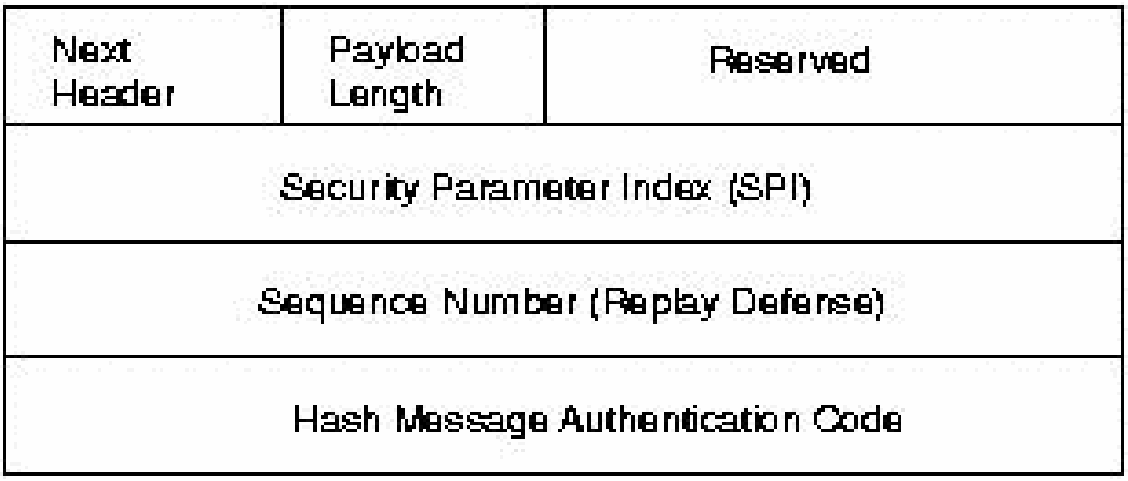


Figura 2.10.2. La cabecera AH protege la integridad del paquete

La cabecera AH mide 24 bytes. El primer byte es el campo Siguiente cabecera. Este campo especifica el protocolo de la siguiente cabecera. En modo túnel se encapsula un datagrama IP completo, por lo que el valor de este campo es 4. Al encapsular un datagrama TCP en modo transporte, el valor correspondiente es 6. El siguiente byte especifica la longitud del contenido del paquete. Este campo está seguido de dos bytes reservados. Los siguientes 4 bytes especifican en Índice de Parámetro de Seguridad (SPI). El SPI especifica la asociación de seguridad (SA) a emplear para el desencapsulado del paquete. El Número de Secuencia de 32 bit protege frente a ataques por repeticón. Finalmente, los últimos 96 bit almacenan el código de resumen para la autenticación de mensaje (HMAC). Este HMAC protege la integridad de los paquetes ya que sólo los miembros de la comunicación que conozcan la clave secreta pueden crear y comprobar HMACs.

Como el protocolo AH protege la cabecera IP incluyendo las partes inmutables de la cabecera IP como las direcciones IP, el protocolo AH no permite NAT. NAT (Network address translation - Traducción de direcciones de red, también conocido como Enmascaramiento de direcciones) reemplaza una dirección IP de la cabecera IP (normalmente la IP de origen) por una dirección IP diferente. Tras el intercambio, la HMAC ya no es válida. La extensión a IPsec NAT-transversal implementa métodos que evitan esta restricción.

ESP - Carga de Seguridad Encapsulada

El protocolo ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. La cabecera ESP consta de dos partes y se muestra en Figure 2.10.3.

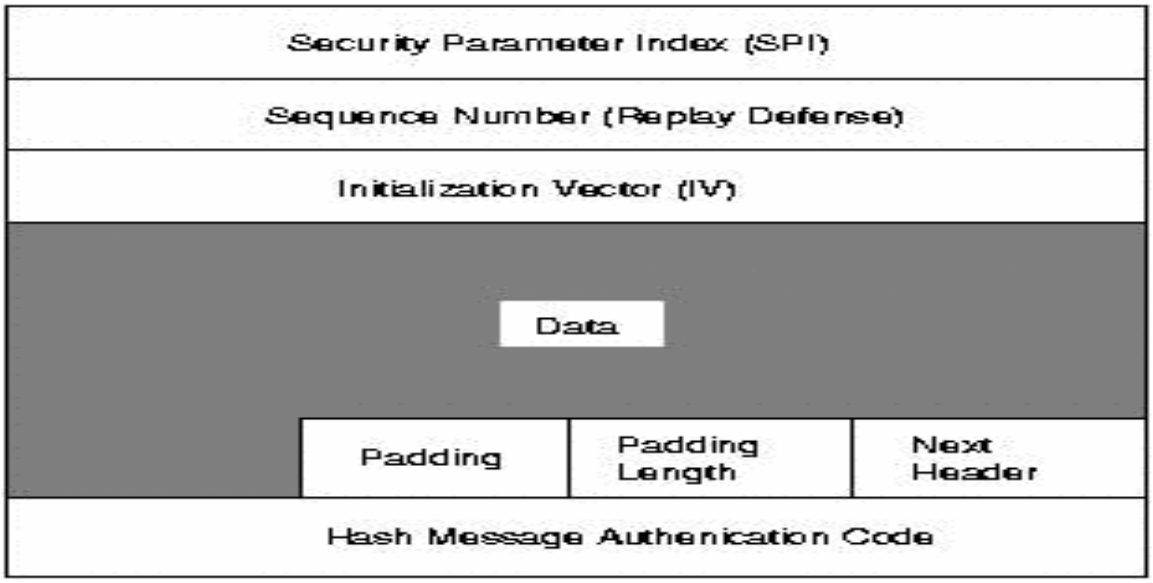


Figure 2.10.3. La cabecera ESP

Los primeros 32 bits de la cabecera ESP especifican el Índice de Parámetros de Seguridad (SPI). Este SPI especifica qué SA emplear para desencapsular el paquete ESP. Los siguientes 32 bits almacenan el Número de Secuencia. Este número de secuencia se emplea para protegerse de ataques por repetición de mensajes. Los siguientes 32 bits especifican el Vector de Inicialización (IV - Initialization Vector) que se emplea para el proceso de cifrado. Los algoritmos de cifrado simétrico pueden ser vulnerables a ataques por análisis de frecuencias si no se emplean IVs. El IV asegura que dos cargas idénticas generan dos cargas cifradas diferentes.

IPsec emplea cifradores de bloque para el proceso de cifrado. Por ello, puede ser necesario rellenar la carga del paquete si la longitud de la carga no es un múltiplo de la longitud del paquete. En ese caso se añade la longitud del relleno (pad length). Tras la longitud del relleno se coloca el campo de 2 bytes Siguiente cabecera que especifica la siguiente cabecera. Por último, se añaden los 96 bit de HMAC para asegurar la

integridad del paquete. Esta HMAC sólo tiene en cuenta la carga del paquete: la cabecera IP no se incluye dentro de su proceso de cálculo.

El uso de NAT, por lo tanto, no rompe el protocolo ESP. Sin embargo, en la mayoría de los casos, NAT aún no es compatible en combinación con IPsec. NAT-Transversal ofrece una solución para este problema encapsulando los paquetes ESP dentro de paquetes UDP.

El protocolo IKE

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. Tras ello, crea las asociaciones de seguridad y rellena la SAD. El protocolo IKE suele implementarse a través de servidores de espacio de usuario, y no suele implementarse en el sistema operativo. El protocolo IKE emplea el puerto 500 UDP para su comunicación.

El protocolo IKE funciona en dos fases. La primera fase establece un ISAKMP SA (Internet Security Association Key Management Security Association - Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet). En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SAs de IPsec.

La autenticación de los participantes en la primera fase suele basarse en claves compartidas con anterioridad (PSK - Pre-shared keys), claves RSA y certificados X.509 (racoon puede realizar esta autenticación incluso mediante Kerberos).

La primera fase suele soportar dos modos distintos: modo principal y modo agresivo. Ambos modos autentican al participante en la comunicación y establecen un ISAKMP SA, pero el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo. Esto, sin embargo, tiene sus desventajas, ya que el modo agresivo no soporta la protección de identidades y, por lo tanto, es susceptible a un ataque man-in-the-middle (por escucha y repetición de mensajes en un nodo intermedio) si se emplea junto a claves compartidas con anterioridad (PSK). Pero sin embargo este es el único objetivo del modo agresivo, ya que los mecanismos internos del modo principal no permiten el uso de distintas claves compartidas con anterioridad con participantes desconocidos. El

modo agresivo no permite la protección de identidades y transmite la identidad del cliente en claro. Por lo tanto, los participantes de la comunicación se conocen antes de que la autenticación se lleve a cabo, y se pueden emplear distintas claves pre-compartidas con distintos comunicantes.

En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad basándose en la ISAKMP SA. La ISAKMP SA proporciona autenticación para protegerse de ataques man-in-the-middle. Esta segunda fase emplea el modo rápido.

Normalmente, dos participantes de la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias (al menos dos) IPsec SAs unidireccionales.

2.11 “HIPERLAN/2”

HIPERLAN es un estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54 Mbps en la frecuencia de banda de 5 GHz. HIPERLAN/2 es una solución estándar para un rango de comunicación corto que permite una alta transferencia de datos y calidad de servicio del tráfico entre estaciones base WLAN y terminales de usuarios. La seguridad esta provista por lo último en técnicas de encriptación y protocolos de autenticación.

Hiper Lan es similar a 802.11a (5 GHz) y es diferente de 802.11b/g (2,4 GHz). HIPERLAN/1, HIgh PErformance Radio LAN versión 1 es un estándar del ETSI (European Telecomunications Standards Institute).

El plan empezó en 1991. El objetivo de HIPERLAN era la alta velocidad de transmisión, más alta que la del 802.11. El estándar se aprobó en 1996.

El estándar cubre las capas física y MAC como el 802.11. Hay una nueva subcapa llamada Channel Access and Control sublayer (CAC). Esta subcapa maneja las peticiones de acceso a los canales. La aceptación de la petición depende del uso del canal y de la prioridad de la petición. La capa CAC proporciona independencia jerárquica con un mecanismo de Elimination-Yield Non-Preemptive Multiple Access. (EY-NPMA). EY-NPMA codifica las prioridades y demás funciones en un pulso de radio de longitud variable que precede a los datos.

EY-NPMA permite trabajar a la red con pocas colisiones aunque halla un gran número de usuarios. Las aplicaciones multimedia funcionan en HIPERLAN gracias al mecanismo de prioridades del EY-NPMA. La capa MAC define protocolos para enrutado, seguridad y ahorro de energía y proporciona una transferencia de datos natural a las capas superiores.

En la capa física se usan modulaciones FSK y GMSK .

Características de HIPERLAN:

- rango 50 m
- baja movilidad (1.4 m/s)
- soporta tráfico asíncrono y síncrono.
- sonido 32 kbit/s, latencia de 10 ns
- vídeo 2 Mbit/s, latencia de 100 ns
- datos a 10 Mbit/s

HIPERLAN no interfiere con hornos microondas y otros aparatos del hogar, que trabajan a 2.4GHz.

“HIPERLAN/2” efectos en la salud

Las especificaciones funcionales de HIPERLAN/2 se completaron en el mes de Febrero de 2000. La versión 2 fue diseñada como una conexión inalámbrica rápida para muchos tipos de redes. Por ejemplo: red backbone UMTS , redes ATM e IP. También

funciona como una red doméstica como HIPERLAN/1. HIPERLAN/2 usa la banda de 5 GHz y una velocidad de transmisión de hasta 54 Mbit/s.

Los servicios básicos son transmisión de datos, sonido, y vídeo. Se hace énfasis en la calidad de esos servicios. (QoS).

El estándar cubre las capas Física, Data Link Control y Convergencia. La capa de Convergencia se ocupa de la funcionalidad de la dependencia de servicios entre las capas DLC y Red (OSI 3). Las subcapas de Convergencia se pueden usar también en la capa física para conectar las redes IP, ATM o UMTS. Esta característica hace HIPERLAN/2 disponible para la conexión inalámbrica de varias redes.

En la capa física se emplean modulaciones BPSK, QPSK, 16QAM o 64QAM .

Modulación de amplitud en cuadratura

La modulación de amplitud en cuadratura, en inglés Quadrature Amplitude Modulation (QAM), es una modulación lineal que consiste en modular en doble banda lateral dos portadoras de la misma frecuencia desfasadas 90º. Cada portadora es modulada por una de las dos señales a transmitir. Finalmente las dos modulaciones se suman y la señal resultante es transmitida.

Este tipo de modulación tiene la ventaja de que ofrece la posibilidad de transmitir dos señales en la misma frecuencia, de forma que favorece el aprovechamiento del ancho de banda disponible. Tiene como inconveniente que es necesario realizar la demodulación con demoduladores síncronos.

Sistemas analógicos que utilizan la modulación QAM

La modulación de amplitud en cuadratura es utilizada en los sistemas PAL y NTSC de televisión analógica para transmitir las dos señales de crominancia.

Sistemas digitales que utilizan la modulación QAM

La modulación de amplitud en cuadratura es utilizada en sistemas digitales de telecomunicación, como los módems. Según el número de símbolos existentes combinando las distintas amplitudes posibles de las dos señales que se transmiten, la modulación es denominada 4-QAM, 16-QAM, 64-QAM, etc....

QPSK Quadrature Phase Shift Keying

QPSK son las siglas de Quadrature Phase Shift Keying. Es una forma de modulación en la que la señal se envía en cuatro fases, 45, 135, 225, y 315 grados, y el cambio de fase de un símbolo al siguiente codifica dos bits por símbolo. La modulación QPSK es equivalente a la 4-QAM.

Para su mayor comprensión, algunos prefieren decir Quaternary en lugar de Quadrature dado QPSK transmite 4 fases (360°/4).

HIPERLAN/2 ofrece unas medidas de seguridad aceptables. Los datos son codificados con los algoritmos DES o 3DES. El punto de acceso y el terminal inalámbrico se pueden autenticar mutuamente.

HIPERLAN: ¿tecnología obsoleta o futura?

Algunos creen que los estándares IEEE 802.11 ya han ocupado el nicho comercial para el que se diseñó HIPERLAN, aunque con menor rendimiento pero mayor penetración comercial, y que el efecto de la red instalada impedirá la adopción de HIPERLAN. También dicen que como el uso principal de las WLANs es proporcionar acceso a Internet, la falta de soporte para calidad de servicio (QoS) en la Internet comercial hará que el soporte de QoS en las redes de acceso sea irrelevante.

Otros creen que el rendimiento superior de HIPERLAN/2 puede ofrecer nuevos servicios que las variantes de 802.11 son incapaces de suministrar. El desarrollo de

802.11n, que definirá el siguiente nivel de rendimiento en WLANs, no está siendo seguido por ninguna actividad por parte de HIPERLAN.

2.12 WIMAX ("WORLDWIDE INTEROPERABILITY FOR MICROWAVE ACCESS")

WiMAX (del inglés Worldwide Interoperability for Microwave Access, Intercomunicación Mundial para Acceso por Microondas) es un estándar de transmisión inalámbrica de datos (802.16d) diseñado para ser utilizado en el área metropolitana o MAN proporcionando accesos concurrentes en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología portátil LMDS.

Integra la familia de estándares IEEE 802.16 y el estándar HyperMAN del organismo de estandarización europeo ETSI. El estándar inicial 802.16 se encontraba en la banda de frecuencias de 10-66 GHz y requería torres LOS. La nueva versión 802.16a, ratificada en marzo de 2003, utiliza una banda del espectro más estrecha y baja, de 2-11

GHz, facilitando su regulación. Además, como ventaja añadida, no requiere de torres LOS sino únicamente del despliegue de estaciones base (BS) formadas por antenas emisoras/receptoras con capacidad de dar servicio a unas 200 estaciones suscriptoras (SS) que pueden dar cobertura y servicio a edificios completos. Su instalación es muy sencilla y rápida y su precio competitivo en comparación con otras tecnologías de acceso inalámbrico como Wi-Fi.

Esta tecnología de acceso transforma las señales de voz y datos en ondas de radio dentro de la citada banda de frecuencias. Está basada en OFDM, y con 256 subportadoras puede cubrir un área de 48 kilómetros permitiendo la conexión sin línea vista, es decir, con obstáculos interpuestos, con capacidad para transmitir datos a una tasa de hasta 75 Mbps con un índice de modulación de 5.0 bps/Hz y dará soporte para miles de usuarios con una escalabilidad de canales de 1,5 MHz a 20 MHz. Este estándar soporta niveles de servicio (SLAs) y calidad de servicio (QoS).

WiMAX se sitúa en un rango intermedio de cobertura entre las demás tecnologías de acceso de corto alcance y ofrece velocidades de banda ancha para un área metropolitana.

El WiMAX en principio se podría deducir que esta tecnología supone una grave amenaza para el negocio de tecnologías inalámbricas de acceso de corto alcance en que se basan muchas empresas, pero hay entidades muy importantes detrás del proyecto. Las principales firmas de telefonía móvil también están desarrollando terminales capaces de conectarse a estas nuevas redes. Después de la fase de pruebas y estudios cuya duración prevista es de unos dos años, se espera comenzar a ofrecer servicios de conexión a Internet a 4 Mbps a partir de 2007, incorporando WiMAX a los ordenadores portátiles y PDA.

3 “HOGAR Y ENTRETENIMIENTO DIGITAL”

En este tema trataremos las: “Comunicaciones para la transferencia de servicios y contenidos multimedia para el ocio digital – Home Entertainment; Banda ancha, ADSL, movilidad, gíreles, WiFi imagen y sonido digital.

Los contenidos digitales no siempre son percibidos de la manera que pensamos, por ejemplo, el 80% de los menores de 30 años reconocen que hablan por teléfono mientras ven la Televisión. ¿Cómo podemos hacer los contenidos más interesantes? Y ¿Como servirnos de esos contenidos? El ancho de banda ofrece esta posibilidad con interactividad, etc.

En los últimos años se han introducido conceptos como domótica, home entertainment, hogar digital etc., dentro del hogar. Hay que hacía hincapié en separar las distintas áreas. El modelo de negocio del Home Entertainment debería convivir con el hogar digital, haciendo énfasis en la domótica y la seguridad, pero tratándolos de manera independiente. La penetración de los videojuegos en los hogares es una de las más altas del mundo. Cuanto más ancho de banda tengamos mejores contenidos vamos a poder producir. El lanzamiento de los programas de videojuegos que se puede jugar on-line cobra cada vez más protagonismo.

La interactividad de los contenidos es la base en los videojuegos.

En conjunto es muy interesante y todos los temas abordaban temas estratégicos y atractivos para el sector del Hogar Digital. Además se ha dado un paso importante al integrar el sector del Hogar Digital en un contexto tan importante como el Globalcom.

El Hogar Digital es una vivienda que a través de equipos y sistemas, y la integración tecnológica entre ellos, ofrece a sus habitantes funciones y servicios que facilitan la gestión y el mantenimiento del hogar, aumentan la seguridad; incrementan el confort; mejoran las telecomunicaciones; ahorran energía, costes y tiempo, y ofrecen nuevas formas de entretenimiento, ocio y otros servicios dentro de la misma y su entorno

Los productos y sistemas relacionados con el Hogar Digital pueden ser agrupados en las siguientes áreas:

- La Domótica es la automatización y control local y remota del hogar (apagar / encender, abrir / cerrar y regular) de aplicaciones y dispositivos domésticos, con instalaciones, sistemas y funciones para iluminación, climatización, persianas y toldos, puertas y ventanas, cerraduras, riego, electrodomésticos, control de suministro de agua, gas, y electricidad, etc.
- La Multimedia son los contenidos de información y entretenimiento, relacionados con la captura, tratamiento y distribución de imágenes y sonido dentro y fuera de la vivienda, con instalaciones, sistemas y funciones como radio, televisión, audio / vídeo “multi-room”, cine en casa, pantallas planas, videojuegos, porteros y video porteros.
- La Seguridad y Alarmas son sistemas y funciones para alarmas de intrusión, cámaras de vigilancia, alarmas personales, alarmas técnicas (incendio, humo, agua, gas, fallo de suministro eléctrico, fallo de línea telefónica etc.), etc.
- Las Telecomunicaciones es la distribución de ficheros textos, imágenes y sonidos, compartiendo recursos entre dispositivos, el acceso a Internet y a nuevos servicios, con instalaciones, sistemas y funciones como red de telefonía, telefonía sobre IP, red local de datos, pasarelas residenciales, routers, acceso a Internet Banda Ancha, etc.

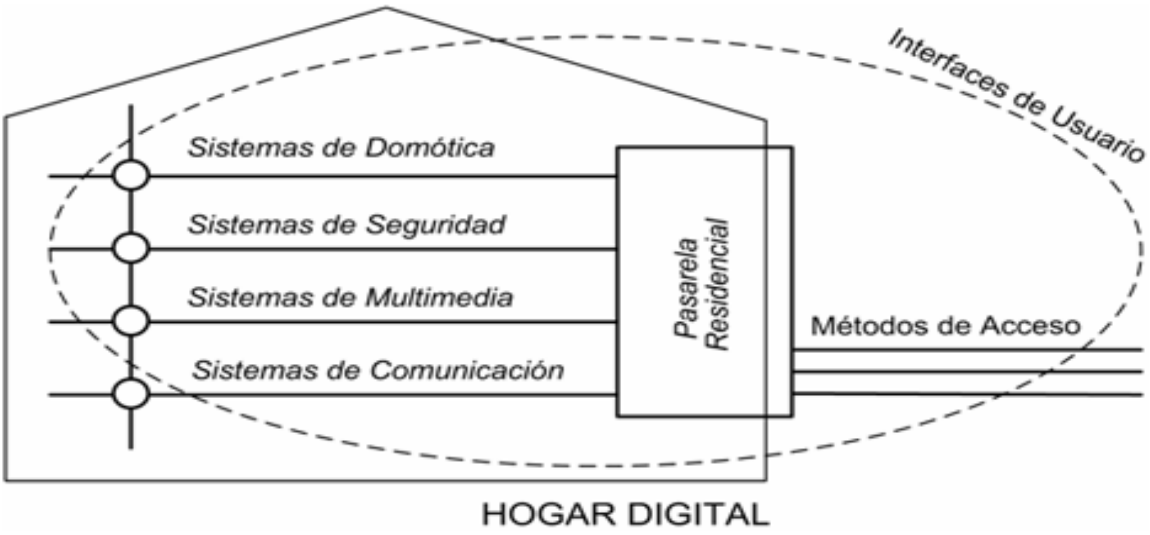


Figura 3. Esquema conceptual del Hogar Digital

Otros Conceptos Básicos

Algunos otros conceptos básicos que se utilizarán en este artículo son:

- Equipo / Dispositivo, es el material (mecánico, eléctrico, electrónico) que realiza una actividad física o lógica determinada.
- Función, es una acción que se pueden implementar con un determinado equipo o un sistema.
- Producto, incluye cualquier elemento que se comercializa y puede ser un dispositivo, equipo, mecanismo, aparato, maquina, etc.
- Sistema, que es un conjunto de redes, controladores, equipos o dispositivos que, una vez instalados y puestos en marcha de forma coordinada, es capaz de implementar un conjunto de funciones o servicios útiles para el usuario.
- Servicio, que demanda la entrada en juego de un tercer actor, esto es, una empresa que permita el acceso, mantenimiento o gestión de la función.

Por ejemplo, un sistema de riego automático está constituido por equipos como tubos, juntas, electro válvulas, un programador, etc. Toda la instalación del riego, en su conjunto, forma el sistema. La apertura/cierre de la electroválvula de agua, sin embargo, es una función. Si en paralelo una empresa de jardinería ofrece la monitorización de la humedad del césped y control remoto del correcto funcionamiento del programador, esto se define como un servicio.

3.1 PROLIFERACIÓN DE COMUNICACIONES INALÁMBRICAS

La invasión de los sistemas "wireless" y sus efectos nocivos sobre los seres vivos.

En el entorno urbano es difícil encontrar un espacio libre de emisiones radioeléctricas, y en el avión o en el hospital preocupa la interferencia de la telefonía móvil con los equipos médicos o de navegación. Todo el espacio está lleno de "ruido electrónico", un ruido de fondo electromagnético que incide permanentemente sobre el sistema nervioso, y que puede incluso percibirse de manera audible, bajo la forma de zumbidos de oídos.

La agresión ambiental más frecuente en el medio urbano es el ruido audible y los campos electromagnéticos de baja frecuencia (CEM 50 Hz), como los generados por

computadoras, electrodomésticos, iluminación, máquinas herramientas, transformadores y líneas de alta tensión.

En la última década, aparecen las microondas (MW 1-3 GHz), producidas principalmente por la telefonía móvil, y la proliferación de antenas de telefonía en los tejados han creado una gran alarma social, pues afectan a todas las viviendas en un radio de varios kilómetros, según la potencia.

Más discretamente, la nueva telefonía inalámbrica DECT-GAP crea un entorno irradiado con plena cobertura hasta 300 m, con emisión de microondas permanente (24/24 h), literalmente pone una estación base de telefonía en la cabecera de nuestra cama.

Preocupados por la amenaza de las antenas, valoramos poco la radiación de los millones de terminales móviles, cuya emisión puede alterar las ondas cerebrales, hasta 80 metros del emisor. Mientras, en el entorno laboral se imponen los microprocesadores ultrarrápidos (chips a 1-2 GHz), y recientemente surgen los sistemas wireless, o redes inalámbricas tipo Bluetooth, con un alcance de 100 m, todos estos sistemas emiten microondas similares a la telefonía móvil.

Desde hace pocos meses, Zamora (España) presume de ser la primera ciudad totalmente cableada mediante el sistema WiFi donde podremos estar permanentemente conectados, sin perder la cobertura como en el sistema GSM, pues los teléfonos WiFi no usan la red de telefonía móvil, se conectan vía Internet.

Principales emisores

- Telefonía WiFi (internet).
- Ropa High-Tech.
- Sistemas wireless (Bluetooth, etc.).
- Telefonía inalámbrica (DECT-GAP).
- Telefonía fija cable-radio (LMDS-MMDS).
- Telefonía móvil (GSM).
- Monitores ordenador (RX, CEM, etc.).

- Materiales dieléctricos y electrostáticos (plásticos, melaminas, etc.).
- Electrodomésticos (Iluminación, alarmas, microondas, etc.).
- Transformadores y redes eléctricas (alta, media y baja tensión).

Electroestrés

La medición de la carga eléctrica en el cuerpo humano, revela que bajo la influencia de campos eléctricos y/o magnéticos, se modifican las constantes bioeléctricas del organismo, es lo que llamamos estrés electromagnético, o "electroestrés."

El chequeo de electroestrés muestra que un individuo sano, en estado de reposo (relax), presenta una descarga eléctrica corporal del orden de 100 mV, y durante la actividad física moderada (trabajo, deporte), esa tensión eléctrica sube hasta 500 mV, lo que se considera fisiológicamente normal.

En presencia de electromagnetismo, como es el caso de un operario de ordenador, esta tensión puede subir hasta 10.000 e incluso 24.000 mV, lo que afecta a diversos sistemas neurológicos.

Este incremento del estrés bioeléctrico nos aleja del equilibrio homeostático que permite la salud óptima y se manifiesta de manera más acusada en los sujetos "electrosensibles", potencialmente alérgicos a la electricidad.

Según estudios del norte de Europa, las personas electrosensibles representan entre el 20 y el 25% de la población, y recientemente la electrosensibilidad ha sido reconocida en Suecia como enfermedad profesional (2002).

Efectos sanitarios

Se producen efectos neurológicos a corto y medio plazo:

- Insomnio, somnolencia matinal (melatonina).
- Estrés, angustia, ansiedad (pannic attack).
- Pérdida de memoria, hemicrania (jaqueca).
- Ruidos y zumbidos de oídos, mareos y vértigo.
- Fatiga crónica, fibromialgia.
- Atonía, desinterés, dificultad en la toma de decisiones.
- Rutina, falta de iniciativa, pérdida de creatividad.
- Depresión, tristeza, pesimismo, trastorno afectivo estacional (TAE).

A largo plazo pueden aparecer otros graves efectos biológicos:

- Patologías cardiovasculares (arritmia, hipertensión, infarto).
- Patologías reumáticas (osteoporosis).
- Patologías respiratorias (asma).

También se ha establecido una relación causa-efecto con diversas patologías degenerativas como Alzheimer, Parkinson, esclerosis, leucemia y cáncer (OMS).

Espacio radioeléctrico

El real decreto de Telecomunicaciones considera el espacio radioeléctrico infinito e ilimitado, por lo que autoriza la emisión de radiaciones que invaden el domicilio privado, del cuerpo humano, y de su cerebro.

Desde el aspecto jurídico, es preciso considerar que la invasión de radiofrecuencias, dentro de las viviendas, significa una invasión de varios Derechos Fundamentales de los Ciudadanos.

En uso del principio de precaución, es importante reglamentar medidas legales contra esta invasión del espacio radioeléctrico, con la creación de zonas libres de radiaciones en todas las áreas sensibles como guarderías, colegios, asilos y hospitales, y en particular en todos los dormitorios.

Esta exposición radioeléctrica es involuntaria, indeseada e inadvertida, permanente y además indiscriminada, pues en grados diferentes afecta en la práctica al 100% de la población.

Medidas preventivas

- Etiquetado riesgo CEM (móviles, electrodomésticos, etc.).
- Reducción de radiaciones (mejor tecnoclogía).
- Distancias de seguridad (antenas, transformadores, etc.).
- Blindaje electromagnético (microwave filter, etc.).
- Medicina ortomolecular y bioenergética.
- Ergonomía invisible (white pollution).
- Evaluación periódica del electroestrés (chequeo médico).
- Control de emisiones (prevención y control).

Principio de precaución

Diversas recomendaciones internacionales sugieren niveles de radiación cientos y miles de veces más bajos que los máximos legales, por lo que es precisa la aplicación de medidas preventivas que reduzcan el riesgo sanitario, pues a corto plazo se prevé un gran crecimiento de las emisiones radioeléctricas, con los nuevos teléfonos WAP (pago por móvil, juegos on-line, etc.), la implantación de la red UMTS, y la generalización de los sistemas wireless.

Quizá el aspecto más nocivo de esta proliferación inalámbrica, es que este “ruido electrónico” permanente, de manera similar al ruido audible, afecta al sistema

neurológico e inmunitario, además altera el ciclo de la melatonina, afecta al sueño y el descanso nocturno (elimina la fase REM), y dificulta la regeneración celular.

Beneficios a obtener

- Mejora del estado de ánimo, del relax y del sueño.
- Mejora del clima social, familiar y laboral.
- Restitución del sistema neurológico, hormonal e inmunitario.
- Reducción de errores y accidentes.
- Reducción del gasto sanitario.
- Incremento del rendimiento laboral.

Esta proliferación inalámbrica afecta a todos los seres vivos, y se ha observado que hormigas, murciélagos, ratas, e incluso el ganado son afectados por las radiaciones electromagnéticas, y recientemente un estudio británico informa de la extinción masiva de más de diez millones de pájaros, en el entorno de las antenas de telefonía.

El costo sanitario para la población es incalculable, como ejemplo las compañías de seguros, excluyen de sus pólizas la cobertura de riesgos electromagnéticos.

El ejecutivo de Intel Corp. Craig Barrett ha afirmado que WiMAX (estándar de transmisión inalámbrica que llega a cubrir un área de hasta 48 kilómetros) competirá directamente con el cable y con el ADSL. Además, según el CEO de Intel, estas conexiones ni siquiera llegan a funcionar correctamente o no se aprovecha toda su capacidad lo que influye en los contenidos multimedia accesibles en Internet. WiMAX en cambio es capaz de moverse entre 50 y 100 Mbps lo que le permite transmitir video de alta calidad sin pérdida.

Barret hizo hincapié no sólo en la velocidad sino también en los lugares donde cable y ADSL no llegan y tan solo hay conexiones RTB y vía satélite: la zona rural será uno de los campos más fuertes donde WiMAX, que integra la familia de estándares IEEE 802.16, se expandirá.

El interés de Intel se debe a la presentación de un nuevo chip, Intel PRO/Wireless 5116 (diagrama de su funcionamiento), primer producto WiMAX del

mercado y un proyecto que aglutina junto a esta compañía a 240 más (ver WiMAX Forum) entre las que cabe destacar AT&T, British Telecom, Iberbanda o TelMex.

Se espera a principios del próximo año las primeras pruebas sobre WiMAX (incluso con relanzamiento de Centrinos que soporten el estándar) que precederán a los ensayos comerciales en móviles para 2007. También en 2006 llegarán los primeros PDAs y portátiles con esta tecnología.

Distintas infraestructuras para dar servicios VoIP Wi-Fi

1) Basada en la cobertura (clásica, sencilla). Se implanta en empresas.

Inconvenientes:

- problemas en el cableado de la red, no se pueden instalar puntos de red en entornos abiertos;
- la frecuencia y los servicios pueden verse saturados fácilmente; problemas de seguridad deducidos de no emplear los mecanismos adecuados.

2) Basada en la conectividad (punto-multipunto, estación base con equipos conectados). Se implanta más para residencial

Inconvenientes:

- no da servicios móviles, sólo es válida en el ámbito residencial; mismos problemas de colapsamiento de red y de seguridad que el modelo de cobertura; no se suele implementar QoS.

3) Tipo Mesh (está llegando ahora, es la opción más completa aunque no la más económica). En la Administración Pública se están diseñando los primeros proyectos serios en Mesh. En municipios como Chaska, Minnesota, se da con ello un servicio de videovigilancia a los ciudadanos.

Inconvenientes:

- coste de los equipos aún muy alto, hay pocos fabricantes y pocos productos homologados en Europa.
- dependencia con backhaul, importancia de funcionalidades de redundancia.
- equipos diseñados sobre todo para interiores, en exteriores deberían ir con cajas estancas.

4) Híbrida punto-multipunto con cobertura WLAN (la más favorable y la que más se está implementando, pero tampoco mucho...).

Ventajas frente a las anteriores:

- servicios tanto de movilidad como fijos, si fuera necesario;
- banda 5GHz que no se satura;
- calidad de servicio QoS.

Inconvenientes:

- todavía hay pocos equipos con ella.

Equipos VoIP Wi-Fi disponibles

- móviles Wi-Fi con gateway de interconexión con centralitas (integración perfecta con la plataforma, pero alto precio de los teléfonos, aunque la bajada de precios está siendo espectacular)
- móviles Wi-Fi con servidor VoIP (tfnos. de cualquier fabricante, se compra un servidor --conectado o no a la centralita-- y se conectan entre sí, pero aún hay muchas incompatibilidades, aunque a medio plazo será la mejor opción)
- fijo con gateway VoIP Wi-Fi (el teléfono no es Wi-Fi, sino la infraestructura, se puede usar con todo tipo tfno. pero plantea problemas cuando hay muchos usuarios).

Problemas que determinan la viabilidad/rentabilidad del modelo de negocio

- tipo de la infraestructura
- coste del backbone de Internet (factor clave)
- tipo de los terminales de voz usados
- disponibilidad y elección del operador de telefonía según el proyecto

Siempre hay que tener en cuenta la limitación de la legislación, ya que mientras en EE.UU. se puede emitir a potencias de más de 1V, en España sólo se permiten 100 milivatios.

El movimiento FON, liderado por Martin Varsavsky es un ambicioso proyecto que persigue crear un país WIFI con el cual podrías acceder a Internet desde cualquier parte, hablar por el móvil gratis, mandar y recibir e-mails desde todos los lugares, bloggear desde la playa o sentados tranquilamente en un banco de cualquier parque. Desde mi punto de vista lo más motivador es la vertiente open source (código abierto) del proyecto “comparte tu conexión” a Internet para compartir la de otros muchos. Un altruismo contra el que los operadores con intereses en el mercado móvil les va a costar luchar, ya que la mayoría de contratos de acceso están blindados en cuanto a "revender" tu acceso a Internet, pero no dicen nada sobre compartir sin ánimo de lucro el ancho de banda que no utilizas.

CONCLUSION

Los protocolos (Wi-Fi) tienen ya un mercado y algunos consideran un nicho para cada uno, sin embargo conforme aumentan las demandas de los consumidores y las necesidades de comunicación a distancia las líneas entre protocolos y sus “nichos” se vuelven más delgados, confundiéndose muchas veces entre sí.

Existe información muy diversa con respecto a los protocolos, así mismo información muy extensa; es por esto que se requiere conocer a la mayor profundidad posible cada protocolo para poder hablar de interoperabilidad o interferencia e inclusive para poder justificar la existencia de las mismas así como de los protocolos y no pensar en que son dos maneras de realizar la misma tarea.

Bluetooth como protocolo más nuevo se encuentra en constante cambio, y muchos de esos cambios obedecen a dibujar una línea más clara que permita coexistir a los protocolos, sin embargo estos cambios todavía están por realizarse y saber a que obedecerán es un tema muy complejo, pero podemos tratar de atender la situación actual y las propuestas que existen ahora para resolver esta diferencia o igualdad de funciones y poder esclarecer efectivamente si existe o no ese nicho para cada protocolo.

Uno de los temas regulatorios pendientes de mayor relevancia, en el sector de las telecomunicaciones. Se trata del uso y aprovechamiento de las tecnologías Wi-Fi y Wi-Max para el acceso a Internet inalámbrico de banda ancha.

El Wi-Fi se da en ambientes cerrados y cuyos espacios no son muy amplios. Se trata de los llamados hot-spots que, en lugares como Starbucks o Sanborns, por ejemplo, puede uno abrir su laptop y navegar por Internet.

En cambio, el Wi-Max tiene un alcance mucho mayor. Pueden ser del orden de los 10 hasta 50 kilómetros, con anchos de banda flexibles y que permiten la prestación de servicios basados en el tráfico IP (protocolo de Internet).

La tendencia mundial para aprovechar estas nuevas tecnologías de la información ha sido a partir de atribuir, para tal propósito, ciertas bandas de frecuencias que no requieren licencia para su aprovechamiento.

Ello no implica un uso arbitrario e indiscriminado de tales frecuencias. Significa que su uso puede ser libre pero regulado en sus aspectos técnicos de operación, potencia y no interferencia.

Conforme la tecnología avanza y estas tecnologías emergen como soluciones normales del día a día, también avanzan las preocupaciones sobre el potencial de interferencia por la misma frecuencia. La necesidad de enviar voz y datos por los mismos canales con la menor pérdida posible y más recientemente el incremento de la demanda de video en los dispositivos móviles al incrementar estos su potencia y al estar, de manera cada vez más común, equipados con dispositivos de video de diversas resoluciones, permitiendo expandir su rango de uso desde el entretenimiento, como por ejemplo mobiTV, hasta las aplicaciones de oficina y video conferencia, nos llevan a las preocupaciones por interferencia entre los diversos protocolos. Ya se están estudiando y proponiendo soluciones por parte de los creadores y responsables de los diferentes protocolos, tanto Wi-Fi como Bluetooth, pero todavía se requiere comparar y estudiar ambos protocolos para poder proponer mejores soluciones, no se trata de ver cual se hace a un lado, sino de tomar lo mejor de ambos y ponerlos a trabajar en conjunto.

Esto permitirá un acceso creciente de usuarios de Internet; un uso más eficiente del espectro; la producción y manufactura de equipos para este propósito; una más vigorosa competencia en el sector y, desde luego, una mayor diversidad y calidad de servicios a mejor precio para el consumidor.

GLOSARIO

HTML: Son las instrucciones del lenguaje que sirven para darle formato al texto para colocarlo en paginas web.(lenguaje de marcado de hipertexto)

URL: Numero de identificación de una pc en red (universal resource locator)

WEB BROWSERS: Navegador de internet. (Internet Explorer, netscape)

FTP: Protocolo para la transferencia de archivos. (fail transfer protocol)

TCP: Protocolo de control de transporte. (transport control protocol).

RIP: Protocolo de información de enrutado (Routing information protocolo).

OSPF: El camino más corto primero (Open shortest path first).

BGP: Protocolo de la pasarela externa (Border gateway protocol).

HOST: Un host, literalmente anfitrión, es un ordenador directamente conectado a una red y que efectúa las funciones de un servidor, y alberga servicios, como correo electrónico, grupos de discusión Usenet, FTP, o World Wide Web) accesibles por otros ordenadores de la red.

RDSI : El servicio RDSI (de Red Digital de Servicios Integrados; las siglas en inglés son ISDN) es una tecnología más antigua pero todavía disponible, ofrecida por las compañías telefónicas en algunas zonas de los Estados Unidos. RDSI requiere lo que se denomina un adaptador RDSI en vez de un módem, y una línea telefónica con una conexión especial que permite enviar y recibir señales digitales. Una línea RDSI tiene una velocidad de transferencia de datos de entre 57 Kbps y 128 Kbps. Debe tratar con su compañía telefónica para la instalación de este equipo. Para obtener más información.

NSFNET: National Science Foundation's NETwork. La NSFNET comenzó con una serie de redes dedicadas a la comunicación de la investigación y de la educación. Fue creada por el gobierno de los Estados Unidos, y fue reemplazada por ARPANET como backbone de Internet. Desde entonces ha sido reemplazada por las redes comerciales.

HDB3: High Density Bipolar-3 Zeros. Se basa en la codificación AMI en el cual se reemplazan las cadenas de cuatro ceros por cadenas que contienen uno o dos pulsos.

CSMA/CD: Acceso múltiple con detección de portadora y de coaliciones. Protocolo de control de acceso al medio de contienda empleado.

BACKBONE: Un backbone es enlace de gran caudal o una serie de nudos de conexión que forman un eje de conexión principal. Es la columna vertebral de una red. Por ejemplo, NSFNET fue el backbone, la columna o el eje principal de Internet durante muchos años.

CONCENTRADOR: Dispositivo de red que se utiliza para conectar otros dispositivos al mismo segmento de red. La señal que recibe la repite hacia los demás puertos conectados.

ENRUTADOR: Dispositivo de interconexión de redes que realiza decisiones sobre la ruta que siguen los datos hacia su destino. Esta decisión se hace en términos de nivel de red.

PASARELA: Dispositivo que permite la interconexión entre dos o mas redes. Una pasarela ofrece interconexión a nivel de aplicación, se utiliza cuando las redes a conectar son muy diferentes.

PUENTE: Dispositivo de interconexión entre dos o mas redes de área local. Funciona al nivel de enlace de datos del modelo OSI.

REPETIDORES: Dispositivo que se utiliza en una red o una línea para aumentar la distancia a la que puede transmitir la información mediante la regeneración y amplificacion de esta.

TOPOLOGÍA: Estructura física y lógica que se utiliza para organizar la conexión de dispositivos en una red.

REFERENCIAS ELECTRONICAS Y BIBLIOGRAFICAS

www.avaya.com

www.motorola.com

www.itu.int

www.ansi.com

www.etsi.com

www.wi-fi.org

www.soe.com

www.wikipedia.org

www.cdnet.com

www.ncsoft.com

www.nationalinstitutesofhelath.com

www.bbs.uk

www.datacottage.com

www.geocities.com

www.htmlweb.net

www.fon.es

www.casadomo.com

www.intel.com

Redes Locales y TCP/IP

Jose Luis Raya

Alfaomega grupo editor S.A de C.V

Tecnología de interconectividad de redes

Merilee Ford, H. Kem Lew

Pretince hispanoamericana S.A

Advanced Electronic Communication Systems
Tomasi, Wayne
Prentice Hall