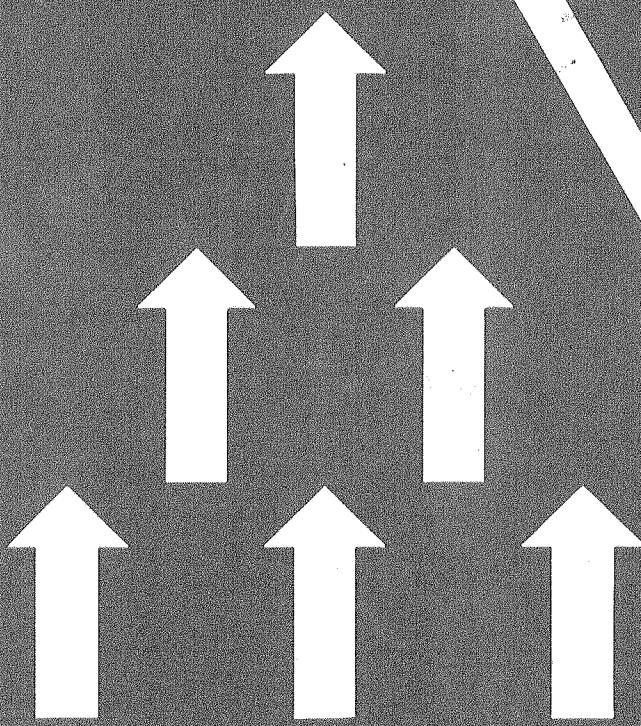


Fundamentos de TELÉMÁTICA



Franz Ramiro Gallardo Portanda

INCLUYE
ICD - ROM

LA PAZ - BOLIVIA

FUNDAMENTOS DE TELEMATICA

Lic. Ramiro Gallardo Portanda

Derechos de autor

CAMARA BOLIVIANA DEL LIBRO

Titulo Registrado bajo el I.S.B.N. 978-99954-0-748-3

Diciembre de 2009



IMPRESO EN:



UMSA

*Tel 2443193 – 2443214
La Paz – Bolivia*

Fotocopiar es delito.

*No se permite la reproducción total o parcial del presente libro,
en cualquier forma o por cualquier medio, sea este electrónico,
mecánico por fotocopia u otros medios. La violación a este
derecho se hará pasible a los infractores de persecución
criminal por incurrir en los delitos penados por Ley.*

INDICE

	Pág.
Prefacio	1
CAPITULO 1 INTRODUCCION	
Objetivos de aprendizaje	1
1.1 Redes	1
1.2 Conexión de redes	4
1.3 Topología de redes	5
1.4 Tipos de redes.....	7
1.5 Protocolos y estándares de red	9
1.6 Conceptos y términos clave	11
1.7 Preguntas de Repaso	12
1.8 Taller	14
CAPITULO 2 ESTRUCTURA DE UNA RED	
Objetivos de aprendizaje	15
2.1 Hosts y subredes	15
2.2 Tipos de transmisión de datos	16
2.3 Modelo Cliente Servidor.....	18
2.4 Modelo Peer to Peer.....	20
2.5 La estructura de la red de la UMSA	21
2.6 Conceptos y términos clave	23
2.7 Preguntas de Repaso	24
2.8 Taller	26
CAPITULO 3 MODELOS DE REFERENCIA	
Objetivos de aprendizaje	27
3.1 Filosofía de los sistemas abiertos	27
3.2 Arquitectura de una red dividida en capas	28
3.3 Encapsulamiento de datos	29
3.4 Modelo OSI	30
3.5 Modelo TCP/IP	32
3.6 Modelo Jerárquico de CISCO	34
3.7 Conceptos y términos clave	35
3.8 Preguntas de Repaso	36
3.9 Taller	39

INDICE

	Pág.
CAPITULO 4 APPLICACIONES DE RED	
Objetivos de aprendizaje	40
4.1 Servicios de la capa de Aplicación	40
4.2 Aplicación Web	41
4.3 Aplicación Correo Electrónico	47
4.4 Aplicación DNS	51
4.5 Otras aplicaciones de la red Internet	54
4.6 Conceptos y términos clave	58
4.7 Preguntas de Repaso	59
4.8 Taller	62
CAPITULO 5 LA CAPA DE TRANSPORTE	
Objetivos de aprendizaje	63
5.1 El Servicio de Transporte	63
5.2 Control de Flujo	65
5.3 Multiplexación/Demultiplexación	66
5.4 El protocolo TCP	67
5.5 El protocolo UDP	70
5.6 Conceptos y términos clave	72
5.7 Preguntas de Repaso	73
5.8 Taller	76
CAPITULO 6 LA CAPA DE RED	
Objetivos de aprendizaje	77
6.1 Servicios de la capa de Red	77
6.2 El protocolo IP	78
6.3 Direccionamiento con subredes	83
6.4 Algoritmos de Enrutamiento	85
6.5 Protocolos de Enrutamiento	92
6.6 Conceptos y términos clave	96
6.7 Preguntas de Repaso	97
6.8 Taller	100

INDICE

CAPITULO 7 LA CAPA DE ENLACE	Pág
Objetivos de aprendizaje	101
7.1 Servicios de la Capa de Enlace	101
7.2 Técnicas de Detección de errores	102
7.3 Creación de tramas	106
7.4 Protocolos de Acceso Múltiple	108
7.5 Conceptos y términos clave	117
7.6 Preguntas de Repaso	118
7.7 Taller	121
CAPITULO 8 LA CAPA FISICA	
Objetivos de aprendizaje	122
8.1 Señales Analógicas y Digitales	122
8.2 Transmisión digital	125
8.3 Características del canal	126
8.4 Problemas en la transmisión de datos	130
8.5 Medios de transmisión de datos	132
8.6 Medios No guiados o inalámbricos	136
8.7 Conceptos y términos clave	138
8.8 Preguntas de Repaso	139
8.9 Taller	142
CAPITULO 9 SEGURIDAD DE REDES	
Objetivos de aprendizaje	143
9.1 Principios de la seguridad informática	143
9.2 Ataques a redes informáticas	144
9.3 Espectro de seguridad	145
9.4 Herramientas de seguridad	146
9.5 Vulnerabilidad de una red	150
9.6 Vulnerabilidad del modelo TCP/IP	153
9.7 Conceptos y términos clave	155
9.8 Preguntas de Repaso	156
9.9 Taller	158

INDICE

	Pág.
CAPITULO 10 REDES WLAN	
Objetivos de aprendizaje	159
10.1 Introducción a las redes WLAN	159
10.2 Estandarización de tecnologías WLAN	160
10.3 Arquitectura WLAN	162
10.4 Protocolos WLAN	163
10.5 Seguridad en WLAN	165
10.6 El futuro de las redes inalámbricas	166
10.7 Conceptos y términos clave	168
10.8 Preguntas de Repaso	169
10.9 Taller	171
CAPITULO 11 TECNOLOGIA VoIP	
Objetivos de aprendizaje	172
11.1 La telefonía tradicional	172
11.2 Fundamentos de VoIP	173
11.3 Dispositivos de hardware y software	174
11.4 Telefonía IP	175
11.5 Estándares de VoIP	176
11.6 Características de equipos y software de comunicación para VoIP.....	180
11.7 Conceptos y términos clave	183
11.8 Preguntas de Repaso	184
11.9 Taller	186
Anexo Redes LAN	
A1.1 Rede Ethernet	
A1.2 Red Token Ring	
A1.3 Red FDDI	
Bibliografia	

PREFACIO

Hay una demanda no satisfecha de profesionales expertos en redes porque actualmente y dentro de por lo menos una década más el desarrollo de redes será un recurso valioso para la economía de las instituciones y de los países.

Un estudio realizado en la región asiática por la International Data Corporation (IDC), reveló que para el 2009, habrá un déficit de más de doscientos mil expertos en redes. En Europa la demanda en el 2008 crecerá a más de 500,000. En América del Norte, la diferencia entre la oferta y la demanda aumenta a una tasa del 9%. Latinoamérica también afronta un déficit de expertos en redes.

En nuestro país, todas las universidades que tienen las carreras de Informática o de Ingeniería de Sistemas contemplan en su plan curricular la enseñanza de redes. La UMSA no es la excepción, porque su carrera de Informática ha incluido esta materia en su plan de estudios y está previsto en la nueva malla curricular del plan académico propuesto. Sin embargo, no se tiene un texto oficial de producción nacional con esta temática.

Este libro de texto de enseñanza tiene el propósito de proporcionar a docentes y estudiantes de Telemática de una referencia bibliográfica con elementos teórico-prácticos para su aprendizaje y demos con uso de herramientas de E-learning.

Visión general de los contenidos

Todos los capítulos del libro se inician con una lista de verificación de objetivos de aprendizaje, su contenido se ilustra con figuras y tablas, finalizando con tres apartados comunes que son: Conceptos y términos clave de cada capítulo, preguntas de repaso del capítulo que fijan el aprendizaje y el taller que es una actividad de dinámica de grupos.

En el capítulo uno, se muestra una introducción general a las redes con varios de los conceptos necesarios para la descripción de una red como las topologías, los protocolos y los estándares de red. En el capítulo dos explicamos las características de la red de la UMSA, los modelos que utilizan las aplicaciones que corren sobre las redes y los tipos de transmisión de datos.

Los modelos de referencia son el objeto de aprendizaje del capítulo tres. Para justificar su inclusión en el libro empezamos por hacer referencia a los sistemas abiertos que son el hecho desencadenante para el establecimiento del modelo de referencia OSI. La red Internet se ha desarrollado gracias al éxito del modelo TCP/IP que explicamos en este capítulo. Finalmente concluimos con la descripción del modelo que utiliza Cisco Systems ® como política para la venta de sus equipos de comunicación.

A partir del capítulo cuatro hasta el ocho desarrollamos el estudio de las redes tomando en cuenta las capas de una red según el modelo de referencia TCP/IP que mostramos en el capítulo tres. Para esto seguimos el método "top down" empezando por la capa superior porque resulta intuitivo mostrar primeramente el uso final que se le dá a una red, conocido como las aplicaciones o servicios de red. El común de las personas en nuestro medio que recurre a la tecnología para sus comunicaciones ha utilizado el correo electrónico o navegado por Internet. Este conocimiento aquí es fortalecido con la descripción de los protocolos de comunicación a nivel de las aplicaciones de red que se realiza en el capítulo cuatro hasta concluir con la capa inferior o capa Física en el capítulo ocho.

En el capítulo nueve desarrollamos un tema ineludible en el estudio de las redes cual es su seguridad. Nadie puede asegurar que su red no es vulnerable a los ataques de intrusos externos o internos a la red. Describimos los principios de seguridad y mostramos cuan vulnerables resultan las redes de no seguirse alguna estrategia de defensa. Por supuesto aquí también nos interesa la seguridad del modelo TCP/IP.

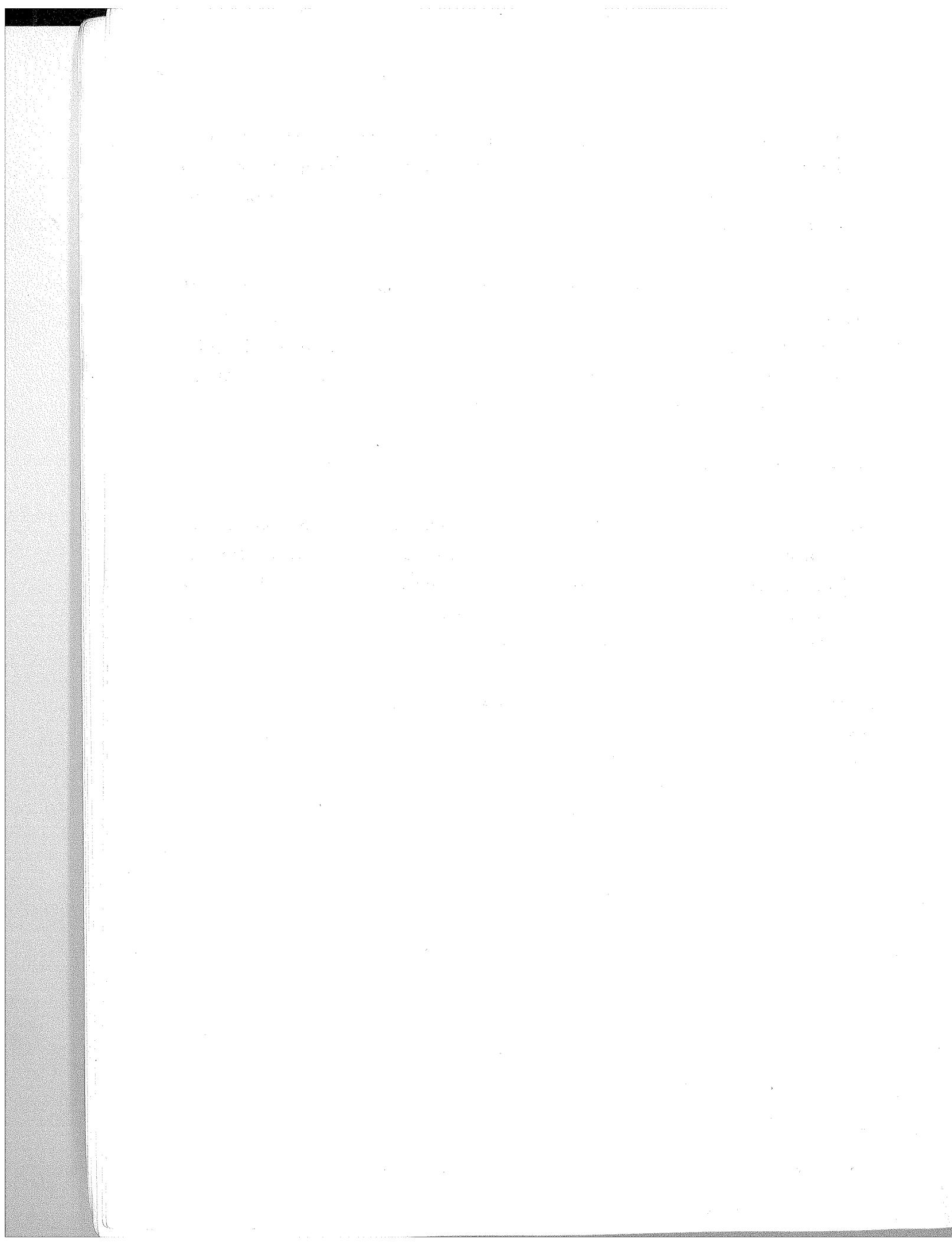
Un tipo de red que poco a poco va ganando aceptación entre los usuarios de las redes domésticas es la red inalámbrica por su facilidad y a la larga, el menor costo en su instalación en comparación con las redes fijas. En el capítulo diez, mostramos las características de este tipo de redes.

Finalmente en el capítulo once mostramos una de las aplicaciones de las redes que está revolucionando la telefonía con el uso del Internet, que es la tecnología voz sobre IP o VoIP. Actualmente ya hay soluciones incluso gratuitas para este tipo de servicios a los usuarios de las redes como las instituciones públicas llámense universidad interesadas en actualizar su gestión de comunicación al interior de sus predios.

CD interactivo de apoyo

Para la construcción de los demos de aprendizaje de los tópicos más importantes tratados en los capítulos del libro, hemos recurrido a las herramientas de autor eXe ® y Captivate ®. Estos recursos digitales los hemos encapsulado para obtener un producto bajo la norma SCORM que lo gestionamos a través de la herramienta Reload ® y lo presentamos junto al libro grabado en un CD interactivo de apoyo para el curso.

Luego de la lectura de los capítulos del libro, el lector encontrará en el CD unos test de autoevaluación de las preguntas impares que se formulan en los repasos de cada capítulo, los que estimularán su aprendizaje.



CAPITULO 1 INTRODUCCION

Objetivos de Aprendizaje: *Al concluir el capítulo, usted será capaz de:*

- *Comprender la importancia de una red de computadoras,*
- *Analizar las diferentes formas de organización interna,*
- *Describir los componentes más importantes de las redes de alcance local, las tecnologías que la implementan y*
- *Realizar una introducción a la red Internet .*

1.1 REDES

La Telemática es un término que surge como conjunción de Telecomunicaciones e Informática, para referirse a *la aplicación de las técnicas de la Telecomunicación y de la Informática a la transmisión a larga distancia de información computarizada.*¹

Gracias a las Telecomunicaciones, una computadora portátil común con mínimos recursos, se constituye en una terminal de la red Internet al igual que millones de computadoras, sin importar los límites geográficos, desde donde compartimos con otros usuarios. De la misma forma, una red de computadoras, no tendría sentido sin que alguna aplicación informática esté corriendo sobre esta red.

En general el término redes se aplica a todo conjunto de objetos interconectados con algún propósito como por ejemplo las redes de comunicaciones, de servicios públicos, redes sociales, de transporte, etc. Aquí en lo sucesivo, nos referiremos a la red como *el conjunto de computadoras y otros nodos o equipos de comunicación interconectados con el propósito de: acceder a información y al conocimiento, compartir recursos, ahorro económico, reducción de tiempo y esfuerzo o trabajo en equipo.*

Hoy en día, la posibilidad de acceder a la información y al conocimiento, es una necesidad de los países y de las personas, llega a ser un indicador de desarrollo y de valoración del recurso humano respectivamente. Las redes son el medio y la infraestructura necesaria para este propósito.

Los recursos computacionales como disco duro, escaner, impresora y otros se pueden compartir entre los usuarios de la red, obteniéndose no solo un ahorro económico sino optimizando su uso, reduciendo el tiempo de ocio de estos equipos.

¹

Minguet Jesús. Informática Fundamental. 2da Edición. Editorial Universitaria Ramón Areces 2008

La red de computadoras apoya al trabajo del grupo de personas de una institución o de los que comparten algún proyecto, independientemente de donde se encuentre el área de trabajo, actualizando en linea la información que se comparte.

En general, el ámbito donde se encuentra una red, es un sistema social como lo es: una empresa privada o pública, una institución educativa o el hogar. Las aplicaciones o usos que corren sobre éstas son diversas, desde las económico financieras, políticas, educativas, sociales o domésticas.

La red Internet, que inspira a desarrolladores de aplicaciones en redes, es el mayor ejemplo del funcionamiento, de estructura o de protocolos de comunicación que tiene una red. Aquí, se la tomará como referencia para describirlas.

El surgimiento de las redes, estuvo precedido del trabajo individual de enormes y costosas computadoras que operaban independientemente, duplicando recursos, con bajo nivel de eficiencia y productividad.

Un importante hito en la historia de las redes es ARPANET² (*Advanced Research Projects Agency Network*) (1969) creada por encargo del Departamento de Defensa de los Estados Unidos como medio de comunicación para sus diferentes organismos.

La tecnología inicial de las redes de principios de los años 80, tanto de hardware como de software era incompatible entre las distintas empresas, con un crecimiento desordenado, por la falta de estándares. Este problema es resuelto parcialmente con las primeras redes de alcance local, las que son interconectadas para satisfacer los requerimientos de los usuarios, hasta formar redes de gran alcance como la Internet.

Los usuarios de las redes conectados a Internet tienen a su disposición aplicaciones de acceso libre o con restricción como correo electrónico, páginas web, juegos en línea, chat, transferencia de archivos y otras, utilizan protocolos de comunicación que controlan el flujo de datos, comprensibles a los *hosts* o equipos terminales de la red como PC's, servidores, celulares o computadoras de bolsillo. La mayoría de estos protocolos pertenecen a la familia TCP/IP en la que está basada Internet.

Según Forouzan, 2007, los protocolos de red, son un conjunto de estándares o reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red. Una entidad es cualquier cosa capaz de enviar o recibir información.

² A History of the ARPANET: The First Decade (Bolt, Beranek and Newman, 1981)

Para que exista comunicación, las entidades deben estar de acuerdo con un protocolo. Un protocolo define tres cosas: que se comunica, como se comunica y cuando se comunica.

Los elementos de un protocolo son:

- Su sintaxis. La estructura del formato de los datos. El orden en el cual se presentan.
- Su semántica. El significado de cada sección de bits. Como se interpreta un determinado patrón y que acción se toma basada en dicha representación.
- Su temporización. Cuando se debería enviar los datos y con que rapidez deberán ser enviados.

Los estándares son esenciales para crear y mantener un mercado abierto y competitivo entre los fabricantes de los equipos y para garantizar la interoperabilidad de los datos, la tecnología y los procesos de telecomunicaciones.

Los protocolos TCP/IP tienen esta denominación por dos de los protocolos más importantes para el funcionamiento de la red pública Internet. El TCP encargado del transporte de paquetes de datos en forma segura y el IP para identificar al host conectado a la red.

Además de estos dos protocolos, la familia TCP/IP comprende a otros que explicaremos más adelante como por ejemplo a: UDP, Telnet, DNS, ICMP, HTTP y otros.

Los extremos de una red como la Internet, están unidos por el denominado núcleo de la red que constituye el conjunto de dispositivos de comunicación interconectados que enrutan los paquetes de datos, filtran información y reenvían al destino correspondiente, denominados routers.

La red más simple está formada por dos hosts (PC's) interconectados por un enlace que es el medio de comunicación cable o señal inalámbrica que transfiere los datos de un dispositivo a otro, configurados por software que se instala sus respectivas tarjetas de red, como se muestra en la figura de conexión punto a punto.

1.2 CONEXIÓN DE REDES

Una propiedad o atributo de las redes es su conexión, que consiste en el acceso directo o indirecto a los otros nodos de la red. Este acceso puede ser utilizando algún medio de comunicación físico o de forma inalámbrica; en ambos casos siguiendo alguna norma o protocolo de comunicación. Para las redes de Area Local o LAN, el estándar más popular es el protocolo Ethernet.

En el capítulo 10 desarrollaremos la conexión Inalámbrica, ahora mostraremos que la Conexión utilizando algún medio de comunicación físico, está ligado al de Topología o disposición física de los nodos y medios de red en una estructura de red a nivel de empresa. La descripción de la Conexión física, se mostrará en la Capa Física con el uso de las diferentes tecnologías Ethernet.

La Conexión a la red Internet, es un indicador TIC (Tecnología de Información y Comunicación) de los países, por cuanto marca el nivel de acceso de sus pobladores y la capacidad de sus canales de comunicación.

1.2.1 Conexión Directa

El acceso es directo si entre los dos extremos de la red, no hay otro dispositivo de comunicación.

Pueden ser a su vez:

- a. Conexión punto a punto

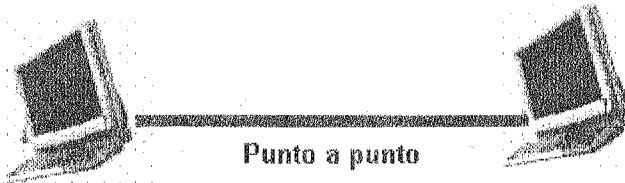


Fig. 1.1 Punto a Punto. Ambos extremos están conectados

Es el modelo más simple de comunicación que involucra conceptos básicos como la modulación y codificación de la señal, aunque poco confiable por el riesgo de la inundación de pedazos de información o tramas al receptor.

- b. Conexión de acceso múltiple

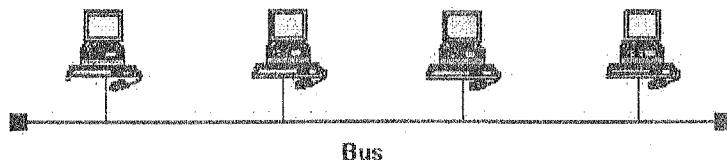


Fig. 1.2 Topología tipo Bus

Sobre un mismo canal de comunicación acceden varios equipos.

1.2.2 Conexión Indirecta

En una red como la Internet, los extremos de la red o hosts, no están unidos directamente, las subredes requieren de equipos de comunicación como los switches o hubs que se encargan de distribuir la señal a más equipos de manera inteligente o no respectivamente. (Ver fig. 1.3).

La distribución de la señal inteligente, se refiere al filtrado de los destinos posibles a un subconjunto de ellos, únicamente los que solicitaron, evitando así inundar con tramas innecesarios el canal.

En la comunicación interredes se deberá lidiar con los problemas de heterogeneidad y escalabilidad, es decir, resolver el problema de manejar bajo estándares comunes la diversidad de equipos y la necesidad de crecimiento de mayor número de subredes respectivamente. Algunos nodos de la red, servirán como postas o destinos intermedios, desde donde los paquetes son reenviados a sus destinos finales. Las topologías correspondientes a este tipo de Conexión son: estrella, anillo o árbol.

1.3 TOPOLOGÍA DE REDES

La Topología de redes se refiere al diseño básico, estructura, arreglo o disposición física de los hosts, dispositivos y medios de comunicación. La topología va a definir el equipamiento necesario, el crecimiento de la red y su forma de administración. Pasaremos a explicar las topologías mencionadas.

1.3.1 Topología tipo Bus.

Esta es la forma más simple de organización de los hosts, como se observa en la fig. un solo enlace o segmento "backbone" une a los nodos extremos, los otros hosts comparten este enlace. Cuando se realiza una transmisión sobre esta red, un solo host puede hacerlo a la vez. Aunque es fácil de instalar, tiene la desventaja de generarse colisiones de tramas al compartirse un solo canal, no se cuenta con control de acceso al medio ni con control de error en las tramas que se envían.

1.3.2 Topología Estrella.

En este diseño, los hosts se conectan a un hub o switch, de tal forma que, se llega de un solo salto a los hosts vecinos, y de éstos a su destino final por reenvío.

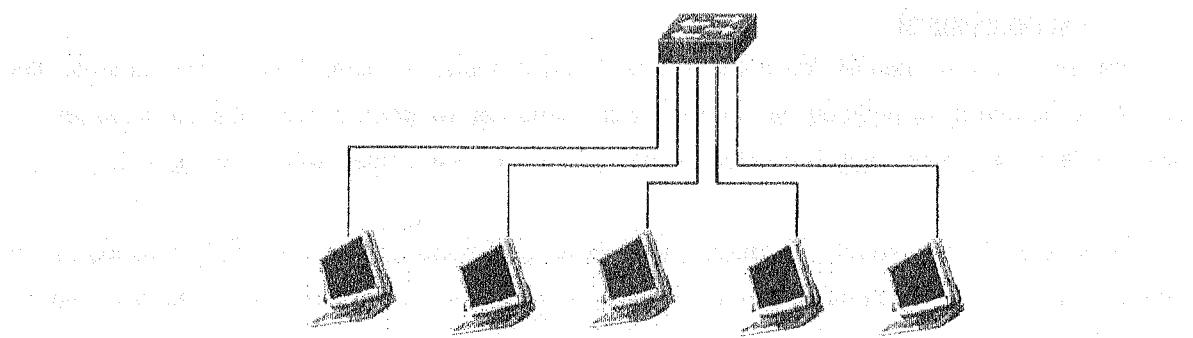


Fig. 1.3 Topología Estrella

Si alguna conexión falla, no afectará al resto de hosts de la red. En esta topología hay una gran dependencia de la eficiencia del switch, porque si éste es lento o si falla, afectará a toda la red.

1.3.3 Topología Anillo.

Aquí, todos los nodos realizan filtrado y reenvío de paquetes, al siguiente y el último con el primero. Si el destino no es el correspondiente, se reenvía al siguiente nodo. Una trama especial denominado "token" es el que se transmite por el anillo, hasta encontrar la dirección del nodo que lo solicitó. Este token se actualiza cada vez que un nodo realiza una nueva transmisión. Si bien todos los nodos tienen las mismas oportunidades de transmisión, una falla en alguno de ellos puede afectar a toda la red y su eficiencia también dependerá de la cantidad de nodos conectados.

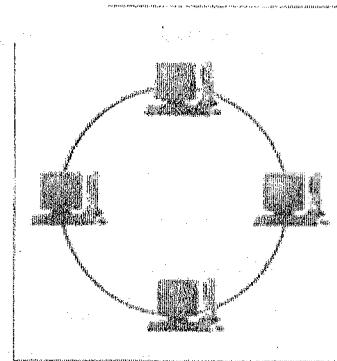


Fig. 1.4 Topología Anillo

1.3.4 Topología Arbol.

En esta forma de disposición de los nodos, éstos están organizados de manera jerárquica. En la figura 1.5, el servidor es el nodo raíz. Esta topología combina las características de la topología bus y la topología estrella. Al enlace principal o backbone se unen ramas con las características de la topología estrella según los requerimientos. Toda la red dependerá de la eficiencia del backbone.

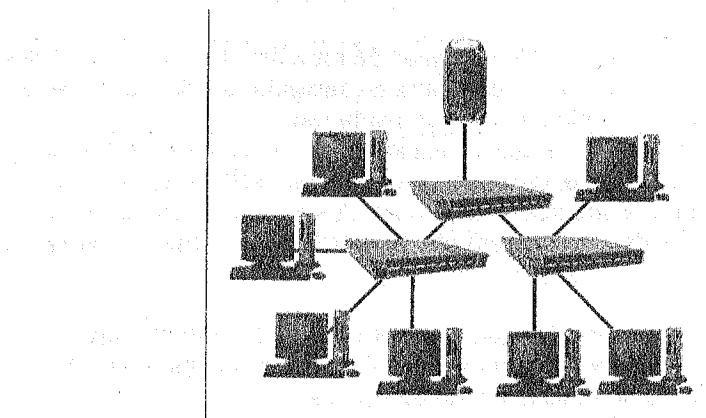


Fig. 1.5 Topologia Arbol

1.4 TIPOS DE REDES

1.4.1 Redes LAN y WAN

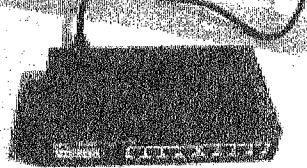
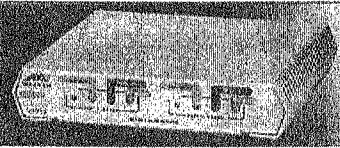
Tomando en cuenta el alcance corto o largo, las redes se clasifican en: LAN y WAN respectivamente.

Las redes LAN (Local Network Area) o de Area Local son redes que enlazan equipos que se encuentran a corta distancia, físicamente adyacentes y con una administración local, como por ejemplo: una oficina, un edificio o un campus universitario. Las redes LAN disponen de un limitado canal por donde se envía la información o ancho de banda, su capacidad de transmisión está comprendida en el rango de 1 Mbps a 1 Gbps. Las tecnologías que la implementan y que mostraremos son: Ethernet, Token Ring y FDDI.

Las redes WAN (Wide Area Network) o de Alcance Extendido, proporcionan un medio de transmisión de datos, voz e imágenes que enlazan equipos en distancias largas uniendo ciudades o países, como por ejemplo la red Internet.

Un host conectado a una red LAN, puede enviar información a todos los demás hosts de la red (comunicación broadcast), a un subgrupo de host (comunicación multicast) o a un único host (comunicación unicast).

Los dispositivos de comunicación que utilizan una red LAN para conectar, segmentar, unir redes LAN y extender los segmentos de red son: Servidores y estaciones de trabajo (hosts), hubs, repetidores, switches, puentes y routers. Los hub y los repetidores son dispositivos capa 1, los switches y puentes operan en la capa 2 y los routers en la capa 3 según el modelo de referencia basado en capas OSI que veremos más adelante.

	Hub. Actúa como punto de conexión para los host de la red, incluso interconectando dos o más hubs en cascada, ampliando de esta manera la extensión a más puntos de red.
	Switch. Físicamente son parecido al hub, es posible realizar el proceso de segmentación de usuarios, es decir, filtrar las tramas únicamente a sus destinos y no a todos los nodos conectados al segmento, de esta manera poder controlar las colisiones de la red.
	Repetidor. Dispositivo que regenera la señal, de forma que es posible extender segmentos de red o añadir nuevos host. Estos dispositivos no realiza filtrado de tramas.
	Puente. Conecta dos redes locales entre sí. Enlaza segmentos con diferentes medios de comunicación (UTP, coaxial, fibra) o enlaza diferentes segmentos de red (Ethernet, Token Ring).
	Router. Dispositivo que maneja direcciones IP y tablas de enrutamiento para conectar dos o más segmentos de red . Realizan filtrado de paquetes a la red remota.

Cuadro. 1.1 Algunos dispositivos de Comunicación

1.4.2 La red Internet

Para la descripción de la red Internet tomaremos en cuenta dos puntos de vista: una visión de servicio y una visión técnica. Es decir, que es lo que representa para los usuarios finales este servicio y por otra parte como se logra implementarla.

El correo electrónico, las páginas web, la compra de pasajes en avión, la telefonía IP, aplicaciones comerciales, educativas, etc son solo algunos de los servicios cotidianos que ofrece la red Internet a los usuarios de esta infraestructura de comunicaciones en todo el mundo. Algunas de estas aplicaciones las desarrollaremos en detalle más adelante.

Como todo servicio, la red Internet también tiene sus interrupciones por diversas causas como falta de pago, cortes de luz o factores metereológicos que afecten a la red local conectada o incluso a redes de mayor alcance cortando el servicio a uno o varios países, como la reportada por una avería de un cable de fibra óptica submarino dejando a parte de India y Egipto sin internet y lo que es importante sin muchos servicios en línea (compra de boletos de avión) para sus pobladores.³

Desde el punto de vista técnico, destacamos los siguientes aspectos de la red Internet:

³

<http://www.20minutos.es/noticia/341694/0/corte/internet/egipto/> 30/1/08

- Red con millones de nodos (hosts, routers, PDAs) que ejecutan aplicaciones de red para más de un billón de usuarios.⁴
- Red con enlaces de comunicación alámbricos (fibra óptica, cable UTP) e inalámbricos (radio, satélite).
- Con diferentes protocolos de comunicación en las distintas capas o niveles de la red que controlan el envío y recepción de información. Destacamos los protocolos de la familia TCP/IP.
- Una red de redes pública a la que se pueden interconectar redes privadas.
- Orientado hacia el mayor o mejor esfuerzo en la comunicación y no así a la calidad del servicio.
- Con múltiples comunicaciones simultáneas
- Una red de redes. Conjunto de redes interconectadas
- Uso de estándares propios, hechos públicos en los documentos RFCs o Request for Comments.

En resumen, se trata de una red de gran complejidad que la tomaremos como ejemplo en la explicación del funcionamiento de una red.

1.5 PROTOCOLOS Y ESTANDARES DE RED

Al igual que la comunicación humana, las redes de computadoras requieren de un mecanismo que les permita comprender cuando un host va a iniciar la transmisión de un mensaje, en qué momento concluye de hacerlo, por otra parte, que el otro extremo reconozca este mensaje o que le avise al trasmisor que no lo ha recibido. Este mecanismo se conoce como protocolo de red.

Los protocolos de red son el conjunto de estándares o normas que definen el formato, controlan el orden de mensajes que se envían y reciben durante una comunicación entre los hosts de una red.

En la red Internet toda comunicación se basa en protocolos y a todo nivel⁵, empezando del superior o de aplicación algunos de los más utilizados son:

- HTTP para el envío y recepción de páginas web
- SMTP para mensajes de correo electrónico
- FTP para transferencia de archivos
- DNS para la administración de nombres de dominio

⁴

http://www.newsfactor.com/story.xhtml?story_id=102000A7FV20&page=2

⁵

Ver Capítulo 3

En los niveles inferiores de la estructura de una red también se utilizan diferentes protocolos para funciones específicas, por ejemplo para el transporte los protocolos TCP y UDP. También es importante el protocolo IP que va a identificar al host y a la red o subred a la que pertenece.

Los estándares son guías que utilizan los vendedores, fabricantes o proveedores de servicio para asegurar el tipo de interconectividad necesario en los mercados actuales y en las comunicaciones internacionales (Forouzan, 2007). Los estándares son desarrollados mediante la cooperación entre comités de creación de estándares, foros y agencias reguladoras de los gobiernos. Entre las organizaciones internacionales de estándares relacionadas al área de la Telemática se encuentran:

[ANSI] - Instituto Nacional Estadounidense de Estándares

[CENELEC] - Comité Europeo de Normalización Electrotécnica.

[CEN] - Organismo de estandarización de la [Comunidad Europea] para normas EN.

[IEEE] - "Institute of Electrical and Electronical Engineers"

[IETF] - "Internet Engineering Task Force"

[ISO] - Organización Internacional para la Estandarización

[ITU-TS] –The International Telecommunications Union-Telecommunication Standards Sector

[CCITT] – Comité Consultivo para la Telefonía y la Telegrafía Internacional

A partir de 1969 se han publicado una serie de notas referidas en principio a Arpanet y posteriormente a la red Internet conocidas como Request for Comment o RFC⁶. Estas notas discuten muchos aspectos de comunicación entre computadoras, enfocándose en los protocolos de red, procedimientos, programas y conceptos. También se incluyen notas de reuniones y opiniones.

En el transcurso del libro hacemos referencia a los protocolos de comunicación y su documento RFC asociado a este protocolo donde se puede acudir para una descripción completa y detallada de este protocolo.

Según el RFC 2026, hay cinco categorías de documentos RFC. Estos pueden ser:

- Estándares, estándares para revisión o estándares propuestos
- Guías o recomendaciones oficiales.
- Experimentales. Documentos no estándares originados dentro o fuera del IETF.
- Históricos.

⁶

<http://www.rfc-editor.org/overview.html>

1.6 CONCEPTOS Y TERMINOS CLAVE

Colisión	Topología Arbol
Comunicación interredes	Topología Estrella
Conectividad	Topología tipo Bus
Conectividad de acceso múltiple	Tramas
Conectividad Directa	UMSATIC
Conectividad Indirecta	Unicast
Conectividad punto a punto	
CSMA/CD	
Ethernet	
FDDI	
Filtrado	
Host	
Hub	
Multicast	
Núcleo de red	
Protocolo TCP	
Protocolos de Red	
Protocolos TCP/IP	
Puente	
Red	
Red ARPANET	
Red de la UMSA	
Red Internet	
Redes LAN	
Redes Metropolitanas	
Redes WAN	
Repetidores	
RFC	
Router	
Servicios de Red	
Switch	
Telecomunicaciones	
Telemática	
TIC	
Token	
Token Ring	
Topología	
Topología Anillo	

1.7 PREGUNTAS DE REPASO

Seleccionar la mejor respuesta

1. Que significa un protocolo de red
 - A. Procedimientos para la comunicación entre usuarios de una red
 - B. Procedimientos sobre como se envían y reciben mensajes a través de entidades de red.
 - C. Procedimientos para establecer la conexión física de una red
 - D. Acciones específicas cuando alguien envía un mensaje

2. Cual es el medio físico de una red de computadoras
 - A. El ambiente donde se instala la red
 - B. Los cables de red, el medio electromagnético
 - C. El hardware de una computadora
 - D. Los protocolos de comunicación

3. Cual describe mejor una conexión punto a punto
 - A. Un módem a cada extremo unidos por un cable de un equipo para una comunicación
 - B. Un módem a cada extremo unido por cable compartido de un equipo para una comunicación
 - C. Un servidor de http conectado a un cliente
 - D. Otro

4. ¿Cuál de las siguientes opciones constituye la mejor definición de topología?
 - A. Una serie de equipos, impresoras y otros dispositivos conectados con fines de comunicación
 - B. La disposición física de los nodos y medios de red en una estructura de red a nivel de empresa
 - C. Un tipo de red que evita colisiones de paquetes de datos
 - D. Un método para filtrar el tráfico de red a fin de reducir la posibilidad de embotellamientos

5. ¿Cuál de las siguientes opciones define mejor la topología en estrella?
 - A. Una topología de LAN en la que un hub central se encuentra conectado mediante cableado vertical a otros hubs que dependen de él
 - B. Una topología de LAN en la que las transmisiones desde las estaciones de la red se propagan a lo largo del medio y son recibidas por todas las demás estaciones
 - C. Una topología de LAN en la que los extremos de una red se encuentran conectados a un switch central común mediante enlaces punto a punto
 - D. Una topología de LAN en la que los puntos centrales de una red se encuentran conectados a un switch central mediante enlaces lineales

6. ¿Cuál es una de las ventajas de usar una topología en estrella?

- A. Gran confiabilidad
- B. Redundancia natural
- C. Bajo costo
- D. Requiere una cantidad mínima de medios de conexión

7. La Transmisión de datos es:

- A. El envío de información mediante señales eléctricas
- B. El movimiento de datos
- C. El movimiento de información codificada, de un punto a uno o más puntos, mediante señales eléctricas, ópticas, e electroópticas o electromagnéticas.
- D. El movimiento de información de un router a una PC.

8. Emparejar los tipos de redes con los ejemplos de redes

- | | |
|----------------------------|--|
| A. Red de transporte | <input type="checkbox"/> Agua Potable |
| B. Red de comunicaciones | <input type="checkbox"/> Teléfono |
| C. Red de servicio público | <input type="checkbox"/> Alcantarillado |
| D. Red social | <input type="checkbox"/> sistema de autopistas |

9. Cual de los siguientes enunciados NO es un objetivo de las redes de computadoras:

- A. Chatear
- B. Trabajo en equipo
- C. Compartir recursos
- D. Ahorro económico

10. Emparejar los conceptos con la descripción

- | | |
|-------------------------------------|---|
| A. Conectividad | <input type="checkbox"/> Servicio Confiable |
| B. Encapsulamiento | <input type="checkbox"/> Acceso Indirecto o directo a los nodos |
| C. Modelo de referencia | <input type="checkbox"/> Colocar cabeceras |
| D. Servicio Orientado a la Conexión | <input type="checkbox"/> Normas de diseño de redes |

11. En un laboratorio de redes se adquieren 5 nuevas computadoras para su red LAN, cuales son las posibles conexiones que se pueden hacer. (Puede existir mas de una respuesta)

- A. Conexión Punto a Punto
- B. Conexión usando un bus de datos (conectividad múltiple)
- C. Utilizando un switch o Hub
- D. Utilizando un router

12. Emparejar los conceptos de Topología con su descripción

- | | |
|-------------|--|
| A. Estrella | _____ La estructura de nodos es jerárquica |
| B. Anillo | _____ Todos los nodos se conectan a un canal veloz |
| C. Bus | _____ Un camino de un solo salto a cualquier nodo |
| D. Arbol | _____ Todos los nodos realizan filtrado y reenvío |

13. Las normas o protocolos de Internet son difundidos en:

- A. Los estatutos de los ISP's
- B. Los RFC's
- C. Las normas de los países donde se accede a internet
- D. No existe documentación estándar

14. Haciendo una analogía de la red de datos con la red telefónica, cuando una persona se comunica con otra, utiliza un servicio:

- A. Sin conexión
- B. Confiable
- C. Orientado a la Conexión
- D. No confiable

15. Indique los tipos de conectividad indirecta

- A. Estrella
- B. Bus
- C. Anillo
- D. Ninguno

1.8 TALLER

1. Dar 3 ejemplos de protocolos de comunicación humana y discutir en el grupo los procesos de: establecimiento de la comunicación, la transmisión de información y el cierre de la comunicación.
2. Para la topología tipo estrella, discuta en el grupo: el equipo de red que se requiere, las posibilidades de crecimiento y la forma de filtrado de información que realiza.
3. Discuta las ventajas y desventajas del trabajo en redes y en el modo "stand-alone"
4. Se desea instalar una red LAN con conexión a Internet, cuales son los aspectos de diseño que deberán resolverse ?

CAPITULO 2 ESTRUCTURA DE UNA RED

Objetivos de Aprendizaje: Al concluir el capítulo, usted será capaz de:

- Describir los componentes de una red,
- Mostrar las técnicas de transmisión de datos a través del núcleo de la red y
- Explicar dos modelos de implementación de redes.

2.1 HOSTS Y SUBREDES

En una vista más cercana a una red, identificamos básicamente a dos componentes que son los extremos de la red o hosts y las subredes que se constituyen en el núcleo de la red conformada por routers, switchs, hubs y otros dispositivos y medios de comunicación.

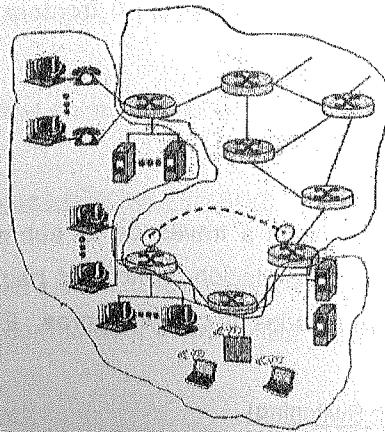


Fig. 2.1 hosts y subredes

En los hosts se ejecutan y corren los programas de aplicación como las páginas web, correo electrónico, chat, etc. Estos equipos están en contacto y se interrelacionan con los usuarios, administradores de red o clientes finales, se los clasifica en dos categorías: clientes y servidores.

Los equipos cliente son las terminales, estaciones de trabajo, computadoras personales, celulares o PDA que descargan información referida a la aplicación. Para esto deberán configurarlos y ejecutarse los protocolos de comunicación respectivos.

Aunque es posible que un equipo pueda configurar como servidor, es recomendable que el servidor tenga mejor capacidad que los clientes, tanto en cuanto al procesador, memoria, almacenamiento interno, ranuras de expansión y velocidad de conexión a la red. (Ver fig. Requerimientos mínimos de hardware para el uso de la red).

12. Emparejar los conceptos de Topología con su descripción
- | | |
|-------------|--|
| A. Estrella | _____ La estructura de nodos es jerárquica |
| B. Anillo | _____ Todos los nodos se conectan a un canal veloz |
| C. Bus | _____ Un camino de un solo salto a cualquier nodo |
| D. Arbol | _____ Todos los nodos realizan filtrado y reenvio |
13. Las normas o protocolos de Internet son difundidos en:
- A. Los estatutos de los ISP's
 - B. Los RFC's
 - C. Las normas de los países donde se accede a internet
 - D. No existe documentación estándar
14. Haciendo una analogía de la red de datos con la red telefónica, cuando una persona se comunica con otra, utiliza un servicio:
- A. Sin conexión
 - B. Confiable
 - C. Orientado a la Conexión
 - D. No confiable
15. Indique los tipos de conectividad indirecta
- A. Estrella
 - B. Bus
 - C. Anillo
 - D. Ninguno
- 1.8 TALLER**
1. Dar 3 ejemplos de protocolos de comunicación humana y discutir en el grupo los procesos de: establecimiento de la comunicación, la transmisión de información y el cierre de la comunicación.
 2. Para la topología tipo estrella, discuta en el grupo: el equipo de red que se requiere, las posibilidades de crecimiento y la forma de filtrado de información que realiza.
 3. Discuta las ventajas y desventajas del trabajo en redes y en el modo "stand-alone"
 4. Se desea instalar una red LAN con conexión a Internet, cuales son los aspectos de diseño que deberán resolverse ?

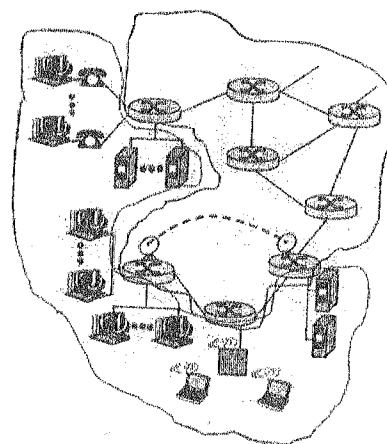
CAPITULO 2 ESTRUCTURA DE UNA RED

Objetivos de Aprendizaje: Al concluir el capítulo, usted será capaz de:

- Describir los componentes de una red,
- Mostrar las técnicas de transmisión de datos a través del núcleo de la red y
- Explicar dos modelos de implementación de redes.

2.1 HOSTS Y SUBREDES

En una vista más cercana a una red, identificamos básicamente a dos componentes que son los extremos de la red o hosts y las subredes que se constituyen en el núcleo de la red conformada por routers, switchs, hubs y otros dispositivos y medios de comunicación.



— Extremos
— Subredes

Fig. 2.1 hosts y subredes

En los hosts se ejecutan y corren los programas de aplicación como las páginas web, correo electrónico, chat, etc. Estos equipos están en contacto y se interrelacionan con los usuarios, administradores de red o clientes finales, se los clasifica en dos categorías: clientes y servidores.

Los equipos cliente son las terminales, estaciones de trabajo, computadoras personales, celulares o PDA que descargan información referida a la aplicación. Para esto deberán configurarlas y ejecutarse los protocolos de comunicación respectivos.

Aunque es posible que una PC se pueda configurar como servidor, es recomendable que el servidor tenga mejor capacidad de hardware en cuanto al procesador, memoria, almacenamiento interno, ranuras de expansión, que otro equipo cliente de la red. (Ver fig Requerimientos mínimos de hardware para el usuario, capítulo 11).

Por estas características, los servidores son los encargados de almacenar información de la aplicación y de permitir o denegar el acceso y envío de esta información al cliente, también mediante protocolos de comunicación con el cliente.

Como la aplicación se ejecuta en uno o más equipos cliente, que están conectados a un extremo de la red y en el servidor que se encuentra en el otro extremo, estas se denominan *aplicaciones distribuidas*. Este modelo de comunicación se denomina Cliente Servidor que explicaremos en este capítulo.

El conjunto de routers que forman la subred¹ o malla de routers constituyen el *núcleo de la red*. Por los routers circulan los paquetes de información, se filtran los paquetes y se encaminan a su destino final en el otro extremo.

El encaminamiento por el núcleo de la red podrá ser dividido en regiones de manera jerárquica para llegar a todos los nodos de la red. Los tramos en la frontera y al interior de la red serán administrados mediante protocolos de enrutamiento.

2.2 TIPOS DE TRANSMISIÓN DE DATOS

Para la transmisión de datos entre los hosts a través de la subred o analizaremos dos tipos fundamentales de técnicas llamadas de comutación "switching" haciendo referencia a un estado de paso libre o no, que tenían las primeras redes de computadoras. Estas técnicas son:

2.2.1 Comutación de circuitos (Circuit Switching)

Una red de comutación de circuitos consta de un conjunto de comutadoras (nodos) conectados por enlaces físicos. Cada enlace normalmente se divide en n canales. En esta técnica durante una sesión se reservan los recursos necesarios (buffer, ancho de banda) para proveer comunicación de un extremo al otro, formando un circuito o canal entre nodos y marcando la trayectoria antes que los usuarios se comuniquen.

Un circuito que ya está reservado, garantiza su eficiencia, no se puede utilizar hasta que sea liberado y se establezca una nueva comunicación. Esta técnica de transmisión la utiliza el sistema telefónico, donde la persona que llama a otra, utiliza la red local, nacional o con conexión internacional de telefonía la cual primeramente activa los nodos necesarios para establecer la conexión entre la persona que llama y la que recibe.

¹ Este concepto difiere del que explicaremos en la capa de Red.

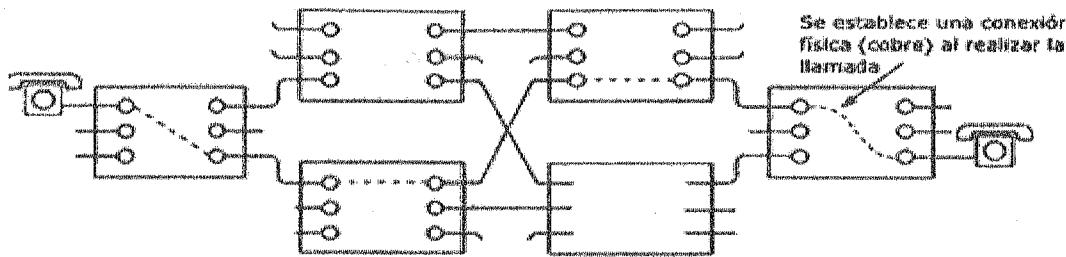


Fig. 2.2 Comutación de circuitos

Cuando ya se ha establecido la comunicación o conversación, hay momentos de pausa donde las dos personas callan. En estos períodos de tiempo "muertos", el canal no puede ser utilizado por otro enlace porque los recursos están reservados para estas personas.

El enlace de un circuito que está siendo utilizado divide el espectro de comunicación asignando:

- un rango de frecuencias a las conexiones que solicitan mientras dure la conexión, o FDM
- divide el tiempo del enlace en períodos cortos o slots TDM.

2.2.2 Comutación de paquetes (Packet switching)

Los flujos de datos se dividen en bloques de datos o paquetes que se envían a la red a través de los denominados *routers* o "comutador de paquetes" pero a diferencia de la anterior técnica, no se reserva ningún recurso.

Si un enlace de la red está congestionado, porque otros paquetes requieren ser enviados, entonces nuestro paquete deberá primeramente esperar su turno almacenándose en el buffer del router formándose una cola de paquetes y luego ser reenviado al enlace, utilizando todo el ancho de banda.

La mayoría de los routers almacenan y reenvían los paquetes en la entrada de los enlaces. Es decir, el router debe recibir el paquete entero antes de reenviarlo, lo cual produce una demora en la entrada de cada enlace. Esta demora es directamente proporcional al tamaño del paquete e inversamente proporcional al ancho de banda. Por ejemplo, si un paquete tiene L bits y el ancho de banda del canal es de R bps, entonces la demora es L/R segundos.

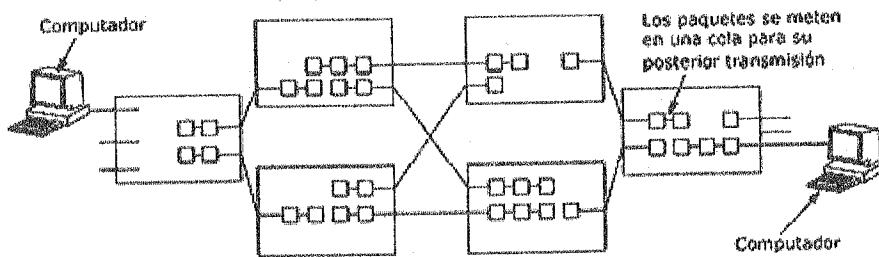


Fig. 2.3 Comutación de paquetes

Esta técnica es utilizada por Internet donde múltiples solicitudes, para compartir un enlace, son atendidas al mismo tiempo haciendo más eficiente que la comutación por circuitos especialmente cuando hay un volumen repentino de datos.

2.3 MODELO CLIENTE SERVIDOR

Este modelo es el que prevalece en Internet y consiste en compartir el trabajo referido al procesamiento de datos que realizan los extremos de la red o hosts que se están comunicando, denominados cliente y servidor.

El cliente sirve de interfaz con el usuario, es el responsable de presentarle al usuario información legible, interactúa con el servidor y despliega la información que recibe de éste.

El servidor básicamente está dedicado al almacenamiento y administración de los datos. Esta administración consiste en el ordenamiento de datos, extracción de los datos solicitados y envío al usuario a través del cliente.

Como ejemplo, del proceso de comunicación Cliente/Servidor, mostramos un caso básico entre un cliente A y un servidor B para una aplicación X :

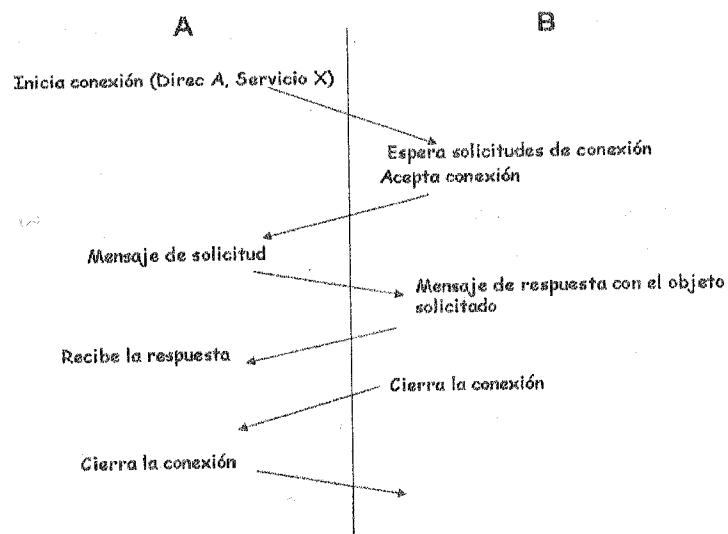


Fig. 2.4 Comunicación Cliente Servidor

Este modelo, no requiere tener necesariamente dos computadoras, incluso en el mismo equipo es posible hacer correr procesos cliente y proceso servidor.

Las aplicaciones que corren bajo este modelo son varias, como por ejemplo: páginas web, correo electrónico, hojas de cálculo, administración de documentos, almacenamiento centralizado de archivos y otros.

Este modelo es beneficioso para una institución que tenga gran cantidad de personas con necesidad de acceso continuo a una gran cantidad de datos. Su administración está centralizada en el servidor.

Hay varias configuraciones o arreglos de este modelo.

- Configuración Simple. A su vez se puede subdividir en:
 - Un cliente y un servidor
 - Un servidor y varios clientes (Fig. 2.5)
- Configuración con servidores distribuidos
 - Servidores sobre una red WAN periódicamente sincronizados
 - Servidores organizados jerárquicamente (Fig. 2.6)

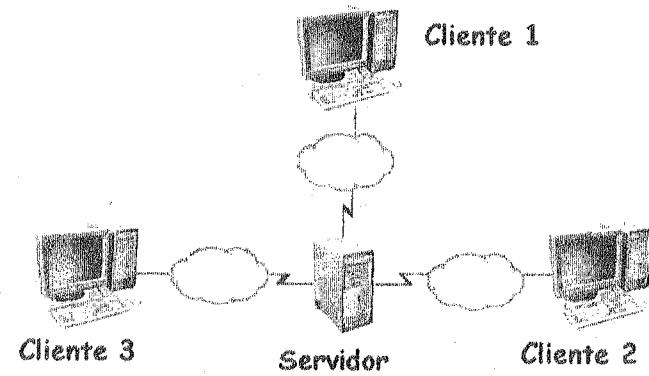


Fig. 2.5 Esquema C/S con un servidor y varios clientes

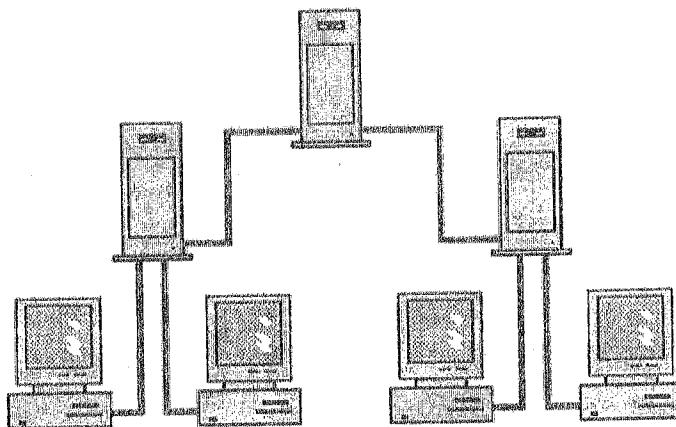


Fig. 2.6 Esquema C/S con servidores distribuidos jerárgicamente

La aplicación más común que utiliza el modelo Cliente Servidor es la administración de bases de datos. Nosotros volveremos con este modelo en el capítulo 4 de Aplicaciones de red.

2.4 MODELO PEER TO PEER

Bajo este modelo, cualquiera de los extremos puede fungir como servidor y cliente, es decir, no hay un servidor dedicado la comunicación es entre iguales y no hay jerarquía entre los computadores, por lo que se los conoce como "peers" o "de a par" o "punto a punto".(P2P).

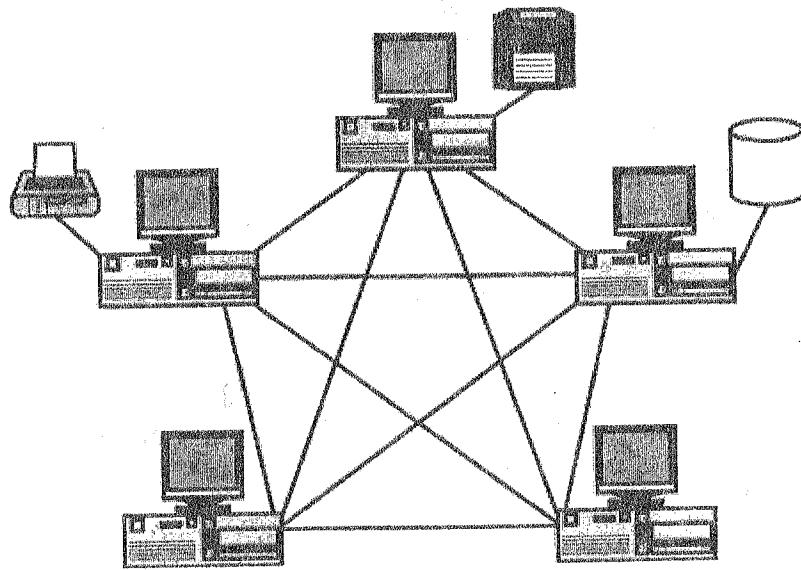


Fig 2.7 Esquema del Modelo Peer to Peer

Este modelo es menos costoso de implementar y mantener que los modelos basados en servidores, no requiere el mismo nivel de seguridad y de rendimiento que el software diseñado para servidores dedicados.

El usuario de cada computador determina cual información del sistema debiera compartirse con los otros usuarios de la red. De esta forma, su rol es más importante que en el modelo Cliente Servidor.

Las aplicaciones más comunes de P2P incluyen sistemas para compartir archivos tales como eDonkey, Kazaa, así como sistemas de voz sobre IP (VoIP) como Skype y Google Talk. Por otra parte, los sistemas P2P contribuyen a más del 50% del tráfico de la red. (Steinmetz, 2005).

Por ejemplo en una aplicación para compartir archivos (música, fotos), bajo el modelo P2P cada usuario dispondrá de mayor almacenamiento según sus requerimientos.

Según Zacker,² las características para implementar este modelo son:

- que los usuarios de la red sean menos de diez
- Todos los usuarios se encuentran en el mismo area
- Que el criterio de seguridad no sea sensible para la red
- Que no se tengan planes de crecimiento
- No hay un administrador encargado de gestionar toda la red
- No se requiere soft ware adicional

2.5 LA ESTRUCTURA DE LA RED DE LA UMSA

La infraestructura ya instalada de la red de la UMSA es de tipo intercampus, hay dos anillos el norte y el sur que interconectan a 23 predios de la UMSA. Su diseño, implementación y administración está basado en el modelo jerárquico de tres capas de Cisco Systems ® con dos núcleos; situados en el área central de cobertura de la UMSA, uno en el edificio Hoy y el otro en el Monoblock Central.

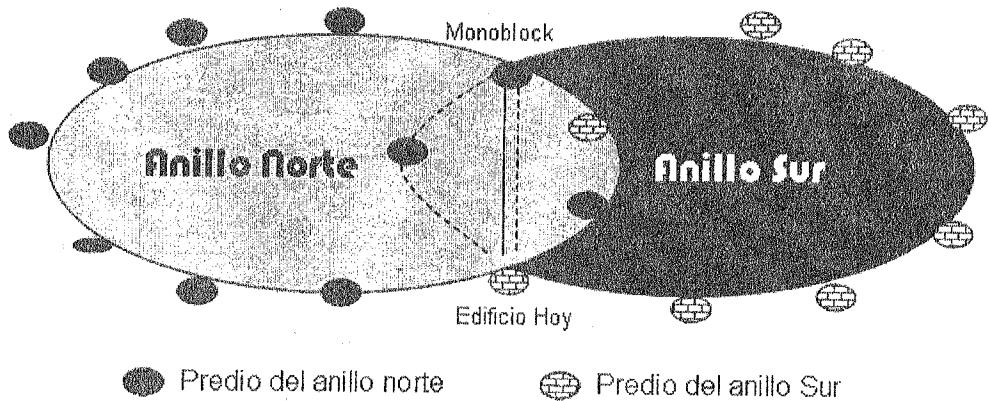


Fig. 2.8 Los anillos de la red de la UMSA

²

Zacker Craig. Networking Essentials, Part. I pág. 101

Ambos núcleos de la red están equipados con switches Cisco Catalyst 6509, que actúan como los routers principales de la red. Estos están conectados vía fibra óptica con puertos Gigabit Ethernet a modems de los proveedores de servicio internet y distribuyen la conectividad a los predios de la UMSA, mediante cableado estructurado (norma IEEE 568 B) con una extensión de 47 Kms de fibra óptica monomodo de 1 Gigabyte de ancho de banda.

Los switches Cisco Catalyst 3750 ubicados en los predios de la UMSA a su vez conectan a las diferentes unidades académicas utilizando para ello cableado estructurado con una extensión de 8 Kms de fibra óptica tipo multimodo de 1 Gigabyte de ancho de banda, contando con diez servicios de distribución principal o MDF (Main Distribution Facility) donde se sitúan los paneles de distribución, concentradores, comutadores, enruteadores y servidores.

A nivel de acceso, según el modelo de Cisco Systems ®, la red de la UMSA cuenta con switches Cisco Catalyst 2950 y 2960 de 48 y 24 puertos que están ubicados en diez servicios de distribución intermedia o IDF (Intermediate Distribution Facility). A este nivel, se han tendido 100 Kms de cable de cobre (UTP) de 100 Mbps.

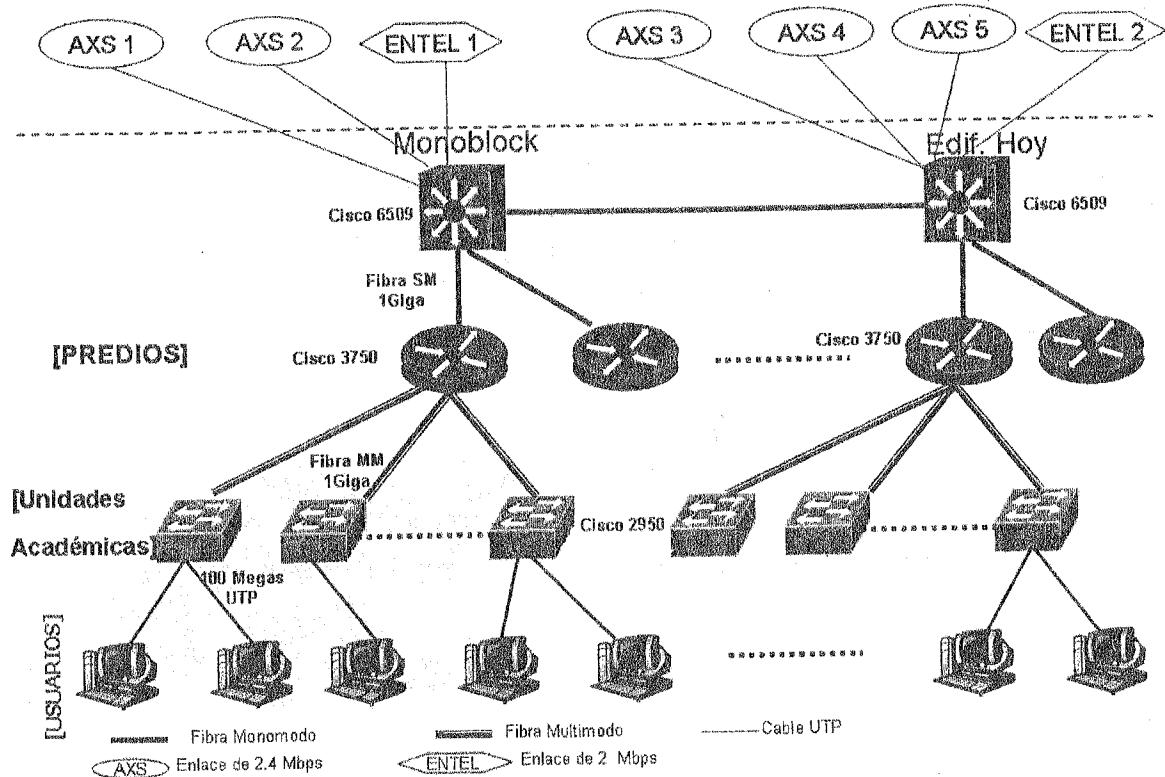


Fig. 2.9 Estructura de la red de la UMSA

La red de la UMSA está equipada con dos switches Cisco Catalyst 6509, que actúan como los routers principales de la red. Estos están conectados vía fibra óptica al backbone y a muchos switches Cisco Catalyst 3750 que distribuyen la conectividad a los predios de la UMSA.

Como conclusión, la red de la UMSA tiene una infraestructura instalada según las normas vigentes y está a la altura de su importancia en el contexto nacional a nivel de una red educativa de servicio. Entre sus fortalezas, tiene redundancia en los enlaces a los predios, sobre la que se podrán realizar aplicaciones, como el servicio de VoIP que próximamente se tiene previsto implementar en todos los predios. No podemos negar que se presentan dificultades en el servicio a los usuarios finales sobre todo para el acceso a Internet desde sus predios, ya que el cuello de botella se encuentra en los enlaces externos de los proveedores de Internet que en promedio no superan los 2 Mbps, a pesar que al interior de la red el ancho de banda es de 100 Mbps a 1 Gbps.

2.6 CONCEPTOS Y TERMINOS CLAVE

Círculo
Cisco Router
Cisco Switch
Cliente
Comutación de Circuitos
Comutación de Paquetes
Encaminamiento
Enlace
Estructura de red
Modelo Cliente/Servidor
Modelo Peer to Peer
Paquete
Servidor
Subredes
Switching
Tipos de transmisión de datos

2.7 PREGUNTAS DE REPASO

1. Con que otro nombre se denomina al Commutador de Paquetes
 - A. Hub
 - B. Host
 - C. Router
 - D. Switch

2. Cual es la función de los hosts en una red
 - A. Ejecutar y correr programas de aplicación
 - B. Delimitar a la red
 - C. Evitar que ingresen hackers a la red
 - D. Transportar los paquetes al destino correspondiente

3. Para que se utilizan los servidores en una red
 - A. Ser la interface con otras redes
 - B. Almacenar la información de la aplicación
 - C. Permitir o denegar el acceso y envío de esta información al cliente
 - D. B y C

4. Para que se utilizan los equipos cliente en una red
 - A. Ser la interface con el usuario
 - B. Almacenar la información de la aplicación
 - C. Permitir o denegar el acceso y envío de esta información al servidor
 - D. Ser utilizados por personas invitadas que ingresan a la red

5. A que se denomina el núcleo de la red
 - A. Al Internet
 - B. Al conjunto de routers
 - C. Al conjunto de servidores
 - D. Al conjunto de hosts

6. Una red de reserva todos los recursos de la red para una comunicación
 - A. Comutación de paquete
 - B. Comutación de circuito
 - C. Comutación de línea física
 - D. Comutación de routers

7. Una red de No puede utilizarse hasta que todos los recursos sean liberados y se establezca una nueva comunicación
- Commutación de paquete
 - Commutación de circuito
 - Commutación de línea física
 - Commutación de routers
8. Una red de almacena los paquetes en un buffer esperando su turno para ser reenviados al enlace correspondiente.
- Commutación de paquete
 - Commutación de circuito
 - Commutación de línea física
 - Commutación de routers
9. En una red que envia paquetes de 20 bits con una demora de transmisión de 5 segundos, cual es el ancho de banda que se utiliza para esta transmisión
- 100 bits/seg
 - 4 K bits/seg
 - 5 bits/seg
 - 4 bits/seg
10. El es el que inicia la comunicación en el modelo Cliente/Servidor
- Servidor
 - Router
 - Cliente
 - Usuario
11. Indique una posible configuración de modelo Cliente/Servidor
- Varios servidores y un cliente
 - Varios clientes y un servidor
 - Servidores organizados jerárquicamente
 - B y C
12. En el modelo Peer to Peer:
- El cliente tiene mayor jerarquía que el servidor
 - No hay jerarquías entre los computadores de la red
 - Hay un servidor dedicado
 - Se mantiene el concepto Cliente/Servidor

13. Una aplicación del modelo Peer to Peer es:
- A. http
 - B. DNS
 - C. Skype
 - D. FTP
14. Cual de los siguientes criterios se utiliza para implementar un modelo Peer to Peer
- A. Que no se tengan planes de crecimiento
 - B. La seguridad de la red
 - C. La administración de la red
 - D. Para un gran número de usuarios
15. En el modelo Cliente/Servidor, como se realiza el cierre de la conexión:
- A. Lo inicia el Cliente
 - B. Simultáneamente el Cliente y el Servidor
 - C. Lo inicia el Servidor
 - D. Ninguno

2.8 TALLER

1. Identificar el concepto genérico del funcionamiento del Modelo Cliente/Servidor y buscar en otras áreas otros modelos o productos que cumplan con esa finalidad genérica. Explicar.
2. Establecer una analogía entre los medios físicos, los enlaces de comunicación, control de flujo, control de congestión, los extremos y el núcleo de una red de datos con otras dos redes.
3. Deseamos adquirir de España, un equipo de computación. Se conoce que el envío debe ser por barco con escalas en 4 países antes de llegar a Bolivia. Si en el primer país se tarda 5 días y se almacena 8 horas, en el 2do. 10 días y se almacena 10 horas, en el 3ro 20 días y se almacena 12 horas, finalmente en el 4to. 15 días y se almacena 16 horas, sabiendo que las distancias son de 1,000 Kms, 5000 Kms, 15000 Kms y 4000 Kms respectivamente. Si el barco viaja a 50 Kms / hora. En cuantos días llegará a La Paz si la distancia al puerto más cercano es de 8 hrs y el transporte terrestre va a 80 Kms/h.

CAPITULO 3 MODELOS DE REFERENCIA

Objetivos de Aprendizaje: *Al concluir el capítulo, usted será capaz de:*

- *Conocer la arquitectura de redes en el que están basados los modelos de referencia OSI, TCP/IP y el modelo jerárquico de CISCO.*
- *Identificar las funciones básicas de las capas del modelo OSI*
- *Determinar las características principales del modelo TCP/IP*
- *Establecer los aspectos básicos del modelo jerárquico de CISCO para describir la red*

3.1 FILOSOFÍA DE LOS SISTEMAS ABIERTOS

Durante las últimas dos décadas ha habido un enorme crecimiento en la cantidad y tamaño de las redes. Al principio (1980) éstas se desarrollaron utilizando implementaciones de hardware y software diferentes. Como resultado, muchas de ellas redes eran incompatibles y se volvió muy difícil para las redes que utilizaban especificaciones distintas.

Los sistemas de comunicación de hardware y software que ofrecían los fabricantes, solo permitía que sus propias computadoras intercambiaran información. Estos sistemas se denominaron Cerrados o Propietarios porque las computadoras de otros fabricantes no podían intercambiar información a menos que se ajusten a las normas de un fabricante determinado.

Para solucionar este problema, diversas organizaciones internacionales como ISO, ITU-TS, realizaron varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) y compatibilidad utilizando estándares abiertos.

La primera estandarización conocida como el modelo de referencia OSI (Open Systems Interconnection), la introdujo la ISO en 1984, con el propósito de apoyar a los vendedores y desarrolladores de software para producir sistemas de redes interoperables. El término "Open System" se refiere a que las especificaciones técnicas se hacen públicas disponibles a todos.

3.2 ARQUITECTURA DE UNA RED DIVIDIDA EN CAPAS

Hay varias razones por las cuales se utiliza una técnica estructurada donde las redes se dividen en capas o niveles. Mencionamos las siguientes:

- Reduce la complejidad de su diseño. Al estar organizadas como un conjunto de capas o niveles, cada una construida sobre la anterior. No muchas capas, para no dificultar su descripción más de lo necesario.
- Estandariza las interfaces. Facilita el intercambio de información de un fabricante a otro.
- Asegura la interoperatividad de la tecnología. Ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto.
- Acelera la evolución. Con un modelo de red dividido en capas, el desarrollo de cada una es más rápido, una capa debiera crearse donde las funciones son fácilmente localizadas. Esto facilita el rediseño de la capa para aprovechar las nuevas tecnologías.
- Simplifica la enseñanza y el aprendizaje. Bajo este enfoque, las problemáticas de cada capa es analizada por separado, por ejemplo, similares funciones se deben realizar en la misma capa. Para su descripción intervienen protocolos de comunicación, entidades y servicios según cada capa.
- Facilita la técnica modular. Una capa debiera crearse donde haya necesidad de un diferente nivel de abstracción en el manejo de datos y los cambios de funciones o protocolos de una capa no debieran afectar a las otras.

El número de capas y el nombre difiere de un modelo de referencia a otro. El propósito de una capa es ofrecer servicios a las capas superiores tal que no se tengan que ocupar del detalle de la implementación real de los servicios.

La comunicación entre las capas es de dos tipos: Real y Virtual. La primera se establece cuando la información generada en la capa superior baja a las capas inferiores a través de interfaces entre capas y procesos. Un proceso que las redes utilizan para una comunicación real es el de Encapsulamiento de datos que veremos a continuación.

La comunicación virtual se lleva a cabo cuando cada par de capas de un mismo nivel se ponen en contacto a través de los protocolos específicos para cada capa. En estos protocolos va información de encabezado que identifica al origen y al destino de los datos. El protocolo par del sistema de recepción leerá esta información. En la figura se aprecian estos tipos de comunicación.



Fig. 3.1 Tipos de comunicación en una red

3.3 ENCAPSULAMIENTO DE DATOS

La información que envían los usuarios finales por la red, como correo electrónico o páginas web antes de ser enviadas a sus destinos, deberá pasar por las capas inferiores de la red de origen hasta la capa Física donde se transforma en secuencias de bits, para su transmisión por el medio que utilice la red y la entidad de destino entregará a donde corresponda.

Este proceso se denomina Encapsulamiento que consiste en empaquetar los datos, añadir cabeceras o información de control a medida que los datos se desplazan a través de las capas y realizar la transformación a bits para su transmisión. En el otro extremo de la red, se produce el proceso es inverso, es decir el desencapsulamiento. En la figura mostramos este proceso, para el caso de envío de correo electrónico.

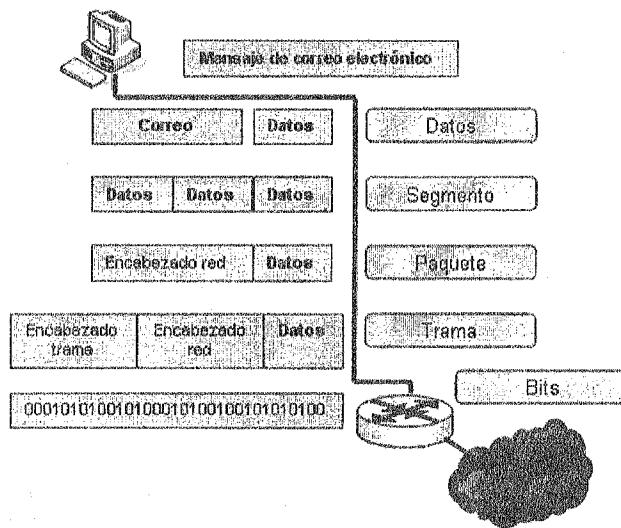


Fig. 3.5 Encapsulamiento de datos

En la figura 3.5, cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden enviarse por la red. Luego estos datos se empaquetan formando una unidad de información a nivel de la capa de Transporte denominado Segmento. A éstos se añade encabezados y se forman los Paquetes. Cuando pasan a la capa de Enlace, nuevamente se añade otra cabecera, denominado Encabezado de trama. Finalmente se transforma en secuencia de bits para su transmisión.

3.4 MODELO OSI

El Modelo de referencia Open System Interconnection (OSI) que fue lanzado en 1984 por una de las primeras instituciones dedicadas a la estandarización como es la International Organization for Standardization (ISO) surge a tono con la filosofía de los sistemas abiertos, para enfrentar el problema de incompatibilidad de las redes y su imposibilidad de comunicarse entre sí, es uno de los dos modelos de referencia que está orientada hacia una arquitectura de red dividida en capas y a la comprensión de la comunicación de datos.

A pesar de tener un conjunto de protocolos (FTAM, X.400, X.500), el modelo OSI es considerado un modelo teórico porque solo es utilizado como una herramienta de referencia y aprendizaje, porque estos protocolos nunca han sido lo suficientemente prácticos como para liberarlos como producto comercial.

Este modelo (ver fig 3.2) presenta siete capas claramente diferenciadas, con funciones específicas para cada una. Una perspectiva de análisis del modelo es tipo Top Down (de arriba hacia abajo) , como sugiere Kurose (1999), iniciando en la capa superior, concluyendo en la inferior y son las capas de: Aplicación, Presentación, Sesión, Transporte, Red, Enlace y Física.

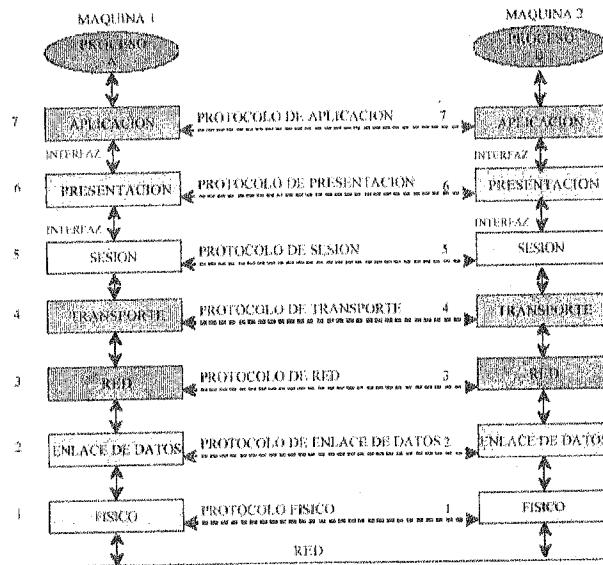


Fig. 3.2 Capas y protocolos del Modelo OSI

3.3.1 Capa de Aplicación

Es la capa que provee un medio para que el usuario acceda a información de la red a través de programas denominados Agentes de Usuario, los que a su vez interactúan con el usuario. Por ejemplo, el usuario que desea ver su correo electrónico lo hace a través de un programa que está instalado en su equipo.

Proporciona servicios a procesos de aplicación que corren tanto en el cliente como en el servidor. Aquí se sincronizan las aplicaciones que cooperan entre sí y establece los procedimientos para la recuperación de errores y el control de la integridad de los datos.

3.3.2 Capa de Presentación

Transforma los datos (conversión de formatos, encriptación y compresión de datos) para proveer una interface estándar a la capa de Aplicación, de tal forma que se garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. Por ejemplo convertir un archivo de texto en formato EBCDIC a otro archivo en formato ASCII.

3.3.3 Capa de Sesión

Esta capa controla el establecimiento, la gestión y cierre de sesiones entre la aplicación local y la remota. Las sesiones se refieren a los diálogos y a las conexiones que realizan las aplicaciones. Es decir, con quien y como mantener la comunicación.

En el establecimiento se controlan los derechos de acceso, en la gestión, se administran los puntos de parada y recuperación , y finalmente esta capa es la encargada de cerrar la sesión de una manera adecuada.

3.3.4 Capa de Transporte

Aquí se provee transporte fiable de datos entre los usuarios finales, liberando a la capa de Aplicación de esta función. La capa de transporte controla la fiabilidad de un enlace a través del control de flujo, el entramado y el control de error, de tal forma que si es necesario se tengan que retransmitir algunos paquetes.

El control de flujo se refiere a evitar una saturación del sistema receptor cuando el emisor envía datos, el entramado es la división de los mensajes y reajustar su tamaño para que sea válido para la capa de red. El control de error permitirá recuperar el sistema de errores y fallos.

3.3.5 Capa de Red

Esta capa es la responsable de la transmisión de paquetes entre dos sistemas finales (el origen y el destino final) proporcionando conectividad y selección de rutas para que los paquetes lleguen a sus destinos.

Cuando esta capa recibe los paquetes de la capa de Transporte, añade su propia cabecera que contiene la información necesaria para trasladar el paquete desde el emisor hasta el receptor. La unidad de información de esta capa es el paquete.

3.3.6 Capa de Enlace

Esta capa provee el tránsito de datos a través de un enlace físico. Se ocupa del direccionamiento físico, de la topología de red, el acceso a la red, la detección y corrección de errores que pueden ocurrir en la capa Física, la entrega ordenada de datos empaquetados (tramas) y el control de flujo.

La trama incluye un mecanismo de detección de error para verificar que los paquetes llegaron intactos. En redes LAN, el protocolo de la capa de Enlace también implementa un mecanismo de control de acceso al medio o MAC. Este mecanismo es el algoritmo que usa un computador para negociar el acceso al medio que comparte con otros que se encuentran en la red y evitar que aquellos computadores transmitan sus datos al mismo tiempo.

3.3.7 Capa Física

Esta es la capa inferior del modelo OSI y es la responsable de la transmisión de un conglomerado de bits que no reconoce tramas, cabeceras u otros protocolos a través de un medio de red, como ser un cable o un medio inalámbrico.

La capa Física también define las especificaciones eléctricas y mecánicas, las características de hardware del medio físico de la red como el tipo de cable, y detalles de instalación como longitud del cable, los conectores, etc.

3.5 MODELO TCP/IP

Este modelo de referencia diseñado en los años 70 en el proyecto DARPA¹, es el que utiliza la red Internet y su nombre se deriva de dos de los más importantes protocolos que lo conforman: el Transmission Control Protocol (TCP) y el Internet Protocol (IP). El conjunto de protocolos se denomina "suite" o familia de protocolos TCP/IP. El principal objetivo del diseño de TCP/IP fue construir una interconexión de redes o inter-red que provea servicios de comunicación universal sobre redes físicas heterogéneas, independiente de la plataforma y del hardware.

Actualmente, gracias al TCP/IP es posible la comunicación entre hosts de diferentes redes que pueden encontrarse separadas geográficamente por grandes distancias. Otras ventajas son:

- Soporte por la mayor parte de proveedores informáticos.
- Independencia de la tecnología.
- Desarrollo de programas de interface.
- Interconexión Universal
- Elimina las fronteras entre plataformas.
- El administrador puede asignar y re-asignar direcciones.

Este modelo al igual que el modelo OSI, está basado en una pila de capas porque para que una aplicación que corre sobre el host de destino obtenga un paquete de una aplicación que corre sobre el host de origen, el paquete tiene que bajar y volver a subir por las capas (la pila).

¹

Agencia de Proyectos de Investigación Avanzada para la Defensa, EEUU.

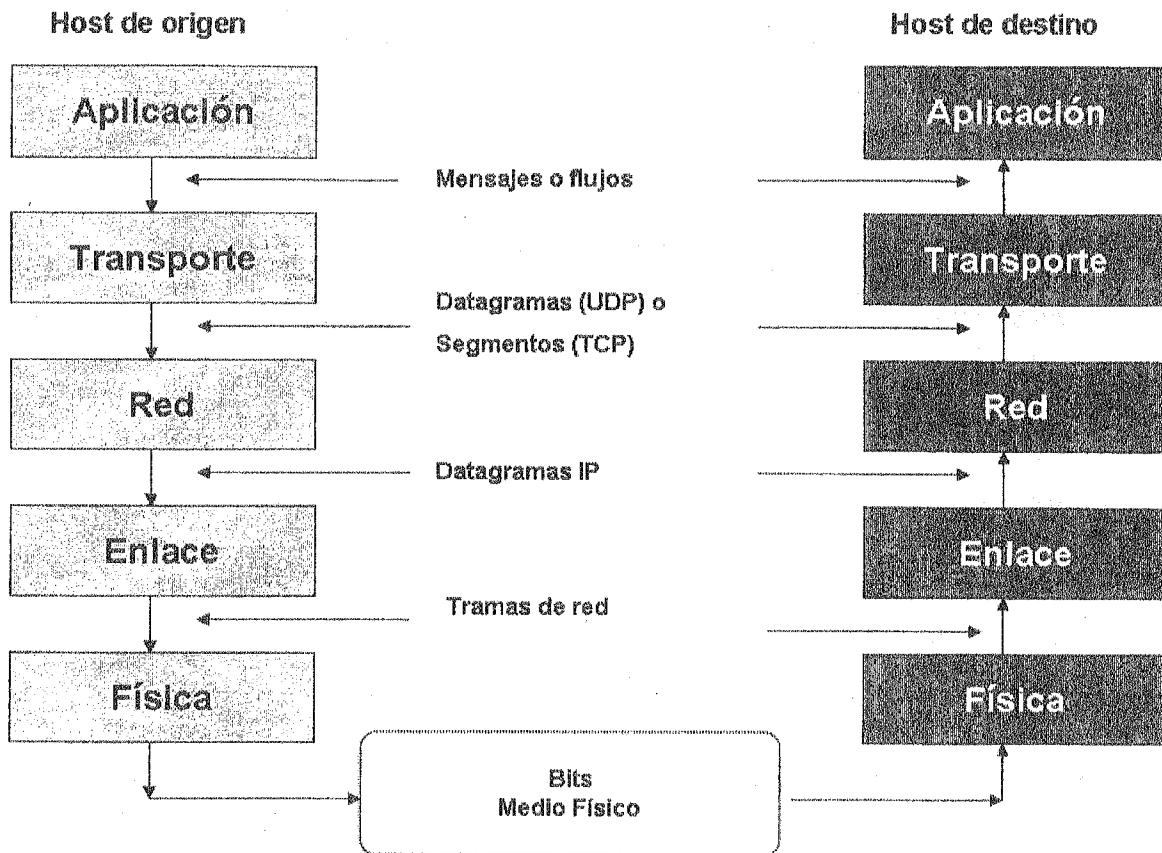


Fig. 3.3 La pila de capas del modelo TCP/IP

A diferencia del modelo OSI, las capas del modelo TCP/IP son cinco² (de arriba hacia abajo): La capa de Aplicación, la capa de Transporte, la capa de Red, la capa de Enlace y la capa Física. Otras referencias acerca del modelo dan otro nombre a la capa de Red (Internet) y a la capa de Enlace (Acceso a red o Interfaz de red), además que solo consideran las cuatro primeras capas. En los siguientes capítulos describiremos en detalle cada una de estas capas.

La capa de Aplicación del modelo TCP/IP tiene mayor número de funciones que su equivalente del modelo OSI, ya que cubre a las funciones de las capas de Aplicación, Presentación y Sesión de este modelo. La familia de protocolos TCP/IP está descrita en el RFC 2151. En la siguiente figura mostramos algunos según la capa a la que corresponden:

²

Se toma como referencia el libro de Kurose (1999)

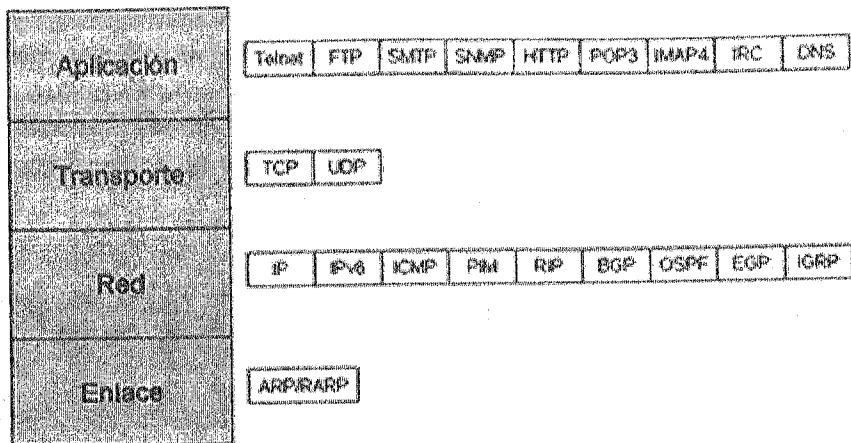


Fig. 3.4 Algunos protocolos TCP/IP

En los siguientes capítulos desarrollaremos los protocolos de las capas de este modelo.

3.6 MODELO JERÁRQUICO DE CISCO

Para el diseño, implementación y administración de las redes, como es el caso de la red de la UMSA, Cisco Systems ® propone un modelo Jerárquico de tres niveles o capas que son: el núcleo (backbone) principal de la red, la capa de Distribución y la capa de Acceso. Comprende el *backbone* o núcleo de la red hasta el equipo de usuario final. (McQuerry. 2001). Esta filosofía de Cisco le ha dado el éxito la venta de routers, switches, hubs, servidores y otros dispositivos de comunicación que integran esta arquitectura.

Para la descripción de este modelo, lo haremos de arriba hacia abajo, como lo hicimos con los otros modelos y utilizamos como referencia el libro de (McQuerry. 2001).

3.6.1 Capa del núcleo principal

Esta capa se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios globales o corporativos apropiados que solicita un usuario a través de la capa de distribución. En el caso de la red de la UMSA, un núcleo se encuentra en el Edificio Hoy de la Av. 6 de Agosto y el otro en el Monoblock. En este caso el transporte entre los núcleos y desde la capa inferior que es la capa de Distribución, se realiza a 1 Gigabit/seg.

3.6.2 Capa de Distribución

La capa de distribución de la red o de grupo de trabajo proporciona a los paquetes de información que envían los usuarios, accesibilidad a los servicios principales de la red. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa del núcleo principal. Realiza funciones tales como enrutamiento, filtrado y acceso a WAN. En un entorno de campus, como es el caso de la UMSA, se encarga de:

- Servir como punto de acumulación para acceder a los dispositivos de capa.
- Erutar el tráfico para proporcionar acceso a los departamentos, facultades o grupos de trabajo.

- Segmentar la red en múltiples dominios de difusión / multidifusión.
- Traducir los diálogos entre diferentes tipos de medios, como Token Ring y Ethernet.
- Proporcionar servicios de seguridad y filtrado.

3.6.3 Capa de Acceso

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Los usuarios, así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales. En la capa de acceso de la red de la UMSA se encuentran sus usuarios que constituyen las autoridades, los docentes, estudiantes, investigadores y personal administrativo que accede a la red y se conecta a los servidores a través de switches como el modelo 2950 y el 2960 de Cisco.

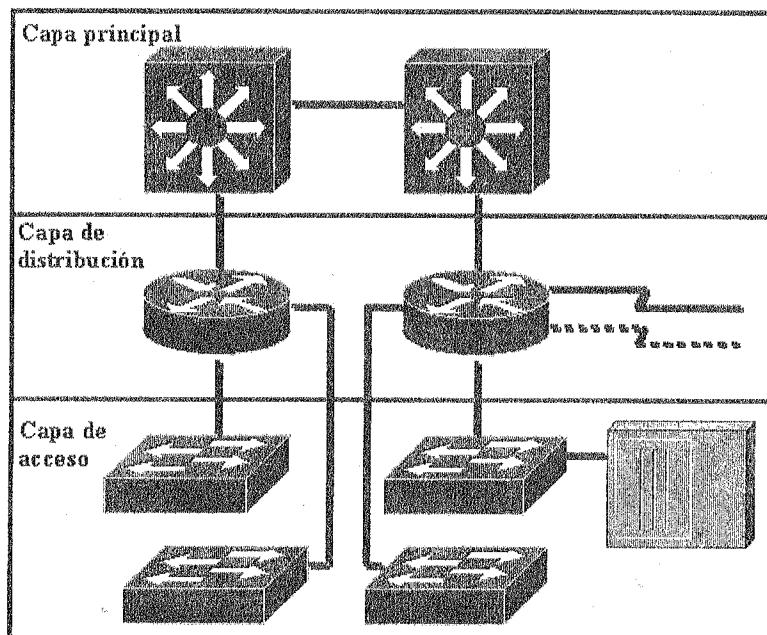


Fig. 3.5 Modelo Jerárquico de Cisco Systems ®

3.7 CONCEPTOS Y TERMINOS CLAVE

Encapsulamiento de datos

MAC

Modelo Cisco.

Capas del Modelo Cisco

Modelo OSI.

Capas del Modelo OSI

Modelo TCP/IP.

Capas del Modelo TCP/IP

Sistemas Abiertos

Sistemas Cerrados o Propietarios

3.8 PREGUNTAS DE REPASO

1. ¿Cuál de las siguientes respuestas no constituye una razón para que el modelo OSI sea un modelo de red dividido en capas?
 - A. Un modelo dividido en capas aumenta la complejidad.
 - B. Un modelo dividido en capas estandariza las interfaces.
 - C. Un modelo dividido en capas hace posible un esfuerzo de desarrollo especializado.
 - D. Un modelo dividido en capas impide que los cambios que se realizan en un área afecten a las otras

2. ¿Cuál de las capas del modelo OSI maneja la notificación de errores, la topología de red y el control de flujo?
 - A. La capa física
 - B. La capa de enlace de datos
 - C. La capa de transporte
 - D. La capa de red

3. ¿Cuál de las capas del modelo OSI establece, mantiene y administra las sesiones entre aplicaciones?
 - A. La capa de transporte
 - B. La capa de sesión
 - C. La capa de presentación
 - D. La capa de aplicación

4. ¿Cuál de las sgtes opciones describe más correctamente la función de la capa de presentación?
 - A. Suministra la representación de datos y el formateo de códigos.
 - B. Maneja la notificación de errores, la topología de red y el control de flujo.
 - C. Suministra servicios de red para las aplicaciones de usuario.
 - D. Suministra medios eléctricos, mecánicos, de procedimiento y funcionales para activar y mantener el enlace entre sistemas.

5. ¿Cuál de las capas del modelo OSI suministra servicios de red para aplicaciones de usuario?
 - A. La capa de transporte
 - B. La capa de sesión
 - C. La capa de presentación
 - D. La capa de aplicación

6. ¿Cuál de las siguientes opciones describe más correctamente los cinco pasos de conversión de la encapsulación de datos cuando un equipo envía un mensaje por correo electrónico a otro equipo?
- A. Datos, segmentos, paquetes, tramas, bits
 - B. Bits, tramas, paquetes, segmentos, datos
 - C. Paquetes, segmentos, datos, bits, tramas
 - D. Segmentos, paquetes, tramas, bits, datos
7. El Host A envía un mensaje por correo electrónico al Host B a través de una LAN. Para enviar este mensaje, los datos deben encapsularse. ¿Cuál de las siguientes opciones describe más correctamente el primer paso de la encapsulación de datos?
- A. Los caracteres alfanuméricos se convierten en datos.
 - B. El mensaje se divide en bloques que se pueden transportar con facilidad.
 - C. Se agrega un encabezado de red al mensaje (dirección fuente y dirección de destino).
 - D. El mensaje se convierte al formato binario.
8. El Host A envía un mensaje por correo electrónico al Host B a través de una LAN. Antes de enviar este mensaje, los datos deben encapsularse. ¿Cuál de las siguientes opciones describe más correctamente lo que sucede una vez que se ha creado un paquete?
- A. El paquete se transmite a través del medio.
 - B. El paquete se coloca en una trama.
 - C. El paquete se divide en tramas.
 - D. El paquete se convierte al formato binario.
9. El Host A envía un mensaje por correo electrónico al Host B a través de una LAN. Antes de poder enviar este mensaje, los datos deben encapsularse. ¿Cuál de las siguientes opciones describe más correctamente lo que sucede una vez que los caracteres alfanuméricos de un mensaje de correo electrónico se hayan convertido en datos?
- A. Los datos se convierten al formato binario.
 - B. Se agrega un encabezado de red a los datos.
 - C. Los datos se segmentan en bloques más pequeños.
 - D. Los datos se colocan en una trama.
10. ¿Cuál de las siguientes opciones describe más correctamente lo que es un datagrama?
- A. Un mensaje que se envía a la fuente para confirmar que los datos se han recibido sin daños
 - B. Una representación binaria de la información de enrutamiento
 - C. Un paquete de datos cuyo tamaño es inferior a 100 bytes
 - D. Un paquete de la capa de red.

11. En una arquitectura de red dividida en capas se estandariza las interfaces porque:
- A. Se facilita el intercambio de información de un fabricante a otro.
 - B. Las capas se encuentran una encima de la otra
 - C. Lo ha determinado así la organización ISO
 - D. Se mejora la conexión de una capa a la otra
12. En la arquitectura de red dividida en capas, porque una capa debiera crearse donde haya necesidad de un diferente nivel de abstracción en el manejo de datos.
- A. Para simplificar su aprendizaje
 - B. Reducir la complejidad de su diseño
 - C. Facilitar la técnica modular
 - D. Acelerar la evolución
13. Cual es el propósito de una capa en una arquitectura de red dividida en capas
- A. Facilitar la interface con los usuarios
 - B. Ofrecer servicios a las capas superiores
 - C. Transmisión de datos
 - D. Proporcionar seguridad a la red
14. Cual de las siguientes organizaciones fue la precursora de los Sistemas Abiertos
- A. La ISO
 - B. La CERT
 - C. La OSI
 - D. La IEEE
15. A que se refiere el término "Open System" en relación al tema
- A. Contrario a lo que determina la Microsoft
 - B. Una marca de red
 - C. Especificaciones de hardware
 - D. Especificaciones técnicas que se hacen públicas disponibles a todos.

3.9 TALLER

1. Discutir por qué el modelo de red dividido en capas, asegura la interoperatividad de la tecnología.
2. Supongamos que se desea "bajar" una página web que se encuentra en una universidad de EEUU.
 - a) Indicar cuales son los elementos involucrados de hardware y software
 - b) Indicar quienes son los actores involucrados
 - c) Describir todo el proceso de comunicación según el modelo OSI
 - d) Describir todo el proceso de comunicación según el modelo TCP/IP
3. Por qué se dice que tanto el modelo OSI como el TCP/IP son modelos que están basados en stacks
4. Realizar el sgte análisis para una red de datos dividida en capas según el modelo TCP/IP:
 - a) Que fluye por cada capa
 - b) Cuales son las diferentes formas del flujo
 - c) Que reglas rigen para el flujo
 - d) Donde se produce el flujo

CAPITULO 4 APPLICACIONES DE RED

Objetivos de Aprendizaje: *Al concluir el capítulo, usted será capaz de:*

- *Identificar las principales aplicaciones de red,*
- *Comprender los procesos, protocolos e interfaces*
- *Mostrar el funcionamiento de los protocolos más importantes a nivel de aplicación*

4.1 SERVICIOS DE LA CAPA DE APLICACIÓN

En nuestro análisis de la arquitectura de una red, primeramente nos hacemos la pregunta ¿Como utilizamos la red?, Este capítulo trata justamente de las aplicaciones o servicios que podemos tener con una red. Sin duda sobre la red pública Internet, se han desarrollado la mayor cantidad de aplicaciones, mostraremos las más importantes, sin embargo, hay aplicaciones que por razones de seguridad de su información corren sobre redes privadas.

En una aplicación de red, entran en juego varios componentes como ser: los procesos, los protocolos de Aplicación, los programas Agentes de Usuario y el modelo de referencia que utilizan los extremos de la red (Cliente/Servidor o Peer to Peer).

Un proceso es un programa que esta corriendo en un host. Más de un proceso puede correr en un solo host o en hosts diferentes. Cuando lo hacen en el mismo host, su comunicación está definida en el sistema operativo. Lo que nos va interesar, es la comunicación de los procesos distribuidos en hosts diferentes, que lo hacen con protocolos de aplicación.

Un proceso identifica al otro proceso con el que quiere comunicarse, mediante: la Dirección IP del host corriendo el otro proceso y el número de puerto que permite al host receptor determinar cual proceso debe recibir el mensaje.

Los protocolos definen el formato y el orden de los mensajes que se intercambian entre los procesos que corren en los extremos de la red, así como las acciones y reglas que se toman en cuenta cuando se transmite o recibe un mensaje. Usa servicios provistos por protocolos de niveles inferiores.

Un programa Agente de usuario es una interface entre el usuario y la aplicación de red, es decir, es aquel programa que permite acceder a la aplicación. Por ejemplo en la aplicación

web, este programa se denomina Navegador de Web o Browser como el Internet Explorer o el Firefox, en el correo electrónico, es el lector de correo.

Las aplicaciones de red que desarrollaremos en detalle son: Web, correo electrónico y DNS (Servidor de Dominio de Nombres). Los protocolos de estas aplicaciones son de dominio público y están documentados en RFCs (Request for Comments).

4.2 APPLICACIÓN WEB

La Web, World Wide Web o simplemente www es un sistema de documentos de hipertexto y/o hipermedios enlazados y accesibles como lo diseñó su creador Tim-Berners Lee en 1992 “*..a través de cualquier navegador*”.¹

Según (Forouzan, 2007), la Web es un servicio distribuido de tipo Cliente/Servidor que tiene una única combinación de flexibilidad, portabilidad y características amigables para el usuario que la distinguen de otros servicios ofrecidos por Internet.

Este servicio está distribuido sobre muchas localizaciones o sitios web como se muestra en la figura comunicación Cliente/servidor. *Un sitio web* es la localización en internet de empresas, instituciones educativas, de gobierno y otras que tienen al menos una página base HTML y muchos objetos referenciados a través de enlaces.

Las páginas web están formadas por objetos (textos, imágenes, sonidos, etc), construidas por el lenguaje en base a marcas HTML (HyperText Markup Language) y localizadas por un identificador denominado URL (Uniform Resource Locator) que la dirección de la página web en la Internet.

HTML tiene un conjunto de marcas que pueden ser intrepretadas por todos los navegadores y los servidores web. Estas marcas o “tags” describen los elementos básicos de un documento web, tales como: encabezados, párrafos, estilos de texto y listas. Hay otras marcas más sofisticadas que crean tablas e incluyen elementos interactivos tales como formularios, scripts o Java applets.²

El lenguaje XML o Lenguaje de Marcas Extensible, describe una clase de objetos llamados documentos XML que son almacenados en computadoras y parcialmente describe el comportamiento de los programas que procesan estos objetos.

¹ Tim-Berners Lee (1992)

² Programa en Java que se inicia desde dentro de la página web que puede estar autorizado para acceder a recursos locales como el sistema de archivos

La búsqueda de extensión de la funcionalidad del lado del cliente, ha llevado al desarrollo de tecnologías capaces de soportar dinamismo en el contenido de un documento que solicita el navegador. Este tipo de documentos se denominan Dinámicos porque su contenido cambia de una solicitud a otra que realiza el navegador. Un ejemplo es obtener la fecha y hora del servidor. Por supuesto que la generación de este tipo de documentos es a través de la ejecución de funciones. Hay varias tecnologías para crear documentos dinámicos como: CGI, APIs, Servlets, SSI (Server Side Include), JSP (Java Server Page).

Los documentos Activos son programas que se ejecutan en el lado del cliente. Cuando un navegador solicita un documento activo, el servidor envía una copia del documento o un script³. El documento se ejecuta a continuación en el navegador.

4.2.1 Comunicación Cliente/Servidor Web

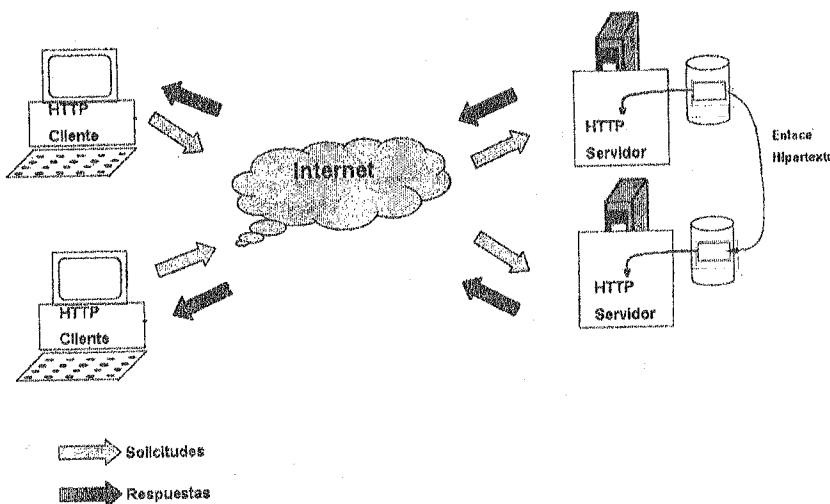


Fig. 4.2 Comunicación Cliente/Servidor

Bajo el modelo Cliente/Servidor, el cliente web envía su solicitud consistente en un mensaje que describe la operación a realizarse (método).

Como se muestra en la figura, uno o más clientes HTTP envían sus solicitudes a un servidor HTTP, utilizando un navegador, el cual puede derivar la solicitud a otro servidor mediante un enlace hipertexto.

La línea de inicio de una solicitud tiene el siguiente formato:

³ Pedazo de código

METODO	URL	VERSION	<CR><LF>
--------	-----	---------	----------

Donde:

METODO es la operación a realizar como GET, HEAD, POST,

PUT, DELETE, LINK, UNLINK TRACE

URL es la dirección de la búsqueda

VERSION se refiere a la versión de HTTP (HTTP1.0 HTTP1.1)

<CR><LF>comandos de salto de carro y alimentación de línea
respectivamente.

METODO	DESCRIPCION
GET	Recupera la información identificada por la dirección URL. Si ésta se refiere a un proceso que produce datos, en la respuesta retorna la entidad
HEAD	Idéntico a GET, excepto que el servidor no devuelve el documento HTML en la respuesta. Este método es utilizado para probar la validez de enlaces hipertexto, accesibilidad y modificación reciente.
POST	Es usado para solicitar que el servidor destino acepte la entidad enviada en la solicitud y se añadan datos a la URL.
PUT	Solicita que la entidad sea almacenada en la dirección URL
DELETE	Solicita que el servidor origen borre la URL indicada.
LINK	Establece uno o más enlaces entre recursos existentes identificados por URL
UNLINK	Elimina uno o más enlaces de recursos existentes identificados por el URL
TRACE	Permite al cliente ver que información está recibiendo el otro extremo de la cadena de solicitud y usar aquella información para testear o diagnosticar.

Tabla 4.1. Métodos del protocolo HTTP

Ejemplo 4.1

Recuperar el archivo logo.jpg del host www.mi_sitio.bo y mostrar la respuesta del servidor

Solución

Utilizamos el método GET de la siguiente forma:

GET /Imagen/logo.jpg HTTP/1.1

Host: www.mi_sitio.bo

El servidor devuelve códigos de estado en la primera linea en el mensaje de respuesta al cliente. La respuesta del servidor a la anterior solicitud de GET es:

HTTP/1.1 200 OK

Server: Microsoft-IIS/5.0

Date: Wed, 08 Mar 2008 22:41:19 GMT

Server: Apache/1.3.0 (Unix)

Last-Modified: Mon, 04 Mar 2008

Content-Length: 6821

Content-Type: text/html

< documento HTML >

La primera línea de la respuesta contiene a la versión de HTTP seguido del código 200 que significa solicitud exitosa. Las siguientes son campos de cabecera y al final el documento HTML solicitado.

Otros códigos de estado en la primera línea de respuesta pueden indicar que:

CODIGO	EXPLICACION
200	Solicitud exitosa, el objeto solicitado esta después en el mensaje
404	el objeto solicitado no se encuentra en el servidor
403	No está permitido el acceso
301	El objeto ha sido movido a una nueva ubicación especificada mas adelante en el mensaje
400	El mensaje de solicitud no se entiende en el servidor

Tabla 4.2 Algunos códigos de respuesta del servidor HTTP

Y otras respuestas que están descritas en RFC 1945 para la versión 1.0 y en el RFC 2068 para la versión 1.1 de HTTP.

Algunas diferencias entre ambas versiones de HTTP se muestran en la siguiente tabla:

HTTP/1.0	HTTP/1.1
conexiones No persistentes	Conexiones Persistentes
El servidor entiende la solicitud, responde y cierra la conexión TCP	En la misma Conexión TCP el servidor interpreta la solicitud, responde y interpreta una nueva solicitud
2 RTTs ⁴ para traer cada objeto. Cada transferencia de objeto sufre de un comienzo lento	Menos RTTs y menos comienzos lentos
Métodos: GET, HEAD, POST, PUT, DELETE, LINK, UNLINK	Métodos: GET, HEAD, POST, PUT, DELETE, LINK, UNLINK TRACE

Tabla 4.3 Comparación de HTTP/1.0 y HTTP/1.1

⁴ Round Trip Time. Tiempo que tarda un paquete enviado desde un emisor en volver a este mismo emisor habiendo pasado por el receptor de destino.

4.2.3 Caché de Web.

Esta es una comunicación intermedia entre el Cliente y el servidor http, llamado también Servidor Proxy que se utiliza para satisfacer la demanda del cliente y reducir el tráfico a servidores distantes. Está situado en la misma red del cliente y guarda copias de los objetos solicitados, de manera que para la próxima solicitud de ese objeto, ya no será necesario que se recupere del servidor remoto, sino de este proxy. El usuario deberá configurar el navegador para acceder vía un cache de web. El cliente envia todos los pedidos de http al cache Web. Si un objeto esta en el cache de web inmediatamente devuelve el objeto en respuesta a la solicitud, sino solicita el objeto del servidor de origen devuelve la respuesta http al cliente.

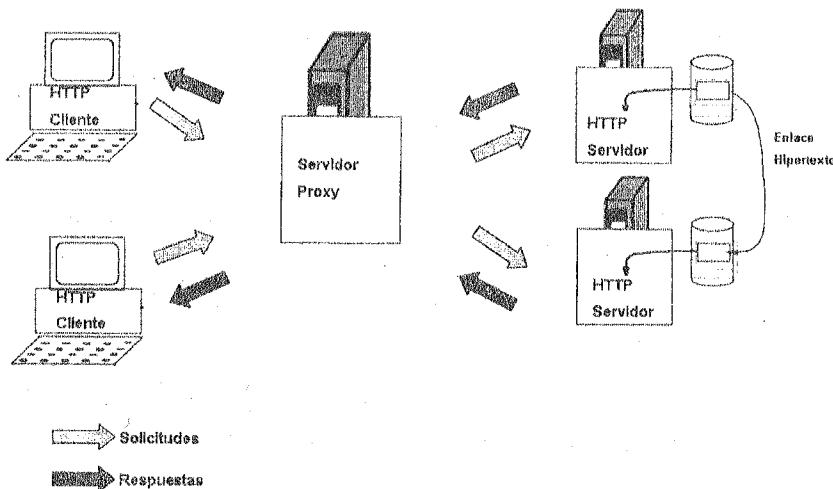


Fig. 4.3 Caché de Web

4.3 APLICACIÓN CORREO ELECTRÓNICO

El correo Electrónico ha sido y es una de las aplicaciones más populares de los usuarios de Internet y de los sistemas intranet. Se inicia como una herramienta para las comunicaciones internas de una organización (Zacker, 1999). Su función y componentes son análogos al correo tradicional, ser un medio de comunicación para el envío y recepción de documentos, con o sin certificación.

En una carta electrónica hay un remitente, un destinatario con su dirección, copias a otras personas. Pero además de estas analogías, este sistema tiene muchas mas funcionalidades, como el reenvío a otros usuarios, envío de archivos adjuntos, o que su recepción, sin importar la distancia, se puede producir en tan solo instantes.

Los mensajes en cualquier idioma, los archivos de imágenes, sonido o video adjuntos en los mensajes, son posible gracias a una ampliación o extensión del formato de los mensajes que se denomina MIME (Multipurpose Internet Mail Extensions RFC 2045, 2056).

Las funciones del correo electrónico son:

- Guardar la correspondencia del usuario en un cajón postal electrónico o *mailbox*.
- Notificar cuando llega una nueva correspondencia
- Responder sin necesidad de registrar nuevamente la dirección del destinatario.
- Adjuntar archivos de texto, hojas electrónicas, bases de datos, imágenes, sonido a los mensajes.
- Autentificar al usuario antes que pueda leer su correspondencia.
- Realizar el mantenimiento de un directorio de correos

4.3.1 COMPONENTES DEL CORREO ELECTRÓNICO

Los componentes de esta aplicación de red son: el agente de usuario, el servidor de correo y protocolos de comunicación para el envío o transferencia de mensajes y recepción o acceso como el SMTP (Simple Mail Transfer protocol) y el POP3 (Post Office Protocol) respectivamente.

El agente de usuario, es el lector de correo, el encargado de componer y editar mensajes. Es decir, es el programa interface del usuario con la aplicación. Mencionamos al programa Outlook de la Microsoft o el Thunderbird de Mozilla.

El host servidor de correo, va a almacenar los mensajes entrantes (mailbox) y la cola de mensajes salientes. Además interactúa con el protocolo SMTP, pues corre el lado del cliente SMTP para enviar correo y también con el lado del servidor SMTP para recibir correo.

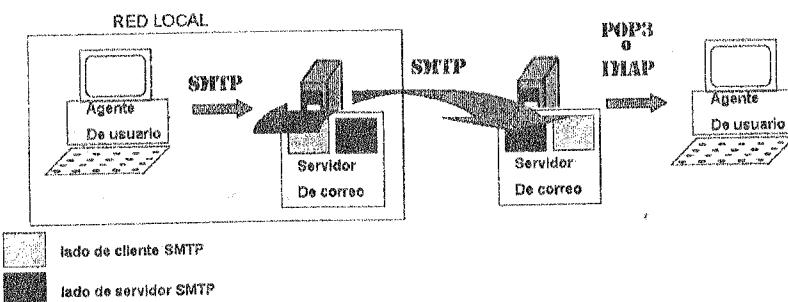


Fig. 4.4 Sistema de Correo Electrónico

4.3.2 Protocolo de envío de mensajes SMTP

El Protocolo Sencillo de transferencia de correo electrónico, SMTP es un protocolo eficaz en formato ASCII de 7 bits. Trabaja con otros programas de correo para enviar y recibir mensajes electrónicos. Utiliza un servicio confiable de transporte de mensajes como es el TCP (Ver RFC 2821).

Como la mayoría de los protocolos de la capa de Aplicación, tiene dos lados: el lado del cliente que se ejecuta sobre el servidor de correo que envía el mensaje y el lado del servidor que se ejecuta sobre el servidor de correo receptor. Ambos, el lado del cliente y el lado del servidor de SMTP corren sobre cada host servidor de correo. Cuando un servidor de correo envía un mensaje, actúa como cliente SMTP, cuando lo recibe, actúa como servidor SMTP.

El cliente SMTP envía comandos en formato de caracteres ASCII y el servidor SMTP devuelve códigos de estado y frases. Algunos comandos y códigos son los siguientes:

COMANDO / CODIGO DE RESPUESTA	DESCRIPCION
HELO 250 (éxito) 550 (falla)	Identifica al que envía el correo. Ejemplo: C: Helo <SP>umsanet.edu.bo<CRLF> S: 250 OK
MAIL FROM 250 (éxito) 550 (falla)	Quién envía el correo. Ejemplo: C: MAIL FROM: <u>juan@gmail.com</u> S: 550 Failure
RCPT TO:	Identifica un destinatario del correo. Ejemplo: C: RCPT TO: <u>docente@umsa.bo</u> S: 250 OK
DATA 354	Le indica al servidor que lo que sigue es el texto del mensaje. C: DATA S: 354 Start mail input; end with <CRLF>.<CRLF> C: bla..bla.... S: <CRLF>.<CRLF>
QUIT	Cierre de la sesión

Tabla 4.4. Comando y códigos de estado del protocolo SMTP

Con el fin de producir de una manera consistente y manejable por la cual los clientes y servidores SMTP puedan ser identificados y los servidores SMTP señalar las extensiones soportadas a los clientes conectados, se ha definido la extensión ESMTP (RFC 1869).

4.3.3 Protocolos de recepción o acceso de correo

a) El protocolo POP3 (Post Office Protocol, RFC 1939)

Es un protocolo simple de acceso al correo (Ver figura del sistema de correo electrónico) que le ofrece al usuario descargar en su computadora los mensajes del servidor de correo de su predilección (p.e. Gmail, Hotmail), a través de los respectivos programas cliente o agentes de usuario asociados a cada servidor de correo.

El software Cliente de POP3, se instala en el Agente de Usuario; el servidor POP3 se instala en el servidor de correo. El acceso al correo se inicia en el cliente cuando el usuario necesita descargarlo del buzón situado en el servidor de correo. El cliente abre una conexión TCP con el servidor en el puerto 110. Una vez establecida la conexión, se ejecuta el protocolo POP3 en tres fases: autorización, transacción y actualización. Durante la primera fase, el servidor solicita la autentificación del usuario receptor de correo (le pide el nombre de usuario y la contraseña), luego en la fase de transacción el Agente de usuario recupera su correo, elabora estadísticas, marca aquellos que serán borrados, los lista y elimina los mensajes marcados. La fase de actualización se produce cuando el cliente envía el comando QUIT para el cierre de sesión y conexión.

El protocolo POP3 interactúa con el host del usuario (Cliente) que solicita el servicio y el host (Servidor) donde se reciben los correos a través de un intercambio de comandos y códigos de respuesta. Los comandos más importantes son:

COMANDO	DESCRIPCION
USER	Identificación del usuario
PASS	Contraseña del usuario
STAT	Estadísticas de los mensajes
RETR	Retira los mensajes del buzón
DELE	Marca mensaje para borrado
QUIT	Cierra la conexión

Tabla 4.5. Comandos POP3

En la fase de transacción, solo se consideran dos posibles respuestas del Servidor:

- OK. Que significa la aceptación
- ERR. Que es indicación de Error

Además contiene un texto descriptivo cuando se trata de un error.

b) El protocolo IMAP (Internet Message Access Protocol, RFC 1730)

Es un protocolo que permite al usuario descargar los mensajes del servidor de correo a su máquina para que se pueda acceder a su correo, fuera de línea con un programa cliente como Outlook.

Con IMAP, los mensajes siempre son retenidos en el servidor. El cliente puede usar comandos para bajarlos o borrarlos, el servidor siempre mantiene el buzón de correo.

A diferencia de POP, el protocolo IMAP ofrece comunicación bidireccional entre la web del servidor de correo de su predilección y su programa cliente. IMAP proporciona un mejor método para acceder a su correo desde múltiples dispositivos (celular, PDA, computadora de escritorio). IMAP garantiza que los nuevos mensajes sean igualmente accesibles en cualquier momento dado.

c) Webmail o los correos basados en web

Son servicios de correo electrónico a los que se accede vía navegador web, como por ejemplo: Gmail, Hotmail o Yahoo Mail. La mayor ventaja de este servicio, es que el usuario tiene la posibilidad de acceder a su buzón de correos desde cualquier computador conectado al Internet,

El webmail suele estar basado en lenguaje HTML. Los mensajes y los archivos adjuntos quedan almacenados en el servidor del/de la proveedor/a de correo, pudiendo accederse a ellos desde cualquier lugar remoto sin necesidad de descargarlos en ninguna máquina local. Para usar webmail es necesario que el navegador tenga habilitada la aceptación del JavaScripts y Cookies.

Sin embargo, el webmail tiene problemas de seguridad⁵ porque permite a los usuarios eludir el protector de virus de una institución, por lo que está siendo prohibido su uso.

4.4 APLICACIÓN DNS

La identificación de los host de una red conectada a Internet por un conjunto de números o direcciones hosts, sería un problema para muchos usuarios al momento de recordarlos y nada práctico para añadir otros host a la red. Sin embargo, la gestión de nombres en las capas inferiores, como la capa de Red, no sería eficiente por la poca información que tienen para ubicarla en la red.

Por otra parte, una base de datos centralizada con la identificación de todos los host de la red Internet, sería imposible, por el gran volumen de tráfico, bases de datos distantes, difícil mantenimiento y ninguna posibilidad de escalabilidad.

⁵ Revista E-Security Communications. Volume 3, Issue 2, Fall 2006
<http://www.esecurity.ch/communications.html>

La aplicación DNS (Domain Name Server, RFC 1034) tiene como propósito resolver estos problemas de identificación de redes y de los host que tienen estas redes.

DNS es una aplicación Cliente/Servidor que tiene un espacio de nombres(dominiós) para recuperar direcciones de hosts y almacenarlos en registros de una base de datos distribuida conjuntamente el nombre asociado a una dirección de host.

Tiene tres componentes: Dominios y los datos asociados con los nombres o registros, Clientes que hacen las consultas a los servidores y éstos que hacen disponible el dominio.

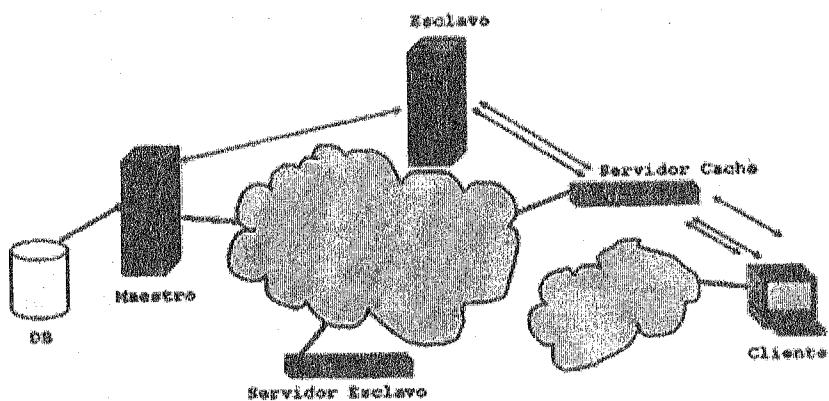


Fig. 4.5 Sistema de DNS

El Dominio o nombre de Dominio es una especificación para un espacio de nombres organizados jerárquicamente. Los objetos que se encuentren en la red, se nombrarán de esta forma jerárquica:

- localidad (país, organizaciones, empresas, etc)
 - unidad dentro de la localidad (empresa X)
 - objeto dentro de una unidad (el nombre de una persona que trabaja en la empresa X)

Los clientes DNS, son programas de usuario que extraen información de los servidores DNS, por ejemplo solicitando la dirección de red de un determinado sitio o viceversa, dada una dirección de red, averiguar el nombre del sitio.

Los servidores DNS contienen información de la estructura jerárquica del espacio de nombres, un servidor DNS en particular tiene una completa información de un subconjunto espacio de dominio y punteros a otros servidores, que servirán para llevar la información a cualquier parte del árbol de dominio.

Como observamos en la figura 4.5 en un sistema de DNS hay varios tipos de servidores de nombres:

- Autorizados
- Maestro
- Esclavo
- Servidor Cache
- Mixtos

Los servidores Autorizados conocen las partes del árbol de dominio por donde ellos tienen una completa información. La información autorizada está organizada en unidades denominadas Zonas, y estas zonas pueden ser distribuidas automáticamente a los servidores DNS que proveen servicio de redundancia para los datos en la zona.

El servidor Maestro contiene una copia de la base de datos, con atributos de lectura/escritura. El Esclavo es un servidor secundario que interactúa con el servidor Maestro. El servidor Caché es recursivo a las solicitudes del cliente. Para modificar cualquier registro de la base de datos DNS, el administrador accede al servidor Maestro o primario.

Los registros de recursos (RR) almacenan información asociada con un nombre en particular. Su formato es el siguiente:

RR: (name, value, type, ttl)

Tipo	Descripción
Type = A	<i>name</i> es hostname <i>value</i> es dirección IP
Type = NS	<i>name</i> es dominio (e.j. umsa.bo) <i>valor</i> es dirección IP del servidor DNS Autorizado para este dominio
Type = CNAME	<i>name</i> es un alias para algún nombre real <i>value</i> es el nombre real
Type = MX	<i>value</i> es hostname del servidor de correos asociado al nombre

Tabla 4.6 Registro DNS

Los tipos de registro más comunes son:

SOA	Inicio de zona
A	Dirección de host
MX	Correo
CNAME	Alias
NS	Servidor DNS

El administrador del servidor DNS tiene que registrar los nombres de los hosts y de las direcciones IP en la base de datos que el servidor DNS utiliza para resolver consultas.

Por ejemplo, el administrador del servidor DNS de umsanet.edu.bo registró que www.umsanet.edu.bo tiene como IP 166.114.17.11. en una DB.

Algun servidor DNS que busque resolver umsanet.edu.bo, consultará al servidor DNS de umsanet.edu.bo por la dirección IP de www.umsanet.edu.bo

A continuación mostramos un ejemplo de resolución para encontrar un sitio

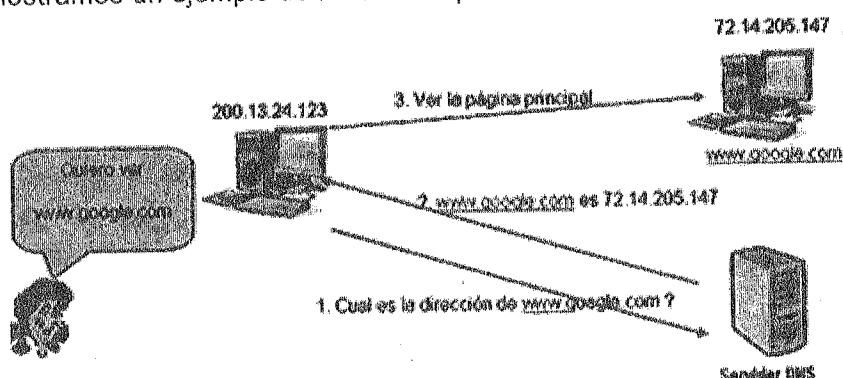


Fig. 4.6 Proceso de Resolución

El cliente consulta con el servidor DNS, éste le responde con la dirección IP del sitio, luego se despliega en la máquina del usuario la página principal del sitio solicitado.

4.5 OTRAS APLICACIONES DE LA RED INTERNET

4.5.1 Transferencia de archivos

Esta aplicación que surge en una red local, es considerada una aplicación popular del Internet. Consiste en copiar información almacenada en un servidor remoto al que el usuario accede previa autentificación. También el usuario puede transferir sus archivos locales al servidor remoto.

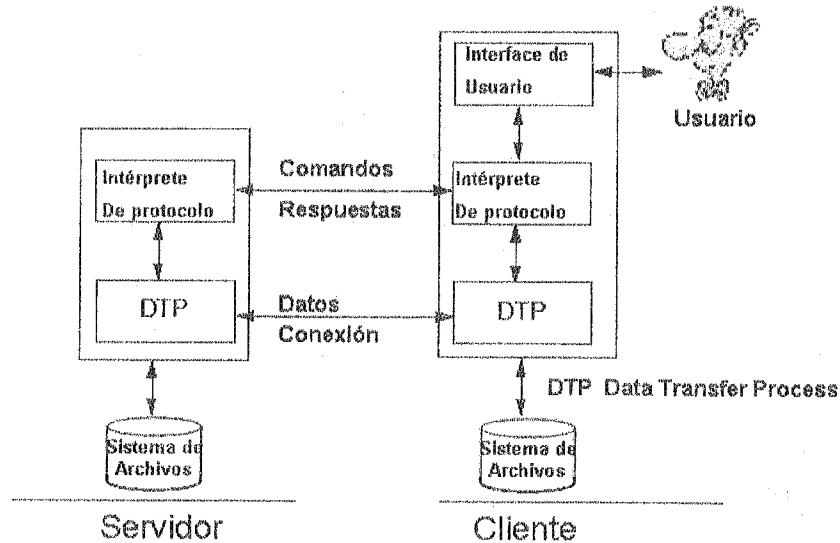


Fig. 4.7 Protocolo FTP

El Protocolo File Transfer protocol (FTP, RFC 959), es uno de los estándares de la familia TCP/IP. El modelo de funcionamiento de este protocolo, está basado en los siguientes aspectos:

- Modelo cliente/servidor. El cliente envía comandos y el servidor devuelve códigos de respuesta.
- Establece dos conexiones entre los extremos. Una conexión se utiliza para la transferencia de datos (puerta 20), la otra para enviar información de control (comandos y respuestas) (puerta 21).
- La conexión de control permanece abierta durante toda la sesión FTP interactiva, mientras que la de datos se abre y se cierra para cada archivo a transferir.
- Ambos extremos del enlace están construidos con un intérprete de protocolo y un proceso de transferencia de datos.
- El intérprete de protocolo tiene que comunicar cualquier comando de control al sistema remoto. En el otro extremo, el intérprete de protocolo, además responde al protocolo TELNET para iniciar la conexión de datos.
- La administración de datos es realizada por la unidad de proceso de transferencia de datos o DTP durante la transferencia de archivos.
- Luego que se completa la solicitud del usuario, el intérprete de protocolo del lado del servidor, cierra la conexión de datos.

El usuario de FTP realiza las siguientes operaciones:

- Conexión al host remoto
- Elección del directorio
- Lista de archivos disponibles para su transferencia
- Definición del modo de transferencia
- Copiar archivos del o al host remoto
- Desconexión del host remoto

Algunos comandos en formato de texto ASCII que realizan estas operaciones, son:

OPEN	Selecciona el host remoto e inicia una sesión
USER	Identifica al ID del usuario remoto
PASS	Autentifica al usuario
SITE	Envía información al host foráneo que provee el servicio específico a aquel host.
CD	Cambia de directorio
DIR o ls	Despliegue de los archivos disponibles
GET	Copia un archivo del host remoto al host local
PUT	Copia un archivo del host local al host remoto
QUIT o BYE	Desconecta del host remoto y termina FTP
CLOSE	Desconecta del host remoto pero deja el cliente FTP corriendo. Se puede usar el comando OPEN para trabajar con un nuevo host.

Tabla 4.7 Comandos FTP

Las respuestas a los comandos enviados son códigos de estado. Algunos de estos códigos y con su explicación (traducida) respectiva son:

331 Nombre de usuario OK, se requiere contraseña

125 la conexión de datos ya está abierta; se inicia la transferencia

425 No puede abrirse la conexión

452 Error al grabar archivo

Muchos sitios implementan el servicio de FTP anónimo, que significa que aquellos sitios permiten el acceso público a algunos directorios de archivos.

Si un servidor posee el servicio 'FTP anonymous', el usuario remoto coloca en el nombre de usuario la palabra "anonymous". No se necesita ninguna contraseña preestablecida, normalmente se suele utilizar la dirección de correo electrónico propia.

Una versión básica de FTP, es el protocolo TFTP (Trivial File Transfer Protocol) o Protocolo de Transferencia de Archivos Trivial que a diferencia del FTP utiliza el servicio de transporte del protocolo UDP con puerto 69. Se utiliza para transferir pequeños archivos.

4.5.2 E-Aplicaciones

Alrededor de 1995, se adoptó el uso del prefijo mágico "e-" a aplicaciones relacionadas al apogeo de la industria de la Internet que invierte cientos de millones de dólares. Algunas de éstas son E-Learning, E-Commerce, E-Business, E-Government, para referirse respectivamente a entrenamiento, comercio, negocios y gobierno basado en Internet.

El E-Learning, se refiere al uso de la tecnología para llevar a cabo programas de enseñanza. En el presente libro, se ofrecen al final de cada capítulo, demos de aprendizaje, utilizando herramientas de E-Learning.

E-Commerce incluye la compra y venta de productos en línea con dinero digital y vía intercambio electrónico de datos.

E-Business es una contracción de negocio electrónico o "electronic business". Se refiere a la puesta en marcha un negocio de forma electrónica. Incluye la compra y venta de bienes y servicios de forma electrónica, el trato con clientes en línea y otros negocios vía Internet.

E-Government se refiere a llevar a cabo la administración de un gobierno municipal o nacional utilizando medios tecnológicos como una forma de llegar a la población a través de la difusión de información pública vía Internet y los otros medios mencionados.

Finalmente, las aplicaciones basadas en Internet, no se acaban, hay investigaciones, productos comerciales o cursos de postgrado que tienen el interés de desarrollar, explotar y llegar a todos los usuarios que tienen un punto de acceso a Internet. El último capítulo del libro está dedicado a otra aplicación, Voz sobre redes IP o VoIP.

4.6 CONCEPTOS Y TERMINOS CLAVE

Administrador de servidor
Agente de Usuario
Caché de Web
Cliente DNS
Cookie
DNS
Dominio
E-Business
E-Commerce
E-Goverment
E-Learning
FTP
HTML
HTTP
IMAP
POP3
Proceso
Protocolo de correo
Registro de recursos
Resolución
Servicios de la capa de Aplicación
Servidor de Correo
Servidor DNS
SMTP
Transferencia de Archivos
URL
Web

4.7 PREGUNTAS DE REPASO

1. Cuales son los componentes principales de la aplicación Correo Electrónico
 - A. Encabezado, referencia, cuerpo
 - B. Agente de Usuario, Servidor de Correo, Protocolo de transferencia
 - C. Navegador, Servidor de Correo, Protocolo de transferencia
 - D. Usuario, Servidor de Correo, Protocolo de transferencia

2. Para qué utiliza el Caché una aplicación Web
 - A. Almacenar páginas repetidas evitando ir al servidor web
 - B. Ampliar la memoria del servidor web
 - C. Ampliar la memoria del cliente web
 - D. Garantizar el ancho de banda

3. Una función del servidor DNS es:
 - A. Asignar un número IP a una máquina
 - B. Asignar un nombre de máquina a un número IP
 - C. Traducir los nombres de dominio a su número IP correspondiente
 - D. Almacenar números IP

4. Un proceso se define como el:
 - A. algoritmo de enrutamiento
 - B. programa que corre en los routers
 - C. programa que esta corriendo en un host
 - D. Programa que corre solo en los servidores

5. Como se identifica un proceso:
 - A. Dirección IP del host y el número de puerto
 - B. Dirección MAC del host y número de puerto
 - C. Dirección IP del host
 - D. Número del puerto

6. A que se refiere un programa Agente de Usuario
 - A. interface entre el usuario y la aplicación de red
 - B. aquel programa que permite acceder a los datos del usuario
 - C. Interface entre el usuario y el núcleo de la red
 - D. A y B

7. Un ejemplo de Agente de usuario es:

- A. Chat
- B. Firefox Mozilla
- C. La PC conectada a Internet
- D. El Correo Electrónico

8. El modelo en el que se basa una aplicación web es:

- A. ISO
- B. Top Down
- C. Cliente/Servidor
- D. Peer to Peer

9. Los componentes de una aplicación web son:

- A. El protocolo HTTP, el navegador Web y el servidor HTTP
- B. El protocolo XML, el navegador Web y el servidor http
- C. El protocolo http, el navegador Web y el cliente http
- D. El protocolo http y el servidor http

10. El protocolo http permite:

- A. Realizar la interface con el usuario
- B. Desplegar objetos una vez que se instale en el cliente
- C. Buscar y recuperar páginas web.
- D. Controlar el flujo de páginas web

11. Que tipo de documentos se visualiza con un navegador

- A. Archivos de Texto
- B. Archivos de sonido
- C. Archivos de imágenes
- D. todos los anteriores

12. Los componentes de un navegador son:

- A. Un protocolo cliente, caché y controlador
- B. un controlador, caché, un protocolo cliente e intérpretes
- C. El servidor web y el protocolo http
- D. El intérprete, las páginas web

13. Que protocolo se puede usar en un navegador

- A. http
- B. FTP
- C. SSL
- D. Todos los anteriores

14. Indicar un intérprete que maneja un navegador

- A. Java Script
- B. HTML
- C. XML
- D. PDF

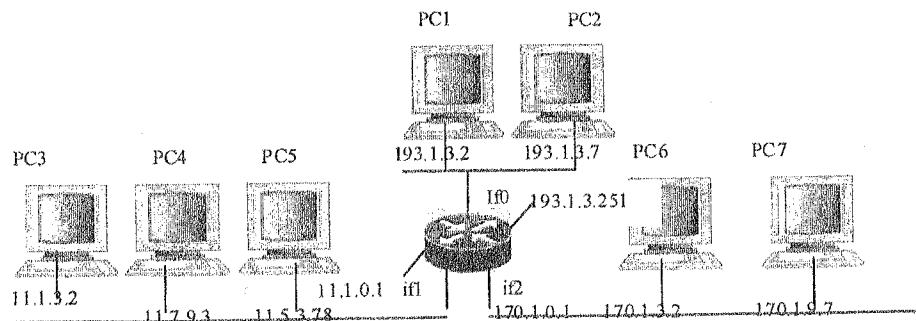
15. Los fragmentos de información que se almacena en el disco duro del cliente a través de su navegador se denomina

- A. Paquete
- B. slots
- C. Cookie
- D. Bytes

4.8 TALLER

Leer los artículo ipj2-3.pdf (Web Caching) y ipj3-2.pdf (Overview of Internet Mail Standards) de la revista The Internet Protocol Journal (<http://www.cisco.com>)

1. Dar 3 ejemplos de aplicaciones Cliente/Servidor que no se vieron en clases y Discutir si son sensibles a la pérdida de datos y al tiempo.
2. Que ocurre si el web cache no tiene una copia local de una URL.
3. Cual es la medida de la proporción de solicitudes individuales http que pueden ser enviados por el cache independientemente del tamaño de la página.
4. Cual es el beneficio económico de una Cache. A quienes beneficia, cuales son las variables que se deberán considerar.
5. Sea la red



Si PC1 es el servidor de páginas web y PC2 es el servidor DNS. Elaborar el registro DNS.

CAPITULO 5 LA CAPA DE TRANSPORTE

Objetivos de Aprendizaje: *Al concluir el capítulo, usted será capaz de:*

- *Comprender los principios y servicios de la capa de Transporte,*
- *Describir los protocolos de transporte TCP y UDP*
- *Analizar una técnica de detección de errores a nivel de Transporte*

5.1 EL SERVICIO DE TRANSPORTE

El objetivo de la capa de Transporte es trasladar los datos a y desde una aplicación de red. Es decir, brinda una comunicación lógica de extremo a extremo entre procesos de aplicación que corren sobre diferentes hosts. Según el modelo de referencia TCP/IP se encuentra por debajo de la capa de Aplicación, es a esta capa que presta sus servicios. Los servicios de la capa de Transporte pueden ser orientados a la conexión o sin conexión.

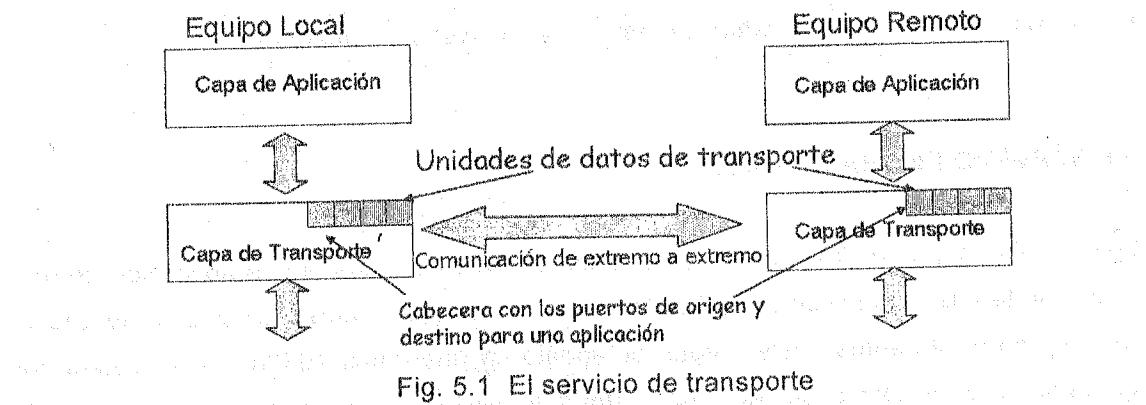
Servicios orientados a la Conexión. Se establece primero una conexión entre emisor y receptor. Garantizan que los mensajes enviados sean recibidos por el otro extremo. Es decir, hay una fiabilidad en la transmisión, si por alguna causa se produce un error o se pierde el mensaje, éste se retransmite. Un ejemplo de protocolo de transporte que utiliza este servicio es el TCP. Algunas aplicaciones como la transferencia de archivos requieren este tipo de servicio. Al final de la transferencia, se libera la conexión.

Servicios sin conexión, los paquetes son enviados de un extremo al otro, sin necesidad de establecer o liberar una conexión. Los paquetes no están numerados, pueden retrasarse, perderse o llegar fuera de orden.

En este servicio, no se interrumpe la comunicación, el término “sin conexión”, se refiere a un tipo de servicio no fiable, que no garantiza la transmisión, pero que tiene la ventaja de ser más rápidos. El protocolo de transporte UDP, utiliza este servicio. Habrán aplicaciones como los video conferencias que hacen uso de este servicio por ser altamente sensibles al factor tiempo y tolerables en cuanto a su fiabilidad.

La capa de Transporte tiene los servicios de: Control de Flujo, Multiplexación, detección de errores¹, y encapsulamiento/desencapsulamiento de mensajes en un datagrama IP para enviar mensajes de un proceso a otro.

El software de transporte, divide el stream de datos que se transmite de la aplicación en unidades de datos de transporte, cada una de estas unidades lleva en su cabecera información que identifica a la aplicación de origen y a la aplicación de destino.



Esta identificación es a través de un número, que es conocido como *puerto*. El número de puerto (RFC 1700) tiene 16 bits, comprendido en el rango de 0 a 1023, controlados y asignados por la IANA² cuyo uso está restringido y reservado para los protocolos de aplicación y ejecutados por administradores de redes o por usuarios autorizados. Tiene el propósito de elegir entre múltiples procesos que se ejecutan en la computadora de destino. El número de puerto de destino es necesario para la entrega y el número de puerto de origen es necesario para la respuesta.

Para que el proceso cliente acceda al servidor, deberá conocer su número de puerto. Los servidores de uso público tienen asignado un número de puerto universal. La siguiente tabla muestra algunos de estos números:

¹ Ver Capítulo 7
² Internet Assigned Numbers Authority

SERVICIO	puerto	Protocolo de transporte	Descripción
FTP	21	TCP, UDP	Trasferencia de archivos
SSH	22	TCP, UDP	Terminal en red segura
TELNET	23	TCP, UDP	Terminal en red
SMTP	25	TCP, UDP	Trasferencia de correo
HTTP	80	TCP, UDP	Transferencia hipertexto
POP3	110	TCP, UDP	Acceso a correo

Tabla 5.1 . Puertos de comunicación

5.2. CONTROL DE FLUJO

Este servicio se realiza a nivel de la capa de Enlace y de la capa de Transporte donde lo provee el protocolo TCP. Consiste en la regulación de la información que envía la aplicación asociada al host emisor antes de que deba esperar una confirmación del receptor, para que éste no se sobrecargue, ni se pierdan paquetes por el cambio dinámico que se produce en el intercambio de información entre los extremos de la red, guardando los datos transmitidos no certificados en el buffer del receptor. Por su parte, el receptor leerá los datos de este buffer no necesariamente en el momento que llegan e informa al emisor de la cantidad de espacio libre en el buffer.

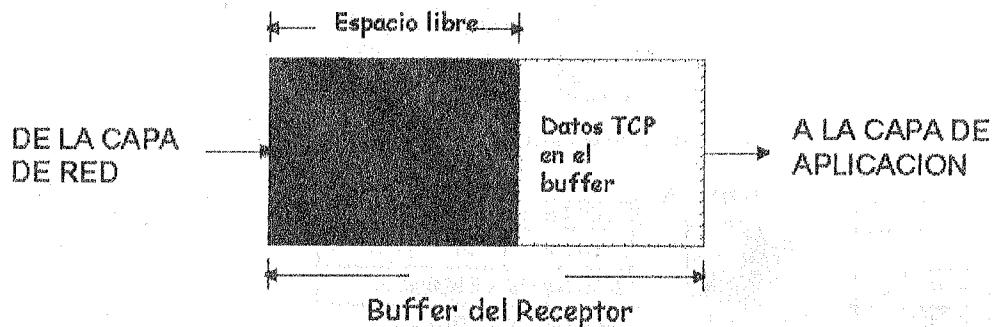


Fig. 5.2 Control de flujo en la capa de transporte

Si el buffer comienza a llenarse, el receptor, cuya velocidad de procesamiento es más lenta que la velocidad de transmisión, debe ser capaz de decir al emisor que detenga la transmisión hasta que vuelva a ser capaz de recibir.

Se produce esta regulación porque cualquier dispositivo de recepción tiene una velocidad limitada para almacenar datos de entrada. Generalmente la velocidad de procesamiento es más lenta que la velocidad de transmisión.

5.3. MULTIPLEXACIÓN/ DEMULTIPLEXACIÓN

La Multiplexación es el proceso mediante el cual se obtienen datos desde múltiples procesos de aplicación del lado del emisor diferenciados por el número de puerto asignado, encapsulando datos dentro la cabecera para crear segmentos y pasar estos segmentos a la capa de red a través de un único nivel de transporte. Por ejemplo, en una aplicación web, el cliente solicita una o más páginas al servidor generándose los correspondientes procesos que se identifican por los puertos de origen como se muestra en la figura.

La función de multiplexación es de muchos a uno.

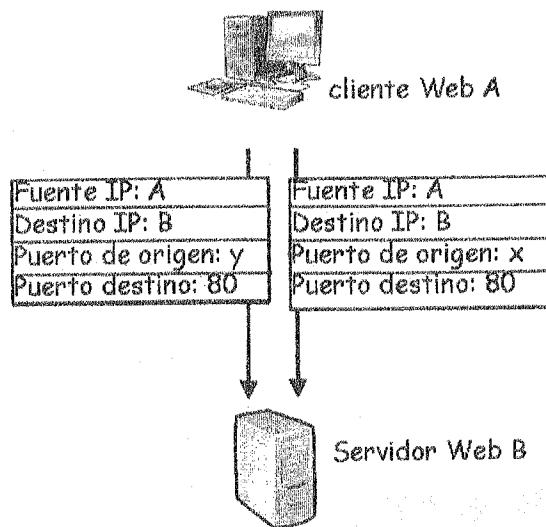


Fig. 5.3 Multiplexación de procesos

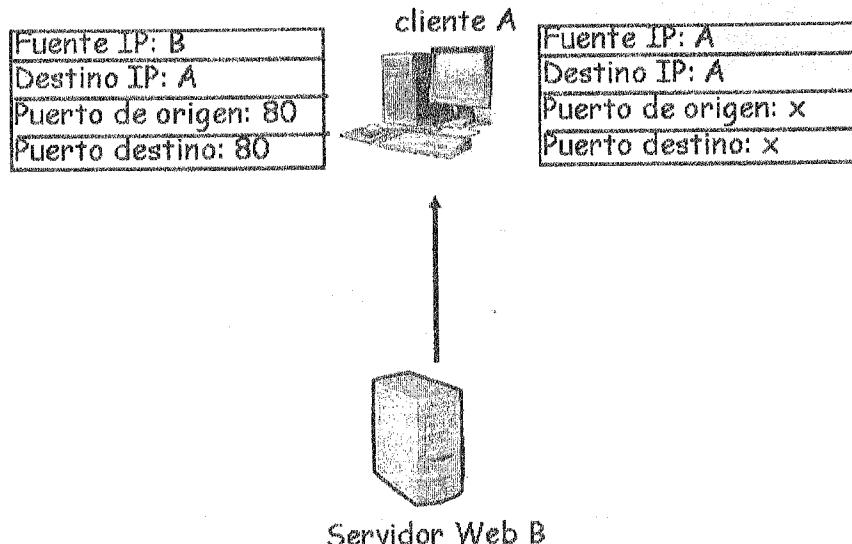


Fig. 5.4 Demultiplexación

En el lado del receptor, la relación es uno a muchos y necesita el proceso inverso que se denomina Demultiplexación. La capa de Transporte recibe datagramas de la capa de Red, después de comprobar si hay errores y quitar la cabecera, la capa de Transporte entrega

cada mensaje al proceso apropiado basándose en el número de puerto. En la figura, el servidor Web devuelve las páginas solicitadas por los respectivos procesos.

Dependiendo de la confiabilidad, del nivel de servicio de transporte o el tipo de aplicación, hay dos protocolos: el Transmission Control Protocol (TCP, RFC 793) y el User Datagram Protocol (UDP, RFC 768). Ambos protocolos utilizan el modelo de comunicación Cliente/Servidor.

5.4 EL PROTOCOLO TCP

El TCP es el protocolo de transporte más utilizado en la mayoría de las redes basadas en el modelo TCP/IP y según (Huston, 2000) actualmente soporta la transferencia de casi el 90% del tráfico total de la red Internet.

Este protocolo tiene las siguientes características:

- ❑ Orientado a la conexión. Con una fase previa de establecimiento de la conexión antes de comunicación entre los extremos o “saludo”,
- ❑ Confiable. Cada paquete enviado requiere acuse de recibo del receptor, sino llega por cualquier motivo (daño o pérdida), el emisor retransmite aquel paquete.
- ❑ El servidor guarda el estado del cliente (*stateful*),
- ❑ Con mecanismo de control de flujo y
- ❑ Usado para transmitir grandes cantidades de datos.
- ❑ El formato de su registro es:

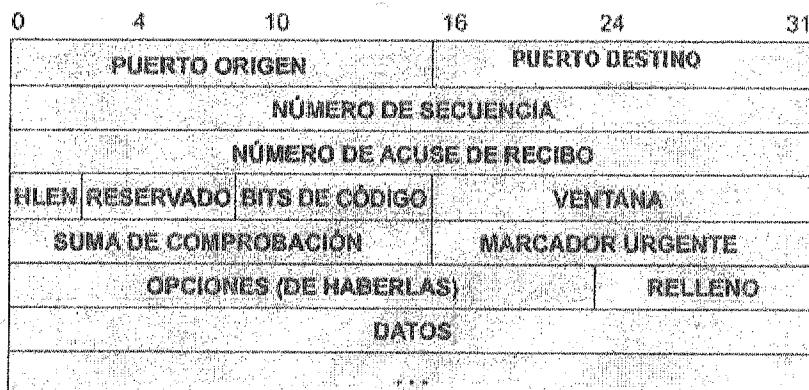


Fig. 5.5 Segmento TCP

Los campos más importantes son:

- El puerto de origen y de destino por donde se establecen las conexiones,
- El número de secuencia. Que define el número del primer byte que transporta este segmento,
- El número de acuse de recibo. Que define el número del siguiente byte que una parte espera recibir. Este número es acumulativo.

- Suma de Comprobación. Que se utiliza para fines de control y detección de error
- Ventana. Que determina el buffer disponible para el flujo de control.

5.4.1 Operación del protocolo TCP

La primera fase de una sesión TCP es el establecimiento de la conexión o "saludo" para asegurar que ambos lados de la conexión tengan ya una comprensión aunque ambigua del espacio del número de secuencia del extremo remoto. Este saludo se inicia en el host de origen que envía un paquete SYN para sincronizar los números de secuencia SEQ, en el otro extremo el host remoto recibe la señal y devuelve el acuse de recibo ACK y su propio número de secuencia (segunda vía) y finalmente el host de origen devuelve su propio acuse de recibo en base al número de secuencia generado por el host remoto. En la siguiente figura se muestra esta operación.

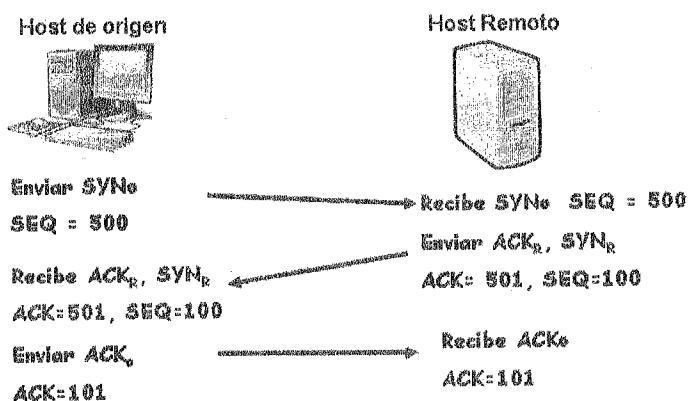


Fig. 5.6 Saludo de tres vías

El uso de ventanas es un mecanismo de control de flujo que requiere que el dispositivo origen reciba un acuse de recibo desde el destino después de transmitir una cantidad determinada de datos. En la Figura:

Si el destino recibe los tres paquetes SYN, envía un acuse de recibo al dispositivo origen, que ahora puede transmitir otros tres paquetes. Si, por algún motivo, el destino no recibe los tres paquetes, por ejemplo, debido a búferes cuya capacidad se ha excedido, no envía un acuse de recibo. Como el origen no recibe un acuse de recibo, sabe que los paquetes se deben retransmitir y que la velocidad de transmisión debe reducirse.

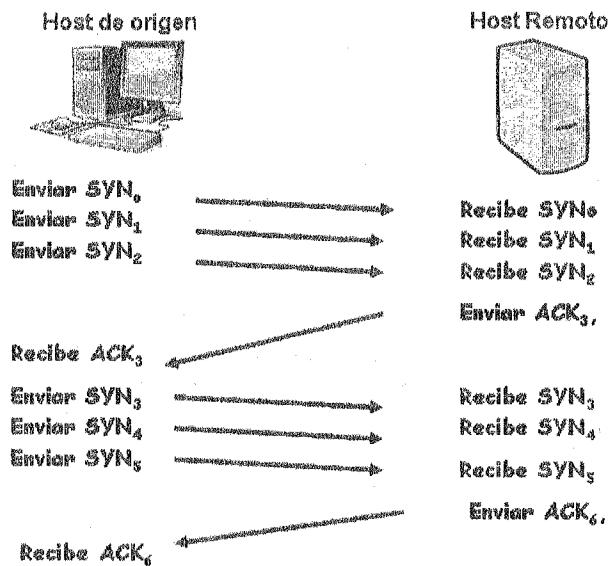


Fig. 5.7 Ventana desizante TCP

El cierre de la conexión necesita de 4 segmentos. TCP para terminar la conexión: como TCP es full-duplex, cada dirección debe cerrar la conexión independientemente de la otra. Para ello cada estación debe enviar un segmento con el flag FIN activado que debe ser reconocido por el otro extremo. El extremo que envía el primer FIN efectúa un cierre activo (active close) mientras que el otro efectúa un cierre pasivo (passive close).

Es posible que los dos extremos hagan un cierre activo, aunque no es una situación típica. En estas prácticas nos centraremos en observar un cierre típico de una conexión TCP: un extremo efectúa un cierre activo y el otro un cierre pasivo como podeis observar en la figura.

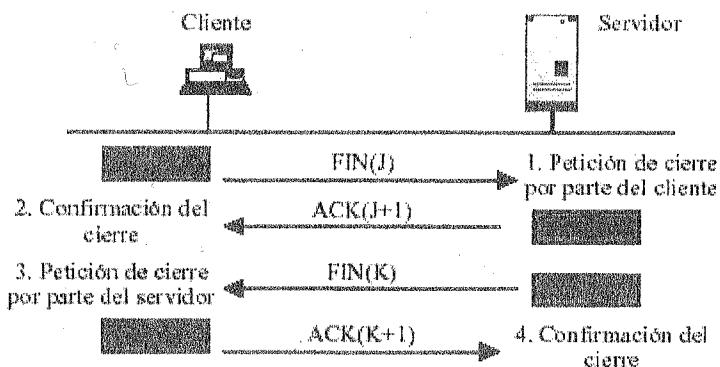


Fig. 5.8 Cierre de conexión TCP

5.5 EL PROTOCOLO UDP

UDP es un protocolo "liviano" que se utiliza para aquellas aplicaciones que requieran transferencias simples de solicitud/respuesta como la transferencia de archivos o aplicaciones que soportan comunicaciones en tiempo real.

Las características de este protocolo son:

- Es un protocolo sin conexión, sin fase de establecimiento previo.
- No es confiable, es decir, no hace acuse de recibo. Los datos que se envían pueden perderse o llegar fuera de secuencia (*stateless*)
- Es rápido porque el segmento de datos UDP es más pequeño,
- No realiza control de flujo,
- No añade nada a los servicios de IP excepto proporcionar comunicación proceso a proceso en lugar de comunicación computador a computador.
- Realiza una limitada comprobación de error
- Adecuado para la transmisión de pequeñas cantidades de datos.
- Tolerante a pérdidas y sensible al tiempo.

El formato del segmento UDP es:

0	16	31
PUERTO ORIGEN UDP	PUERTO DESTINO UDP	
LONGITUD DE MENSAJE UDP	SUMA DE COMPROBACIÓN UDP	
DATOS		

Fig. 5.9 Segmento UDP

5.5.1 Suma de Comprobación

Esta técnica de detección de errores se utiliza también en la capa de Enlace.

De los campos de la anterior figura, destacamos el de la Suma de Comprobación o Checksum que se utiliza para la detección de errores en el segmento transmitido. El transmisor coloca el valor de checksum en el campo checksum de UDP. El receptor calcula el valor de checksum del segmento recibido, revisa si el cálculo del checksum es igual al valor de su campo checksum. Si no son iguales se detecta error.

Se puede simplificar la tarea del receptor si se envía el valor negativo de la suma (el complemento) conjuntamente los datos recibidos.

Ejemplo 5.1

Si se enviaron los números (1,3,8) determinar si hay error por el cálculo de complemento.

Solución

Añadiendo el valor de la suma se tiene (1,3,8,12). Sumando el último valor con su complemento ($12 + (-12)$) se tiene 0. Entonces se asume que no hay error, caso contrario hay error.

En la aritmética complemento a uno se puede representar los números sin signo entre 0 y $2^n - 1$ utilizando solo n bits. Si el número tiene más de n bits, los bits de la izquierda extra necesarios se añaden a los n bits de la derecha. En esta aritmética un número negativo se puede representar invirtiendo todos los bits (los 0 se cambian por 1 y los 1 por 0). Luego siguiendo el anterior razonamiento de la suma del complemento, si no se produce error, la suma incluyendo Checksum tendrá todos 1s.

Ejemplo 5.2

Se envían tres palabras de 16-bit :

- 0110011001100110
- 0101010101010101
- 0000111100001111

Determinar si se produce error por el cálculo de Checksum

Solución

Sumando los tres anteriores valores con la aritmética binaria normal, obtenemos:

1100001011000010

A este resultado aplicamos el complemento a 1, es decir:

0011110100111101

Finalmente sumamos los dos anteriores resultados parciales y obtenemos:

1111111111111111

5.6 CONCEPTOS Y TERMINOS CLAVE

Acuse de recibo
Cierre de Conexión
Control de Flujo
Multiplexación/Demultiplexación
Número de puerto
Saludo de tres vías
Servicio de Transporte
Servicio Orientado a la Conexión
Servicio Sin Conexión
Sesión TCP
Suma de Comprobación
TCP
UDP
Ventana

5.7 PREGUNTAS DE REPASO

1. ¿Cuál es el propósito de los números de puerto?
 - A. Llevar un control de las distintas conversaciones que atraviesan la red al mismo tiempo.
 - B. Elegir entre múltiples procesos que se ejecutan en la máquina de destino.
 - C. Asignar dinámicamente usuarios finales a una determinada sesión
 - D. Los sistemas de origen generan estos números para predecir las direcciones de destino.

2. ¿Para qué se utiliza el intercambio de señales de tres vías/conexión abierta TCP?
 - A. Garantizar que se podrán recuperar datos perdidos si se producen problemas más tarde
 - B. Determinar cuántos datos puede aceptar la estación receptora a la vez.
 - C. Brindar un uso eficiente del ancho de banda por parte de los usuarios
 - D. Convertir las respuestas ping binarias en información en las capas superiores

3. ¿Cuál es la función de una ventana deslizante TCP?
 - A. Amplía la ventana para que se puedan enviar más datos a la vez
 - B. Permitir que el tamaño de ventana se desliza hacia cada sección del datagrama para recibir datos
 - C. Permitir que el tamaño de la ventana se negocie dinámicamente durante la sesión TCP
 - D. Limita los datos entrantes de tal manera que los segmentos se deban enviar uno por uno

4. ¿Cuáles protocolos utilizan los segmentos UDP para proporcionar confiabilidad?
 - A. Protocolos de capa de red
 - B. Protocolos de capa de aplicación
 - C. Protocolos Internet
 - D. Protocolos de control de transmisión

5. El protocolo UDP no es confiable porque:
 - A. Está expuesto al ataque de intrusos
 - B. Los datos que se envían tienen errores
 - C. Los datos que se envían pueden perderse
 - D. Está expuesto a interferencias y ruido

6. Cual servicio evita el problema que se produce cuando un host ubicado en uno de los lados de la conexión hace que se desborden los buffers del host ubicado en el otro lado.
- A. Control de congestionamiento
 - B. Control de flujo
 - C. Multiplexación
 - D. Control de suma de comprobación o checksum
7. Cual método o servicio obtiene datos desde multiples procesos de aplicación
- A. Control de congestionamiento
 - B. Control de flujo
 - C. Multiplexación
 - D. Control de suma de comprobación o checksum
8. Cual método o servicio asegura que la subred sea capaz de transportar el tráfico ofrecido
- A. Control de congestionamiento
 - B. Control de flujo
 - C. Multiplexación
 - D. Control de suma de comprobación
9. ¿Cuál de las siguientes opciones describe más correctamente el control de flujo?
- A. Un método para administrar un ancho de banda limitado
 - B. Un método para conectar dos hosts de forma síncrona
 - C. Un método para garantizar la integridad de los datos
 - D. Un método para controlar si los datos tienen virus antes de realizar la transmisión
10. ¿Cuál de las siguientes opciones controla la cantidad de información que se transfiere de extremo a extremo y ayuda a permitir la confiabilidad TCP?
- A. Broadcast
 - B. Operaciones en ventana
 - C. Recuperación de errores
 - D. Control de flujo
11. Los protocolos HTTP, SMTP y FTP están asignados respectivamente a los siguientes puertos:
- A. 25,80,21
 - B. 80,25,21
 - C. 21,80,25
 - D. 25,21,80

CAPITULO 5 : LA CAPA DE TRANSPORTE

12 . Para el cierre de una conexión TCP cuantos segmentos se utilizan:

- A. Tres
- B. Cuatro
- C. Dos
- D. Uno

13. El protocolo UDP provee un servicio

- A. Con control de flujo
- B. Sin conexión
- C. Sin garantía de ancho de banda
- D. Poco fiable

14. En una conexión de tres vías TCP

- A. El acuse del Rx es igual al número de secuencia del Tx
- B. El acuse del Rx se incrementa en uno respecto al número de secuencia del Tx
- C. El acuse del Rx se decrementa en uno respecto al número de secuencia del Tx
- D. El acuse del Rx es al número de secuencia del Rx

15. Cual técnica de detección de errores utiliza el protocolo UDP

- A. Bit de paridad
- B. Código de bloques
- C. Suma de comprobación
- D. Código de Redundancia Ciclica

5.8 TALLER

Leer el artículo Transfer Protocols Fundamentals

1. Explicar como la capa de Transporte prepara los datos del usuario para la transmisión de la red

2. Completar la información en la siguiente tabla de conexión de tres vías tcp

Transmisor	Receptor
Envia SEQ = 30	Recibe SEQ = Envia SEQ = 45
Recibe SEQ = ACK =	ACK = Recibe ACK =
Envia ACK =	

3. Indicar cual es una diferencia entre un protocolo "stateful" y "stateless". Dar ejemplos

4. UDP es un ejemplo de protocolo sin conexión y sin estado. Para que fue diseñado?

5. TCP es un ejemplo de protocolo orientado a la conexión y de protocolo de estado. Para que clase de datos fue diseñado?

6. Hallar el valor de checksum de las siguientes secuencias:

11111101

00000010

11111011

CAPITULO 6 · LA CAPA DE RED

Objetivos de Aprendizaje: *Al concluir el capítulo, usted será capaz de:*

- *Identificar los tipos de direcciones IP,*
- *Configurar una red,*
- *Comprender el funcionamiento de los algoritmos y los protocolos de enrutamiento*

6.1. SERVICIOS DE LA CAPA DE RED

La capa de Red, tiene el servicio de entrega, reenvío y encaminamiento o enrutamiento de los paquetes, es decir, como un paquete es tratado por la subred, el modo en que el paquete es entregado al siguiente router y como encontrar la mejor ruta respectivamente, desde el host de origen, pasando por la interconexión de routers hasta llegar al host de destino.

Este servicio que presta a la capa de Transporte para la comunicación de los extremos lo realiza gracias al funcionamiento de routers y a los protocolos de Comunicación de esta capa.

- Los routers. Son dispositivos de comunicación de capa 3, que independiente de los protocolos y arquitectura de red que se utilicen; se encargan del filtrado, conexión de segmentos de red y reenvío de paquetes que llegan y salen de una red.
- Los protocolos de Comunicación de esta capa: IP, ARP, ICMP y los protocolos de enrutamiento. Estos se encargan respectivamente, de la identificación de los hosts de origen y de destino a través de un código o número(protocolo IP), de asignar estos números a un código físico de la tarjeta de comunicación, dotar de control al protocolo IP y de actualizar las tablas de enrutamiento que se consultan en el reenvío y el encaminamiento.

6.2. EL PROTOCOLO IP

El Internet Protocol (IP) [RFC 791] es uno de los dos protocolos que sustentan la familia de protocolos TCP/IP. Fue diseñado en sistemas de interconexión de redes, para la transmisión de datagramas del host de origen al host de destino, dependiendo de la topología y cobertura de la red a través de routers y switches.

IPv4 es la versión 4 del Protocolo IP y constituye la primera versión de IP que es implementada de forma extensiva. Su esquema de direccionamiento de datagramas de 32 bits provee 4 billones de posibles direcciones. Según la (APNIC,2007)¹ hasta septiembre de 2007, quedaba por asignar a la institución encargada IANA (Internet Assigned Numbers Authority) solo el 18% de las direcciones Ipv4, un 14% está reservado para uso privado, multicast y propósitos especiales y el 68% restante de direcciones ya ha sido asignado.

A pesar de algunas predicciones en sentido que hasta el 2008 estas direcciones estarían cubiertas,² esas pocas direcciones aún disponibles de Ipv4, el uso de NAT (Network Address Translation) que veremos más adelante y la facilidad de su uso está demorando la inevitable transición a la nueva versión de IP que es la Ipv6. Por lo cual mantenemos en este libro el estudio de los datagramas IP y su manejo correspondiente a la versión 4.

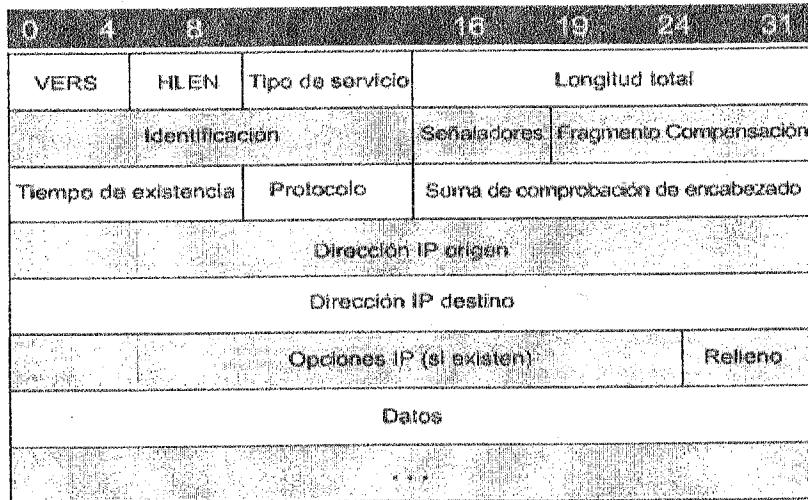


Fig. 6.1 Formato datagrama Ipv4

Dentro del encabezado de este datagrama, están las direcciones IP de origen y de destino. Estas direcciones IP están agrupados en 4 bytes de 32 bits cada uno (notación binaria). Para

¹ Asia Pacific Network Information Centre

² Solensky F. "Ipv4 Address Lifetime Expectations," en Ipng: Internet Protocol Next Generation (S.Badner, A. Mankin, ed), Addison Wesley, 1996.

que las direcciones IP sean más fáciles de leer, se escriben en notación decimal con un punto separando los bytes.

Ejemplo 6.1

Cambiar la dirección IP 200.11.10.26 a notación binaria

Solución

Se reemplaza cada número decimal por su equivalente binario

11001000 00001011 00001010 00011010

Ejemplo 6.2

Cambiar la dirección IP 00111001 11101110 00100011 01010000

Solución

Reemplazamos cada grupo de ocho bits con su número decimal equivalente y añadimos puntos para la separación. Para el ejemplo, tenemos: 57.238.35.80

En general las direcciones IP constan de dos partes: la dirección de red y la dirección de host.



Fig. 6.2 Partes de una dirección IP

La dirección de red identifica al grupo de host y routers del segmento físico al que pertenece y la dirección de host es la máquina en cuestión a la que se quiere identificar. Ambas direcciones, pueden abarcar de 1 a 3 bytes dependiendo de la clase IP, respetando la máxima extensión de 32 bits.

6.2.1 Clases de direcciones IP

El direccionamiento de redes denominado "classfull" o direccionamiento con clases, toma en cuenta la extensión del segmento de red en relación a la cantidad de hosts y de redes para este segmento. Según este criterio, el direccionamiento de redes puede ser de las siguientes 5 clases:

- Clase A corresponde a una gran cantidad de hosts ($2^{24} - 2$) con un rango entre 1 a 127 redes privilegiadas (se reserva el primer bit de la izquierda).
- Clase B tiene ($2^{16} - 2$) hosts, para un rango entre 128 a 191 redes
- Clase C con ($2^8 - 2$) hosts, tiene un rango de redes comprendido entre (192 a 233).
- Clase D. Con un rango de redes (224 – 239) Para Multicast
- Clase E Con rango de redes (240 – 255) Con propósitos de experimentación.³

Para identificar la clase a la que pertenece un número IP cualquiera se siguen las siguientes reglas:

- a. Los bytes están en el rango de 0 a 255
- b. Dependiendo del valor del primer byte de la izquierda el número IP será clasificado según las clases mencionadas.
- c. Las clases (A, B y C) como se muestra en la figura, reservan 3, 2 o 1 bytes respectivamente para las direcciones de hosts y su complemento ocupan las direcciones de red. Así por ejemplo, el número IP del inciso b, es una clase C que destina solo el último byte para la dirección de host y los anteriores bytes forman la dirección de red.

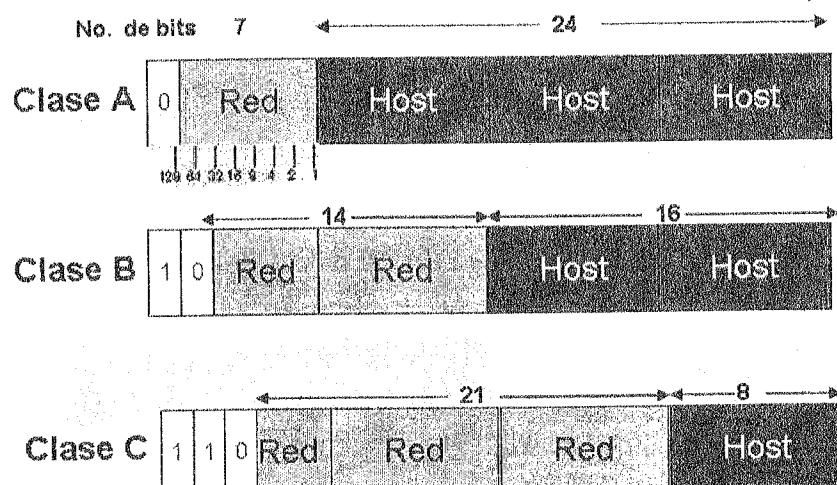


Fig. 6.3 Clases de direcciones IP

Ejemplo 6.3

Hallar la clase de la dirección

- i. 11.35.121.3
- ii. 189.10.1.20
- iii. 00001000 10000010 11000000 10001001
- iv. 11000010 10001001 10000001 10001101

Solución

- i. El primer byte es 11 ∈ (1,127), la clase es A
- ii. El primer byte es 189 ∈ (127,191), la clase es B
- iii. El primer bit de la izquierda es 0. Por lo cual es una dirección clase A.
- iv. Los primeros tres bits de la izquierda son 110. Por lo cual es una dirección clase C

En general la cantidad de host se disminuye en 2 para reservar la dirección del segmento de red que tiene 0's en la parte que corresponde a los hosts y para la dirección de broadcast que tiene 1's binario en el campo de hosts(todos los dispositivos de la red).

³ Se reservaron para uso futuro; solo se usaron algunos pocos, lo que resultó en desperdicio de direcciones.

Ejemplo 6.4

Dada la dirección IP 20.123.14.31. Determinar:

- i. La dirección del segmento de red
- ii. La dirección de broadcast

Solución

- i. El primer byte de la izquierda está en el rango (1,127). Luego se trata de una dirección clase A que en los restantes bytes tiene 0s. Es decir, 20.0.0.0
- ii. La parte de la dirección correspondiente a los host son los tres bytes restantes, luego la dirección de broadcast es: 20.255.255.255

Donde el valor decimal "255", equivale a "1s" en todo el byte.

6. 2.2 Máscara de red

Es un número "comodín" expresado en formato decimal, al igual que un número IP (32 bits con 4 bytes de 8 bits cada uno) que se utiliza para identificar la dirección del segmento de red, varía según la clasificación mencionada. Por definición *asigna el valor 0 a la dirección de host y el valor 1 a la dirección de red*. Así⁴:

Para un IP clase A, su máscara es: 255.0.0.0

Para un IP clase B, su máscara es: 255.255.0.0

Para un IP clase C, su máscara es: 255.255.255.0

Para determinar la dirección del segmento de red, se realiza la operación lógica AND entre el IP dado y su máscara.

Ejemplo 6.5

Dada la dirección IP 130.26.114.2. Hallar el segmento de red

Solución

Observamos que se trata de una clase B, realizando el AND lógico con su respectiva máscara obtenemos la dirección del segmento de red 130.26.0.0.

Ejemplo 6.7

Hallar el segmento de red de la dirección IP 223.10.26.4/21

Solución

En el ejemplo se asigna 21 bits contando de izquierda a derecha al campo de red.

Para la determinación de la dirección del segmento de red, utilizamos la máscara de subred como comodín y la operación AND lógico. Para el ejemplo anterior, tenemos:

10111111	00001010	00011010	00000100	223.10.26.4
11111111	11111111	11111000	00000000	255.255.248.0
10111111	00001010	00011000	00000000	223.10.22.0

Podemos tener tamaños variables de subredes, dependiendo de la cantidad de bits que se le asigne a las subredes (valores en 1) y a los hosts (valores en 0).

Para determinar el número de subredes y el número de hosts aplicamos respectivamente las siguientes fórmulas:

$$2^n - 2 \text{ y } 2^{n^*} - 2$$

donde n^* es el complemento de n .

Por ejemplo, si $n=1$ entonces $n^* = 7$; aplicando las mencionadas fórmulas tenemos:

$$2^n - 2 = 2^1 - 2 = 0 \text{ y } 2^{n^*} - 2 = 2^7 - 2 = 126$$

Siguiendo este procedimiento, formamos la siguiente tabla para una red clase C:

Bits	Subredes	Hosts
1	0	126
2	2	62
3	6	30
4	14	14
5	30	6
6	62	2
7	126	0

Tabla 6.2 Subredes y hosts variables

En el ejemplo anterior, si quisieramos tener 6 subredes, asignamos el valor 1 a los 3 bits del último byte contando de izquierda a derecha: 11100000. Haciendo la operación AND con el IP dado, obtenemos la siguiente dirección de red: 223.10.26.0.

6.4. ALGORITMOS DE ENRUTAMIENTO

Generalmente un router está conectado a varias redes, cuando recibe un paquete, entonces se plantea el siguiente problema fundamental de la optimización de redes: *Por cual red debiera enviarlo de tal forma que de las rutas disponibles se elija la ruta optima?*

La determinación de la mejor ruta, conjunto de enlaces o trayectoria de los paquetes hasta llegar a su destino es implementada por un algoritmo de enrutamiento. Cada enlace tiene un coste que refleja una métrica como por ejemplo: costo, distancia, retardo, productividad.

El router que pasa a través de una red puede tener métricas diferentes. Por ejemplo, si se trata de distancias, lo óptimo es que la métrica total de la ruta sea la mínima. En cambio la ruta óptima considerando el ancho de banda como métrica, será la que tenga su valor máximo.

Un algoritmo de enrutamiento calcula los valores de una tabla de ruteo en cada nodo. Como todo algoritmo, son deseables las siguientes características:

- La correctitud, en relación a su convergencia después de algún cambio, tiene que converger rápidamente hacia la mejor ruta.
- La robustez y estabilidad ante fallas de hardware y software. Adaptarse a cambios en la topología o en la cantidad de tráfico con ninguna o poca intervención humana.
- La justicia y optimalidad. Frecuentemente contradictorias. Se debe equilibrar la eficiencia global y la justicia individual.
- Complejidad. El algoritmo que construye la tabla de ruteo tiene que usar un mínimo de mensajes, almacenamiento y tiempo.

El direccionamiento de paquetes se lo realiza mediante tablas que contienen la siguiente información:

- Las direcciones de las redes conocidas
- Como conectarse a las otras redes
- Las posibles trayectorias entre los routers para llegar a algún destino
- El costo de enviar datos sobre esas rutas.

6.4.1 Clasificación de Algoritmos de Enrutamiento

- Tomando en cuenta el alcance de información que tienen los routers
 - Centralizado. Cálculo centralizado de rutas, obteniéndose una visión global de la red. Cada nodo informa al resto del estado de sus enlaces. Ej. Algoritmo de Estado de Enlace
 - Descentralizado. Cada router ve solo la información local (la propia y la de los vecinos físicamente conectados con él) y calcula la ruta sobre esta base. Ej: Algoritmo Vector Distancia.
- Según la variación del coste del enlace respecto al tiempo
 - Estáticas. Las tablas de enrutamiento cambian lentamente, generalmente en respuesta a la intervención humana. Una tabla estática es una tabla con entradas manuales.
 - Dinámicas. Las tablas de enrutamiento cambian con el tráfico de la red o con los cambios de topología. Una tabla dinámica es una tabla que se actualiza automáticamente cuando hay algún cambio en la red.

Dos enfoques combinan los anteriores criterios:

Algoritmo de Estado de Enlace

- centralizado y dinámico (aunque periódicamente actualizado). Si hay cambios en cualquier nodo (enlace desactivado) la topología debe actualizarse en cada nodo.
- Cada nodo llega a conocer la topología de la red y los costos de los enlaces, a partir de su conocimiento parcial del estado de sus enlaces(tipo, coste).
- Se requieren las siguientes acciones para asegurar que cada nodo tiene la tabla de enrutamiento que muestra el nodo de menor coste al resto de nodos:
 - Creación de los estados de los enlaces por cada nodo, denominado paquete de estado de enlace o LSP.
 - Diseminación de los LSP a cada enrutador o Inundación, de una forma fiable y eficiente.
 - Formación del árbol de camino más corto para cada nodo.
 - Cálculo de una tabla de enrutamiento basado en el árbol de camino más corto.
- Usado en el protocolo OSPF
- Ejemplo: Algoritmo de Dijkstra

Algoritmo Vector Distancia

La ruta de mínima distancia es la ruta de menor coste entre dos nodos. Cada nodo mantiene un vector (tabla) de las distancias mínimas a cada nodo.

- distribuido, cada nodo distribuye información entre sus vecinos, es decir, cada nodo conoce el costo de alcanzar a sus vecinos. Se comparte información entre los vecinos (su tabla de enrutamiento) de forma periódica y cuando hay algún cambio
- Dinámico. Provee respuesta inmediata a cambios y cada nodo lo hace conocer a sus vecinos.
- Asíncrono, No requiere que todos los nodos operen en forma sincronizada con otros.
- Iterativo. El proceso continúa hasta que no quede información que intercambiar entre sus vecinos.
- Usado en el protocolo RIP
- Ejemplo: Algoritmo de Bellman-Ford

6.4.2 Algoritmo de Dijkstra

Este algoritmo fue concebido por Edsger Dijkstra en 1959, para la determinación del camino más corto dado un vértice o nodo origen al resto de nodos en un grafo dirigido y con costos (conocidos) en cada enlace o arista.

Sea un grafo dirigido

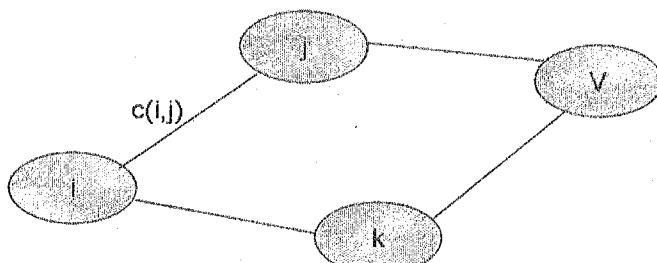


Fig. 6.6 Grafo dirigido

Donde:

$c(i,j)$: el costo de enlace del nodo i al j . costo infinito si no tiene vecinos.

$D(v)$: distancia al destino V

$p(v)$: nodo predecesor del origen a v , que es vecino de v . ej. k, j

N : conjunto de nodos cuya distancia mínima es conocida

En nuestro grafo dirigido de la fig, nuestro problema consiste en determinar el camino más corto, por ejemplo del nodo i a los nodos j, k, V .

La idea central subyacente en el algoritmo de Dijkstra es que cada subcamino del camino mínimo será a su vez un subcamino de coste mínimo.

Mediante un procedimiento de etiquetado, el algoritmo de Dijkstra almacena información computacional de unas etapas a otras, reduciendo su complejidad a una del orden de $O(n^2)$.

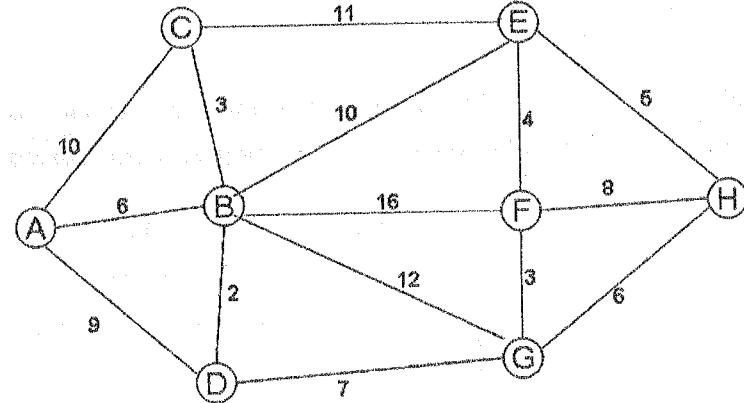
Un pseudocódigo del algoritmo es el siguiente:

```

1 Incialización:
2  $N = \{A\}$ 
3  $\forall v$ 
4   Si v es adyacente a A
5     entonces  $D(v) = c(A, v)$ 
6     sino  $D(v) = \text{infinito}$ 
7
8 Repetir
9   encontrar w  $\notin N$  tal que  $D(w)$  sea mínimo
10   añadir w a N
11   actualizar  $D(v)$ , v adyacente a w y  $v \notin N$ :
12      $D(v) = \min(D(v), D(w) + c(w, v))$ 
13   /* el nuevo costo a v es el anterior costo a v o un camino
14   más corto conocido a w más el costo de w a v */
15 hasta que todos los nodos se encuentren en N
```

Ejemplo 6.8

Sea la red,



Aplicar el algoritmo de Dijkstra para determinar la ruta crítica y la tabla de ruteo

Solución

N	$D(B), p(B)$	$D(C), p(C)$	$D(D), p(D)$	$D(E), p(E)$	$D(F), p(F)$	$D(G), p(G)$	$D(H), p(H)$
A	6,A	10,A	9,A	Infinito	Infinito	Infinito	Infinito
AB		9,C	8,B	16,B	22,B	18,B	Infinito
ABD						15,D	Infinito
ABD G					18,G		21,G
ABD GH							

La ruta crítica del nodo A al H es: ABDGH

Destino	B	C	D	E	F	G	H
Costo, Vecino	6,B	9,C	8,B	16,B	18,G	15,D	21,G

Tabla 6.2 Tabla de Ruteo

6.4.3 Algoritmo de Bellman – Ford

La estructura de datos de este algoritmo es la tabla-distancia mantenida en cada nodo. Estas tablas tienen una fila por cada destino en la red y una columna por cada vecino.

Sea el nodo X, para un destino Y a través de su vecino Z:

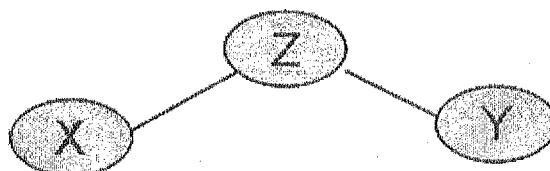


Fig. 6.7 Ejemplo de red

La distancia de X al nodo Y a través de Z es:

$$D^X(Y, Z) = c(X, Z) + \min_w \{ D^Z(Y, w) \} \quad (\alpha)$$

Igual al costo del origen a la vía + min D(via al destino a través de cualquier nodo).

Un pseudocódigo del algoritmo para determinar la Tabla Distancia es el siguiente:

```

1 Inicialización:
2   ∀ los nodos adyacentes v(nodos vecinos vía los mismos nodos)
3      $D^X(v, v) = c(X, v)$ 
4      $D^X(*, v) = \text{infinito}$  /* significa para todos los demás destinos,
5       enviar  $\min_w D^X(y, w)$  a cada vecino /* w sobre los vecinos X's */
6 Repetir
7   esperar (hasta un cambio en el costo de enlace al vecino V
8   O hasta que se reciba una actualización del vecino V)
9
10
11
12 Si ( $c(X, V)$  cambia por d)
13   /* cambiar el costo a todos los dest's vía vecino v por d */
14   /* nota: d puede ser positivo o negativo */
15   Para todos los destinos y:  $D^X(y, V) = D^X(y, V) + d$ 
16
17 sino si (actualización recibida de V al destino Y)
18   /* el camino mas corto de V algún Y ha cambiado */
19   /* V envía un nuevo valor para su  $\min_w D^V(Y, w)$  */
20   /* la llamada a este nuevo valor recibido es "nuevoval" */
21   Para un solo destino y:  $D^X(Y, V) = c(X, V) + \text{nuevoval}$ 
22
23 si tenemos nuevo  $\min_w D^X(y, w)$  para cualquier destino Y
24   enviar un nuevo valor de  $\min_w D^X(y, w)$  a todos los vecinos
  
```

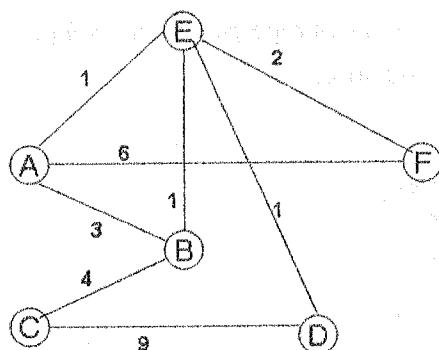
Luego, con los valores óptimos⁵ de los costos de cada fila (destino) de la tabla construimos la tabla de ruteo.

5

Dependiendo de la métrica será un mínimo o en su caso un máximo

Ejemplo 6.9

Sea la red:



Determinar a) la tabla distancia y b) la tabla de ruteo del nodo B.

Solución

a)

En la primera iteración,

- Llenamos las celdas que corresponden a aquellos nodos vecinos a B, vía los mismos nodos

$$D^B(A, A) = 3 \quad D^B(C, C) = 4 \quad D^B(E, E) = 1$$

- La distancia a los nodos no vecinos a B es ∞ (infinito)

$$D^B(D, \delta) = \infty \quad D^B(F, \delta) = \infty$$

Las otras distancias calculamos con la expresión (α), por ejemplo

$$D^B(A, E) = c(B, E) + \min_w \{ D^E(w, w) \} = 1 + \min(1, 4) = 2$$

En la siguiente iteración, con la información que llega de los vecinos, se actualiza la tabla, quedando de la siguiente manera:

D^B	A	C	D	E	F
A	3	10	4	2	6
C	9	4	8	6	10
D	5	10	2	2	6
E	4	9	3	1	5
F	6	11	5	3	3

Tabla 6.3 Tabla Distancia del ejemplo

Donde las filas son los destinos y las columnas las vías.

- b) Para la determinación de la Tabla de ruteo, en este caso tomamos los valores mínimos de cada fila de la anterior tabla.

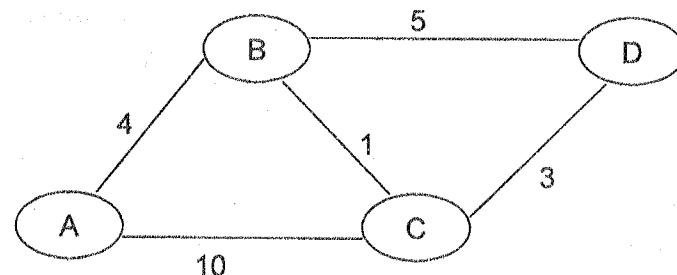
	Costo
A	E, 2
C	C, 4
D	D, E, 4
E	E, 1
F	E, F, 3

Tabla 6.4 Tabla de ruteo del ejemplo

Cuando el nodo detecta un cambio en el costo del enlace actualiza la tabla de distancia. Sin embargo, cuando la convergencia es lenta, se producen los loops de enrutamiento por actualizaciones no válidas en las tablas de enrutamiento denominados *conceo al infinito*.

Este problema se evita de dos maneras: incorporando temporizadores de espera que marcan la ruta como accesible o inaccesible dependiendo de la información que recibe de sus vecinos o definiendo un máximo número de saltos de un router a otro antes de llegar a su destino.

Ejemplo 6.10 Sea la red



Hallar las tablas de Distancia y de ruteo para el nodo C, si hubo enrutamiento dinámico, es decir, si éste detecta cambio en el costo del enlace AB (4) por el nuevo costo 2.

Solución

Siguiendo el procedimiento del ejemplo anterior, la tabla distancia para el nodo A, sin cambios es:

D ^A	B	C
B	4	11
C	5	10
D	8	13

Los otros valores de la tabla, se actualizarán, por ejemplo:

$$D^C(A,B) = c(C,B) + \min(2, 11, 18) = 1 + \min(2, 11, 18) = 3$$

Luego la nueva tabla Distancia para el nodo A y la ruta será:

D ^A	B	C
B	2	11
C	10	10
D	6	13

A	B	3
B	B	1
D	D	3

6.5. PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento determinan las rutas que siguen los protocolos enrutados como el IP hacia sus destinos y son utilizados por los routers para intercambiar tablas de enrutamiento y compartir información de enrutamiento.

Estos protocolos se han creado en respuesta a la demanda de tablas de enrutamiento dinámico. Como no se pueden almacenar todos los destinos posibles en tablas de ruteo locales, porque el intercambio de tablas de ruteo saturarían los enlaces, las redes, por ejemplo la Internet, se divide la red en subredes o regiones, cada una de ellas bajo el control de una sola autoridad, conocida como sistema autónomo o Autonomous System (AS).

Un sistema autónomo AS es un grupo de redes y routers bajo la autoridad de una única administración.

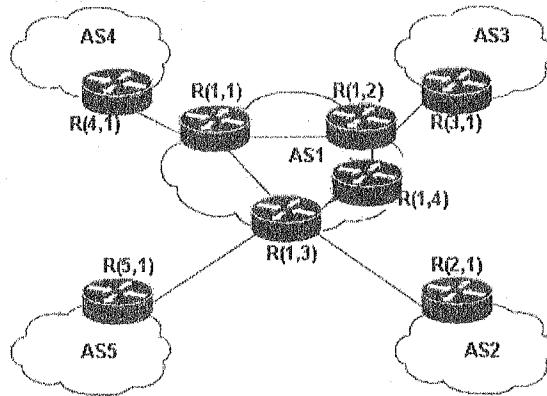


Fig. 6.8 División de la red en regiones AS

Para su estudio, los protocolos de enrutamiento se dividen en dos categorías:

- Protocolos interiores o intra AS (operan dentro de un AS)
- Protocolos exteriores o inter AS (operan entre AS)

Un protocolo intra AS conocido como Interior Gateway Protocol (IGP) se utiliza para configurar y mantener las tablas de enrutamiento dentro de un AS. El enrutamiento intra AS solo involucra a aquellos routers de la misma área. Luego que las tablas de enrutamiento son configuradas, los datagramas son enrutados dentro del mencionado sistema autónomo. En la anterior figura, tenemos el router R(1,4) mantiene las tablas dentro del sistema AS1

Para este propósito, los protocolos intra AS se valen de algoritmos del camino más corto como Vector distancia que usa RIP (Routing Information Protocol) o el Estado de enlace que lo hace OSPF (Open Shortest Path First).

Los protocolos inter AS tienen la tarea de configurar las tablas de enrutamiento, de manera que los datagramas puedan pasar a través de múltiples sistemas autónomos, con la

información proveniente de la ruta. Protocolos de ejemplo de inter AS son: Protocolo de pasarela exterior (EGP) y Protocolo de pasarela de borde (BGP).

Uno o más routers de un AS tendrán la responsabilidad de enrutar paquetes fuera del AS, en la anterior figura, los routers R(1,1), R(1,2) y R(1,3) de AS1. Estos son llamados *routers gateways*, que utilizan los protocolos inter AS para la comunicación entre AS para llegar a su destino.

En los protocolos inter AS no hay una única métrica de coste, la política de enrutamiento deberá ser consensuada entre los actores involucrados en la comunicación entre redes. En cambio en los protocolos intra AS, al existir un solo administrador, no se requieren de decisiones políticas, es decir, es más técnico y están orientados hacia la eficiencia.

6.5.1 Protocolo RIP (Routing Information Protocol) (RFC 1058, 1723)

Es un protocolo de enrutamiento intradominio que utiliza el algoritmo vector distancia donde cada enlace tiene un costo de un salto, es decir, trata a todas las redes por igual, con un límite de costo de 15. Los routers vecinos intercambian información de enrutamiento cada 30 segundos. RIP utiliza el servicio de transporte UDP.

RIP implementa el enrutamiento basado en vector distancia con las siguientes consideraciones:

- En un sistema autónomo, existen routers y redes (enlaces). Los enrutadores tienen tablas de enrutamiento, las redes no.
- El destino en una tabla de enrutamiento es la red, lo que significa que la primera columna define la dirección de red.
- La métrica utilizada por RIP es muy sencilla; se define la distancia como el número de enlaces (redes) necesarios para alcanzar el destino. Por esta razón, la métrica en RIP se conoce como contador de saltos.
- El infinito se define como 16, lo que significa que cualquier camino en un sistema autónomo que utilice RIP no puede tener más de 15 saltos.
- La columna siguiente nodo define la dirección del router al cual se debe enviar el paquete para alcanzar su destino.

En la siguiente figura se muestra la tabla de enrutamiento para el router R(1,3) del anterior ejemplo de la división de red en regiones AS:

Red destino	Siguiente router	Nro. de saltos
AS4	R(1,1)	2
AS2	---	1
AS3	R(1,4)	3
AS5	---	1

Tabla 6.5 Tabla de enrutamiento para R(1,3)

El procedimiento de recuperación del RIP ante un fallo de enlace es:

- Si un router vecino no responde luego de 180 segundos, se lo considera inviable y RIP modifica la tabla local de enrutamiento propagando esta información de advertencia al resto de sus vecinos.
- Los vecinos a cambio mandan nuevos avisos si las tablas cambian.
- La información de falla rápidamente se propaga a toda la red

En la siguiente figura, se muestra un caso de falla de enlace con el router R(5,1):

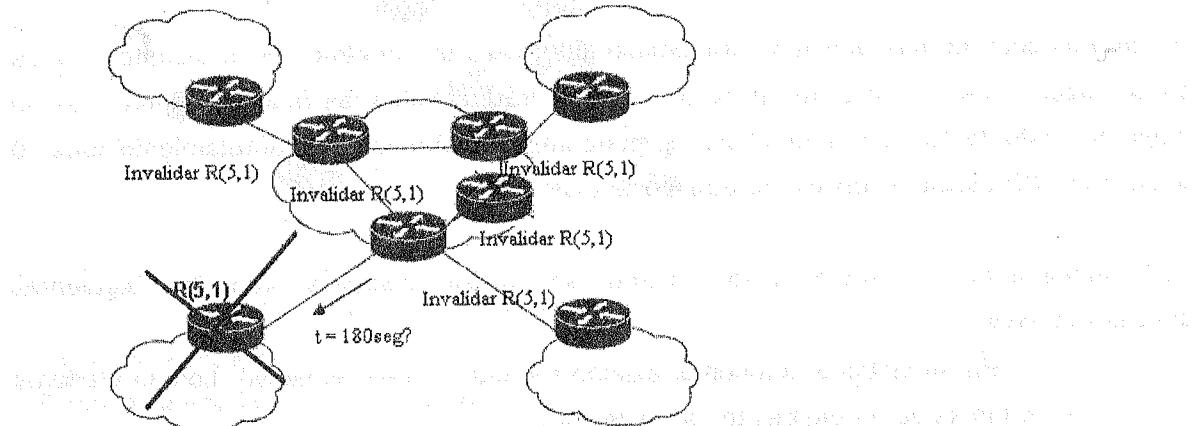


Fig. 6.9 Falla de Enlace RIP

6.5.2 Protocolo OSPF (Open Shortest Path First) (RFC 2178)

Es un protocolo de enrutamiento de estado de enlace. Con OSPF un router construye el mapa de la topología de la subred o AS, enviando periódicamente información de enrutamiento a todos los demás routers del AS (no solo a sus vecinos), luego localmente corre el algoritmo de Dijkstra para determinar el camino más corto a todas las redes. El costo del enlace individual es configurado por el administrador de la red de acuerdo al tipo de servicios requerido. Se permiten múltiples caminos del mismo costo. OSPF utiliza el servicio de transporte TCP.

Una característica importante del OSPF es su habilidad para estructurar jerárquicamente un sistema autónomo AS en áreas. Cada área corre su propio algoritmo estado de enlace, con cada router que retransmite su estado de enlace a los otros routers en el área. Con el Ruteo jerárquico se ahorra el tamaño de las tablas y el tráfico de actualización es reducido.

En una estructura jerárquica se identifican cuatro tipos de router OSPF:

- Routers Internos. Solo realizan enrutamiento intra AS.
- Routers de Area. Pertenecen al Area y al Backbone.
- Routers de Backbone. Realizan el enrutamiento dentro del backbone.
- Routers de frontera. Intercambian información de enrutamiento con routers de otro AS.

En la siguiente figura se muestra un ejemplo de una estructura jerárquica de los routers.

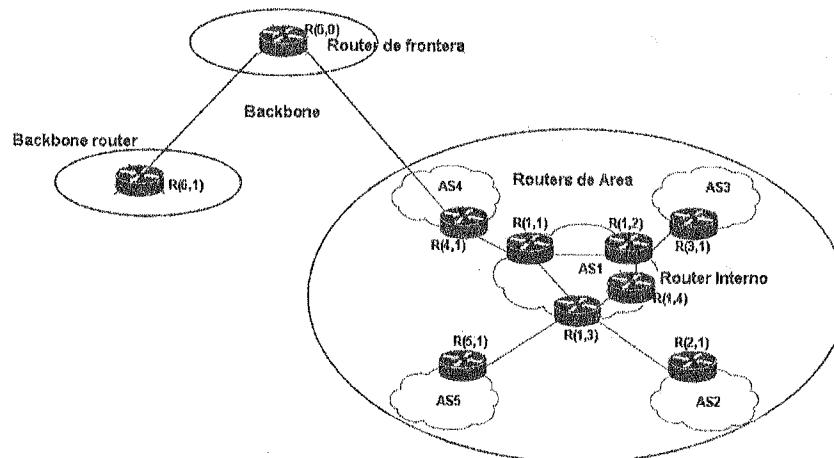


Fig. 6.10 OSPF Jerárquico

6.5.3 Protocolo BGP (Border Gateway Protocol) (RFC 1771-1773)

Es el protocolo de enrutamiento inter AS por defecto de la Internet. Por ejemplo, los ISP registrados en Internet suelen componerse de varios sistemas autónomos. Actualmente entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. El algoritmo de enrutamiento que utiliza, se parece al Vector Distancia, aunque en lugar de propagar información de costo, propaga información de la Ruta, como secuencias de regiones AS de una ruta al AS destino u otra información basándose en las políticas de la red.

Sea la red de la anterior figura, con el protocolo BGP se describe la secuencia de AS del router R(0,0) al router R(5,1):

$$\text{Ruta}(R(0,0), R(5,1)) = R(0,0), R(4,1), R(1,1), R(1,3), R(5,1)$$

El intercambio de información de enrutamiento entre dos routers que utilizan el protocolo BGP tiene lugar en la conexión o sesión que se establece entre los dos routers. Para crear un entorno fiable, el protocolo BGP utiliza el servicio de transporte TCP.

6.6 CONCEPTOS Y TERMINOS CLAVE

Algoritmo de Bellman-Ford

Algoritmo de Dijkstra

Algoritmo de Enrutamiento

AS

BGP

Conteo al infinito

Direccionamiento con subredes

Direcciones IP

Inter AS

Intra AS

IP

IPv4

Máscara de red

Máscara de subred

OSPF

Protocolos de Enrutamiento

RIP

Servicios capa Red

Tabla de Ruteo

Tabla Distancia

6.7 PREGUNTAS DE REPASO

1. La dirección IP 130.114.23.4 tiene como dirección de red:
 - A. 130.114.0.0
 - B. 130.114.23.0
 - C. 255.255.255.0
 - D. 130.0.0.0
2. Los algoritmos de enrutamiento donde en cada nodo se produce un proceso iterativo de intercambio de información con vecinos, se denominan:
 - A. Algoritmos dinámicos
 - B. Algoritmos de estado de enlace
 - C. Algoritmos vector distancia
 - D. Algoritmos estáticos
3. Los algoritmos de enrutamiento donde cada nodo tiene la información completa de la topología de la red, se denominan:
 - A. Algoritmos dinámicos
 - B. Algoritmos de estado de enlace
 - C. Algoritmos vector distancia
 - D. Algoritmos estáticos
4. Indicar cuando ocurre un error en el router, utilizando el algoritmo de Vector Distancia:
 - A. Cada nodo calcula solo su propia tabla
 - B. Un nodo puede avisar un costo de enlace errado
 - C. El nodo puede advertir costos de caminos incorrectos
 - D. Nunca
5. Indicar cuando ocurre un error en el router, utilizando el algoritmo Estado de Enlace:
 - A. El nodo puede advertir costos de caminos incorrectos
 - B. La tabla de cada nodo es usada por otros
 - C. Un nodo puede avisar un costo de enlace errado
 - D. Nunca
6. En el ruteo jerárquico
 - A. Todos los routers son iguales
 - B. Los routers conforman una red plana
 - C. Se agregan routers en regiones
 - D. Ninguno

7. Cual protocolo permite obtener la dirección IP automática y dinámicamente
- A. RIP
 - B. DHCP
 - C. ICMP
 - D. ARP
8. En la capa de red, cual es el manejo que se da a los paquetes o datagramas
- A. Entrega a la subred
 - B. Reenvío al siguiente router
 - C. Encaminamiento del origen al destino
 - D. Todos los anteriores
9. Cual es la función de los protocolos de enrutamiento
- A. Identificar los hosts de origen y de destino a través de un código o número
 - B. Actualizar las tablas de enrutamiento que se consultan
 - C. Asignar un código físico correspondiente a la la tarjeta de comunicación
 - D. Dotar de control al protocolo IP
10. Cual es la máscara de la siguiente dirección IP 10.1.3.21
- A.255.0.0.0
 - B.255.225.0.0
 - C.10.1.3.0
 - D. 255.255.255.0
11. Dada la dirección IP 10.128.3.21/9 determinar la dirección de red
- A. 10.128.3.0
 - B.10.9.3.0
 - C.10.128.0.0
 - D.10.128.3.21
12. A que se denomina Sistema Autónomo AS
- A. Un grupo de redes y routers independientes
 - B. Un grupo de redes y routers bajo la autoridad de una única administración.
 - C. Una red privada sin conexión a Internet
 - D. Ninguno de los anteriores

CAPITULO 6: LA CAPA DE RED

13. A cuales routers involucra el protocolo Intra AS
 - A. A los routers de la misma área
 - B. A los routers de otra áreas
 - C. A routers que se encuentran en la frontera con otras áreas
 - D. A routers organizados jerárquicamente

14. Indicar un protocolo interAS
 - A. Protocolo de Información de Enrutamiento (RIP)
 - B. Protocolo de pasarela exterior (EGP)
 - C. Protocolo de Primero el camino más corto (OSPF)
 - D. Ninguno de los anteriores

15. Cual es la métrica que utiliza el protocolo RIP
 - A. El número de enlaces (redes) necesarios para alcanzar el destino.
 - B. El costo del enlace
 - C. El ancho de banda
 - D. El rendimiento del canal

6.8 TALLER

Leer el artículo ipj9_1.pdf (Working with IP Addresses) ipj8-4pdf (Testing Routing Protocols) de la revista The Internet Protocol Journal (<http://www.cisco.com>)

1. Determinar la dirección de red y sus respectivas máscaras de los sgtes. Números IP
 - a. 150.23.34.70/16
 - b. 200.40.20.50/21
 - c. 100.117.141.239/7
 - d. 149.20.119.13/17

2. Sea el segmento de red



- a. Cuantas PC's soporta este segmento sin desperdiciar el espacio de direccionamiento.
- b. Determinar la máscara de red para este segmento (está relacionado al inciso a).
- c. Supongamos que se quiere instalar 25 PC's, cuál es la máscara a utilizar
- d. Con la máscara del inciso c. Cuál es el máximo número de equipos que se pueden instalar.

3. Sean las figuras

Fig 1.

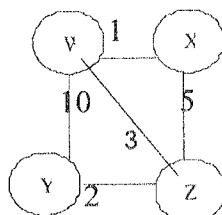
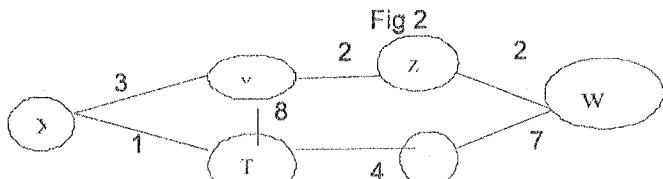


Fig 2



- a. Hallar las tablas de Distancia y de Ruteo de la fig 1 para el nodo Y, utilizando el algoritmo de Vector Distancia.
- b. Si el enlace YW se actualiza con el valor 8, actualizar las tablas de sus vecinos.
- c. Aplicar el Algoritmo de Dijkstra a la Red de la fig.2
- d. Separar en regiones las redes de la fig 1 y fig 2 y construir sus tablas de enrutamiento.

CAPITULO 7 LA CAPA DE ENLACE

Objetivos de Aprendizaje: *Al concluir el capítulo, usted será capaz de:*

- *Conocer los servicios de la capa de Enlace*
- *Comprender las técnicas de detección de errores*
- *Conocer y comprender los protocolos de acceso múltiple*

7.1 SERVICIOS DE LA CAPA DE ENLACE

El contexto general de la capa de Enlace, está referido a los servicios que realiza dentro del modelo de referencia TCP/IP para el estudio de redes que son el control de enlace de datos y el control de acceso al medio. En el primero de los aspectos mencionados:

- Se administra la notificación y detección de errores (control de errores), la topología de red y el control de flujo. También se realiza la entrega segura entre dos dispositivos físicamente conectados, que pueden ser: host-router, router-router, host-host.

El control de acceso al medio consiste en:

- Suministrar acceso a los medios de la red encapsulando los datagramas en tramas (Entramado), añadiendo cabecera.
- Utilizar la "dirección física" en la cabecera de la trama para identificar el fuente y el destino y suministra tránsito de datos confiable a través de un enlace físico utilizando direccionamiento plano o dirección MAC (Control de acceso al medio) diferente de la dirección IP.

El control de error incluye tanto la detección como la corrección de error. Permite al receptor informar al emisor de las tramas perdidas o dañadas en la transmisión y coordina la retransmisión de estas tramas por parte del emisor. En la capa de Enlace, el término control de error, se refiere principalmente a los métodos de detección de error y de retransmisión.

Como ya dijimos en la capa de Transporte, el control de flujo coordina la cantidad de datos que se pueden enviar antes de recibir una confirmación y es una de las tareas más importantes de la capa de Enlace.

La capa de Enlace combina el trámado, control de flujo y control de error a través de los protocolos a nivel de software. Estos pueden ser usados en canales sin ruido (libres de error pero ideales, como el HDLC (High-level Data link Control).

Actualmente millones de usuarios de Internet que necesitan conectar sus computadoras de su domicilio a un servidor de un proveedor de servicios Internet usan el protocolo Punto a Punto.

La capa de Enlace está implementada en una tarjeta o adaptador de red que abarca desde el enlace físico de la red al intercambio de tramas por ejemplo entre un host y un router como en la figura gracias a los protocolos de comunicación de esta capa.

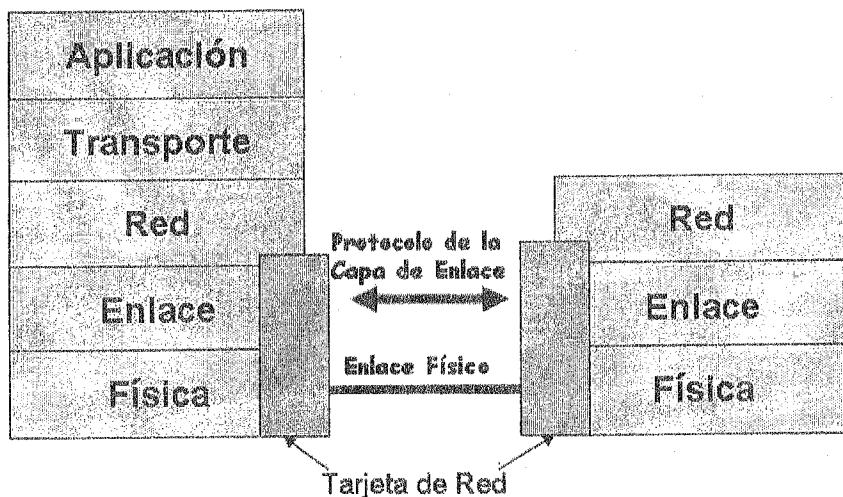


Fig. 7.1 Contexto de la capa de Enlace

7.2 TÉCNICAS DE DETECCIÓN DE ERRORES

Las redes deben ser capaces de transferir datos desde un dispositivo a otro con total exactitud, es decir, que los datos recibidos sean idénticos a los transmitidos. Estos últimos pueden ser corrompidos por errores físicos como el ruido en la línea.

Los errores físicos de la transmisión de datos, son notificados y detectados por los protocolos de la capa de Enlace que utilizan varias técnicas, que tienen en común añadir información de redundancia (r) a la secuencia de bits de datos (m), para formar lo que se denomina una *palabra código* (n):

$$n = m + r$$

Donde r puede estar al final o entre los valores de m .

Dada una palabra código que se transmite (n_T), la técnica de detección, evaluará este código en el receptor (n_R), si son diferentes, se habrá detectado un error y la técnica sirve, caso contrario el resultado es incierto.

Si $n_T \neq n_R$ entonces se detecta un error

7.2.1 Verificación del Bit de Paridad

Que consiste en añadir un bit adicional de paridad al extremo derecho del elemento transmitido para detectar errores individuales. Este bit puede ser de paridad par o impar dependiendo si se quiere completar la paridad o imparidad respectivamente de los bits con valor 1 transmitidos.

Ejemplo 7.1

Determinar el bit de paridad para la siguiente secuencia de bits transmitido:

$m = 0110101000110101$.

Solución

En este caso el valor del bit de paridad es 0, por existir un número par de valores en 1. Luego n_T será 01101010001101010

Para un número impar de errores de ráfaga la técnica de verificación de paridad lo detecta, es decir: si en el lado del receptor la secuencia de bits transmitidos mas el bit de paridad no tienen el mismo valor, la técnica lo detecta, por ejemplo, sea $n_R = 01001010001101011$. Como $n_T \neq n_R$ entonces la técnica detecta el error.

Con la función lógica Distancia Hamming (d), se puede corregir el error. Esta se define como *el número de valores de bits en 1 de la función XOR de dos palabras código*

Al aplicar $d(n_T, n_R)$ se obtiene el valor del bit alterado y su posición en la secuencia.

Ejemplo 7.2

Aplicar la función Hamming para corregir error en el anterior ejemplo.

Solución

01101010001101010 XOR 01001010001101011

Obtenemos: 00100000000000001

Luego es el tercer bit, contando de izquierda a derecha que hay que corregir.

Esta misma técnica es válida en dos dimensiones, para un conjunto de i secuencias de bits se obtiene la paridad de fila $m_{i,j+1}$ para cada secuencia y la paridad de columna $m_{i+1,j}$ en las posiciones de los j bits de las secuencias.

$m_{1,1}$	$m_{1,2}$	$m_{1,3}$	$m_{1,4}$	$m_{1,j}$	$m_{1,j+1}$
$m_{2,1}$	$m_{2,2}$	$m_{2,3}$	$m_{2,4}$	$m_{2,j}$	$m_{2,j+1}$
.....						
$m_{i,1}$	$m_{i,2}$	$m_{i,3}$	$m_{i,4}$	$m_{i,j}$	$m_{i,j+1}$
$m_{i+1,1}$	$m_{i+1,2}$	$m_{i+1,3}$	$m_{i+1,4}$...	$m_{i+1,j}$	$m_{1,j+1}$

Tabla 7.1 Tabla de bits de paridad de dos dimensiones

7.2.2 Código de Bloques

En esta codificación, se divide el mensaje en bloques de k-bits (se cambia el 0 por 1 y el 1 por 0). Permite corregir errores de 1 bit y detectar errores de 2 bits y la posición de éstos. Los demás errores de múltiples bits o error de ráfaga pasan inadvertidos.

Sea el código (n,k)

Donde n es el número de dígitos de la palabra código y k es el número de dígitos fuente.

Los bits de redundancia ocupan las posiciones de bits que sean potencias de 2. Estos completan los dígitos fuente. Para obtener sus valores, se suman con aritmética módulo 2, los dígitos correspondientes a las posiciones de bits que tienen como valor binario 1. Luego ya se puede formar la palabra código correspondiente.

En el receptor se efectúa una operación similar. Se suman los números binarios que corresponden a las posiciones de bits que tienen 1 binario incluyendo los bits de redundancia o verificación. Si no hubo errores de un bit, la suma módulo 2 será cero.

Ejemplo 7.3

Sea la secuencia de origen de 7 bits: 1001101. Determinar la palabra código transmitida.

Solución

Se requieren 4 bits de redundancia. Luego el código de bloque es $(11,7)$. Los bits de redundancia ocupan las sgtes posiciones: 1, 2, 4, 8 (múltiplos de 2). Luego las posiciones de los bits en la palabra código son:

11	10	9	8	7	6	5	4	3	2	1
1	0	0	X	1	1	0	X	1	X	X

Para obtener los bits de verificación, se suman módulo 2 los que tienen 1 binario

$$11 + 7 + 6 + 3 == 1011 + 0111 + 0110 + 0011 = 1001$$

Así la palabra código transmitida es:

11	10	9	8	7	6	5	4	3	2	1
1	0	0	1	1	1	0	0	1	0	1

En el receptor se efectúa la operación similar, se suman los números que tienen 1 binario incluyendo los bits de verificación, si no hubo errores de un bit (individuales) la suma módulo 2 será cero.

$$11 + 8 + 7 + 6 + 3 + 1 = 1011 + 1000 + 0111 + 0110 + 0011 + 0001 = 0000$$

7.2.3 Codigo de redundancia Ciclica (CRC)

Los códigos de redundancia cíclica, también conocidos como códigos polinomiales constituyen el método de detección de errores empleado en redes LAN o WAN. Se utiliza con esquemas de transmisión orientados a tramas (o bloques). Permiten sustanciales mejoras en fiabilidad respecto a los métodos anteriores, siendo a la vez una técnica de fácil implementación.

El método se basa en el uso de aritmética polinomial módulo 2 (No hay acarreos en la sustracción ni en la adición y las operaciones suma, resta y OR-exclusivo coinciden). La trama a transmitir –de n bits – representa un polinomio $P(x)$ de coeficientes binarios. La idea consiste en añadir una secuencia de k bits, al final de la trama, de manera que la secuencia de $k+n$ bits resultante constituya los coeficientes de un polinomio divisible de forma exacta por un polinomio $G(x)$ determinado previamente por emisor y receptor. Cuando el receptor recibe la trama realiza la división entre $G(x)$, si el resto es distinto de cero ha ocurrido un error de transmisión.

Imponiendo condiciones bastante simples sobre los polinomios divisores es posible detectar un gran número de errores. Existen tres polinomios $G(x)$ que se han convertido en estándares internacionales:

CRC 12	$X^{12} + X^{11} + X^3 + X^2 + X + 1$
CRC16	$X^{16} + X^{15} + X^2 + 1$
CRC-CCITT	$X^{16} + X^{12} + X^5 + 1$

Algoritmo para calcular la redundancia del CRC

Sea r el grado de $G(x)$. Agregar r bits cero al extremo de orden inferior de la trama $P(x)$ de tal manera que ahora contenga $m+r$ bits y corresponde a $x^r P(x)$

- Dividir la serie de bits correspondientes a $x^r P(x)$ entre la serie de bits correspondientes a $G(x)$, empleando la división en módulo 2.
- El resto de esta división se añade a la trama original $P(x)$ para constituir el CRC.
- En el receptor dividir CRC entre G. Si el resto es diferente de cero, se detecta error.

Ejemplo 7.4

Determinar el código CRC para el mensaje $M = 11111000001$

con el polinomio generador $G(x) = x^4 + x^3 + x^2$

Solución

Como el grado de $G(x)$ es 4, se añaden 4 ceros a la izquierda de $M \rightarrow M'$ y se divide módulo 2 los coeficientes de M' entre G .

$111110000010000 \mid 11110$

El resto de esta división (0100) se añade al mensaje M para constituir el

CRC = 111110000010100

7.3. CREACIÓN DE TRAMAS

La capa de Enlace, requiere empaquetar los bits en tramas, de forma que una trama se pueda distinguir de otra. El entramado separa un mensaje desde un origen a un destino, o de otros mensajes a otros destinos, añadiendo la dirección del emisor y la dirección del destinatario que define donde debe ir el paquete; la dirección del emisor ayuda al receptor a notificar la recepción.

Normalmente no se envía todo el mensaje en una trama, se divide en tramas pequeñas, para evitar que un error de transmisión afecte a todo el mensaje.

Las tramas pueden ser de tamaño fijo o variable. En las redes LAN se utilizan tramas de tamaño variable donde es necesario definir el final de una trama y el principio de la siguiente.

Se han establecido técnicas para dividir el flujo de datos en tramas. Algunas son las siguientes:

- Conteo de caracteres. El 1er. Campo de la cabecera indica el número de caracteres de la trama
- Inserción de caracteres de relleno. Secuencia de caracteres ASCII Data Link Escape y el inicio de texto (D.LE STX). Y terminar con la secuencia (D.LE ETX)
- Banderas de inicio y final.
 - Cada trama comienza y termina con un patrón de bits
 - Siempre que la capa de Enlace transmisora encuentre cinco unos consecutivos en los datos, automáticamente inserta un bit con valor 0 en el flujo de salida de datos.
 - Cuando el receptor ve cinco bits, de entrada con valor 1, seguido del bit con valor 0, elimina el bit 0.

Muchos protocolos de Enlace utilizan la combinación de conteo de caracteres con uno de los otros métodos para tener seguridad extra.

El formato de una trama de longitud variable y la explicación de algunos campos es:

Inicio de Trama	Dirección MAC	Tipo/longitud	Datos	FCS	Fin de Trama
-----------------	---------------	---------------	-------	-----	--------------

Fig. 7.2 Formato de trama

La dirección MAC (Media Access Control address o dirección de control de acceso al medio) es un identificador de 48 bits que corresponde de forma única a una tarjeta de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits)

El campo de Secuencia de verificación de trama (Frame Check Sequence FCS) contiene un número calculado por el computador origen y se basa en los datos de la trama. Cuando el computador destino recibe la trama, vuelve a calcular el número FCS y lo compara con el número FCS que se incluye en la trama. Si los dos números son distintos, se ha producido un error, se descarta la trama y se le pide al origen que vuelva a realizar la transmisión.

Hay tres formas principales para calcular el número de Secuencia de verificación de trama:

- Verificación por redundancia cíclica (CRC):
- Paridad de dos dimensiones:
- Checksum Internet

7.4. PROTOCOLOS DE ACCESO MÚLTIPLE

Los canales de comunicación que conectan a los nodos de una red (host o router) pueden ser de tres tipos:

- Punto-a-punto (un solo cableado, por ejemplo: PPP, SLIP). Donde el canal está dedicado a un par de usuarios.
- Compartido (radio, satélite, algunas redes LAN)
- Conmutado (Ejemplo., switched Ethernet, ATM)

En un canal punto a punto, un nodo transmite por el canal de comunicación disponible. Sin embargo, surgen los problemas cuando se tiene que compartir un solo canal entre varios nodos de una red. La regulación del tráfico está a cargo de los protocolos de acceso múltiple.

Cuando M nodos quieren transmitir, cada uno envía a un promedio de C/M . Es totalmente descentralizado, no hay un nodo especial que coordine la transmisión, sin sincronización de clocks, slots.

Las características de un protocolo de acceso múltiple son:

- Algoritmo distribuido que determina como las estaciones comparten un canal, por ejemplo, determinar cuando un nodo puede transmitir.
- La comunicación sobre compartir el canal también debe usar el canal
- Se busca la eficiencia y robustez a errores del canal.

Las estrategias o técnicas del acceso múltiple a un canal son tres: Partición del Canal, Acceso al azar y acceso por turnos. En la primera, se divide el canal en partes mas pequeñas (división de tiempo, frecuencia) de manera que se asigna una parte para uso exclusivo de un nodo. Luego en el acceso al azar se permiten colisiones y se determina como recuperarse de estas colisiones. Finalmente la tercera estrategia establece la forma de lograr un acceso coordinado y evitar colisiones.

Si la carga es baja, es eficiente la técnica de acceso al azar porque un solo nodo puede utilizar completamente el canal. Caso contrario, es preferible compartir el canal cuando la carga es alta. La técnica de acceso por turnos, busca combinar ambos extremos, buscando siempre la eficiencia.

7.4.1 Partición del Canal

El canal de comunicación podrá estar disponible, durante un rango de tiempo, de frecuencia o si se asigna a cada usuario una porción del ancho de banda para una fracción de tiempo. Entonces, la técnica se subdivide respectivamente en: División de tiempo, de frecuencia y de código.

Estas técnicas conocidas también como libres de conflictos estáticos, están diseñadas para asegurar el éxito de la transmisión y que no interfiera ninguna otra transmisión. Son tres: TDMA, FDMA y CDMA. En las dos primeras, no se produce solapamiento entre las porciones del canal que son asignados a los usuarios. En las figuras, tomaremos como referencia a 3 usuarios.

a) Acceso Múltiple por División de Tiempo (TDMA)

En TDMA (time division multiple access) todo el ancho de banda es utilizado por cada usuario en un periodo de tiempo; durante el cual el usuario puede transmitir libremente y todos los recursos del sistema son dedicados a él, ineficiente con carga liviana y usuarios de ciclos bajos. La desventaja es que quedan espacios no usados e inactivos.

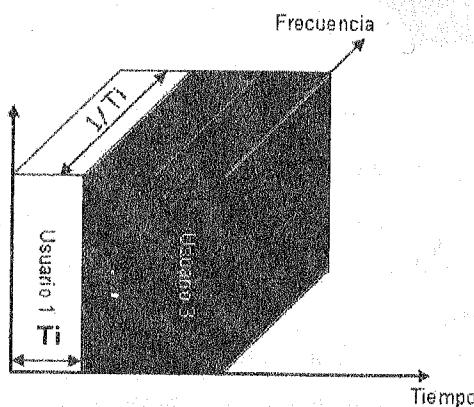


Fig. 7.3 Técnica TDMA

b) Acceso Múltiple por División de Frecuencia (FDMA)

La técnica FDMA (Frequency Division multiple access) consiste en dividir el espectro del canal en bandas de frecuencia. Cada usuario tiene asignada una banda fija durante todo el tiempo. La principal ventaja es su simplicidad, ya que no requiere ninguna coordinación o sincronización entre los usuarios, éstos pueden usar su propia banda de frecuencia sin interferir con los demás.

La desventaja es que se produce un tiempo de transmisión no usado en las bandas de frecuencia.

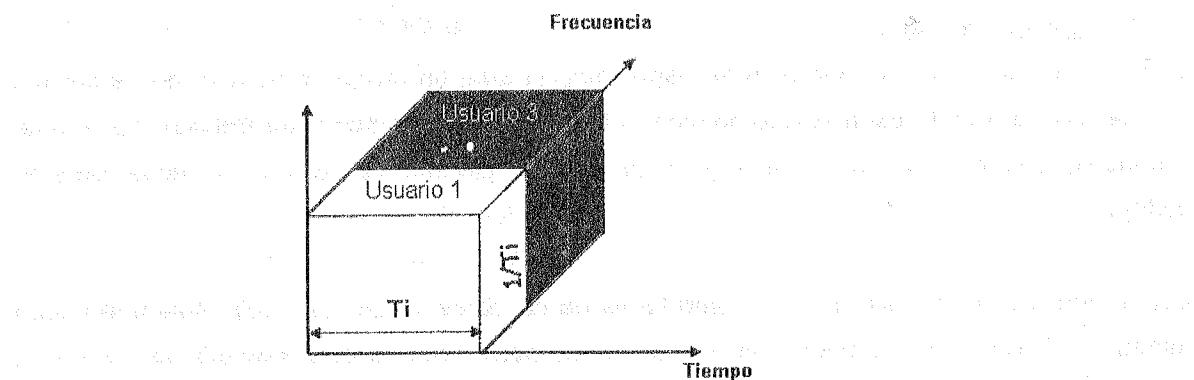


Fig. 7.4 Técnica FDMA

c) Acceso Múltiple por División de Código (CDMA)

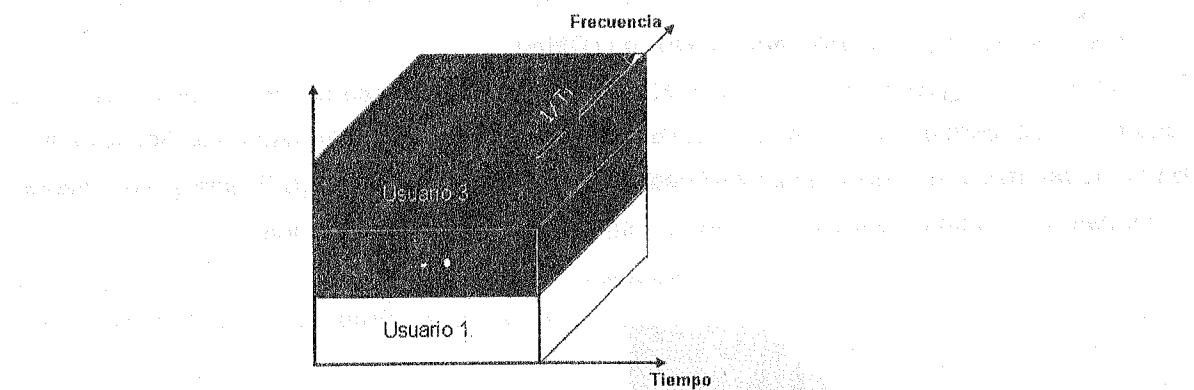


Fig. 7.5 Técnica CDMA

Código único asignado a cada usuario, usado mayormente en canales inalámbricos (celular, satélite, etc). Todos los usuarios comparten la misma frecuencia pero cada usuario tiene su propia secuencia para codificar los datos:

Señal codificada = (datos originales) \times (secuencia, saltos)

decodificación: producto interior de señal codificada y secuencia de saltos

Permite a múltiples usuarios coexistir y transmitir simultáneamente con mínima interferencia (si los códigos son ortogonales), es decir, solapamientos de transmisión en los dominios de tiempo y frecuencia. Los códigos deben ser ortogonales, es decir:

Sea $\langle ei, ej \rangle$ el producto interno de dos códigos distintos

$$\langle ei, ej \rangle = 0$$

$$\langle ei, ei \rangle = 1$$

$$\langle ei, (-ei) \rangle = -1$$

Ejemplo 7.5

Sean $e_1 = (1,0,0)$, $e_2 = (0,1,0)$ y $e_3 = (0,0,1)$ tres códigos. Determinar el código que llega al receptor.

Solución

Sea $\langle e_1, e_2 \rangle$ el producto interno de e_1, e_2 :

$$\langle e_1, e_2 \rangle = \langle (1,0,0), (0,1,0) \rangle = 1 \times 0 + 0 \times 1 + 0 \times 0 = 0$$

$$\langle e_1, e_1 \rangle = \langle (1,0,0), (1,0,0) \rangle = 1 \times 1 + 0 \times 0 + 0 \times 0 = 1$$

$$\langle e_1, -e_1 \rangle = \langle (1,0,0), (-1,0,0) \rangle = 1 \times (-1) + 0 \times 0 + 0 \times 0 = -1$$

Luego, una señal codificada de transmisión será igual a:

$$S_{i,j} = d_i e_j \quad j=1,2,3$$

Donde d_i es el slot de transmisión $\in \{1, -1\}$

$$S_{1,1} = d_1 e_1 = 1 (1,0,0) = (1,0,0)$$

$$S_{1,2} = d_1 e_2 = 1 (0,1,0) = (0,1,0)$$

$$S_{-1,1} = d_{-1} e_1 = -1 (1,0,0) = (-1,0,0)$$

$$S_{-1,2} = d_{-1} e_2 = -1 (0,1,0) = (0,-1,0)$$

En el lado del receptor, se va a recuperar el slot de transmisión, realizando el producto interno de la señal y el código:

$$d_2 = \langle S_{1,1}, e_1 \rangle = \langle (1,0,0), (1,0,0) \rangle = 1$$

$$d_1 = \langle S_{-1,1}, e_1 \rangle = \langle (-1,0,0), (1,0,0) \rangle = -1$$

7.4.2 Protocolos de acceso al azar

En este grupo de protocolos, ningún nodo o estación es superior a otro y ninguno tiene asignado el control sobre otro. El nodo transmisor siempre transmite a la máxima capacidad del canal, cuando lo hacen dos o más nodos simultáneamente, se producen colisiones, cada nodo afectado retransmite su trama hasta que se lo recibe correctamente. Esta retransmisión no es necesariamente inmediata, sino que hay una demora aleatoria.

Ningún nodo permite o impide a otro enviar datos. En cada instante, un nodo que tiene datos para enviar utiliza un procedimiento definido por el protocolo para tomar la decisión de enviar o no. Esta decisión depende del medio (ocupado o vacío).

Ejemplos de protocolos de acceso al azar son: ALOHA dividido, ALOHA puro, CSMA y CSMA/CD.

a) ALOHA puro

Es el protocolo básico de la familia de protocolos Aloha donde llegan tramas de acuerdo a una distribución estadística de Poisson, el nodo la transmite en su totalidad sin sincronización, si colisiona con otras tramas se retransmite más tarde con una probabilidad p . De otra manera, el nodo espera un tiempo para la transmisión de la trama. Luego de esta espera, la transmite con una probabilidad p o espera por otra trama con una probabilidad $1-p$.

$P(\text{éxito de } N \text{ nodos}) = P(\text{enviar un número medio de tramas durante el tiempo de transmisión de una trama})$

$$= N p(\text{éxito de 1 nodo})$$

$$\begin{aligned} P(\text{éxito de 1 nodo}) &= P(\text{nodo transmite}) \times \\ &\quad P(\text{ningún otro nodo transmite en } [p_{0-1}, p_0]) \times \\ &\quad P(\text{ningún otro nodo transmite en } [p_0, p_{0+1}]) \\ &= p \cdot (1-p) \cdot (1-p) \end{aligned}$$

$$P(\text{éxito de } N \text{ nodos}) = N p \cdot (1-p) \cdot (1-p)$$

Optimizamos el valor de p como n tal que tienda a infinito

$$\begin{aligned} \lim_{n \rightarrow \infty} N n(1-n)(1-n) &= 1/(2e) = 0.18 \end{aligned}$$

Luego la máxima productividad es 0.18. Es decir, el 18% de estas tramas alcanza el destino con éxito.

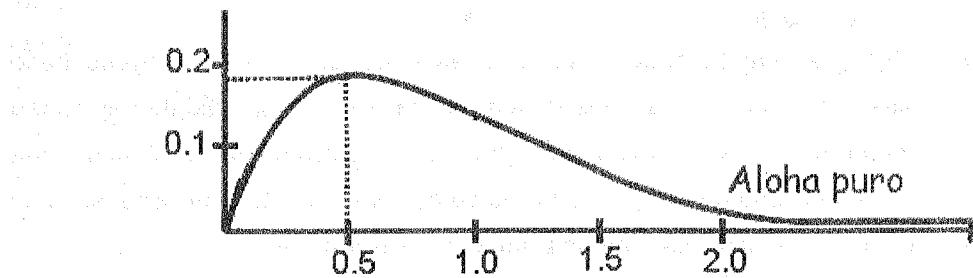


Fig. 7.6 Distribución de tramas Aloha puro

En la siguiente figura, la trama enviada durante un tiempo t_0 , colisiona con otras enviadas antes ($t_0 - 1$) y después ($t_0 + 1$)

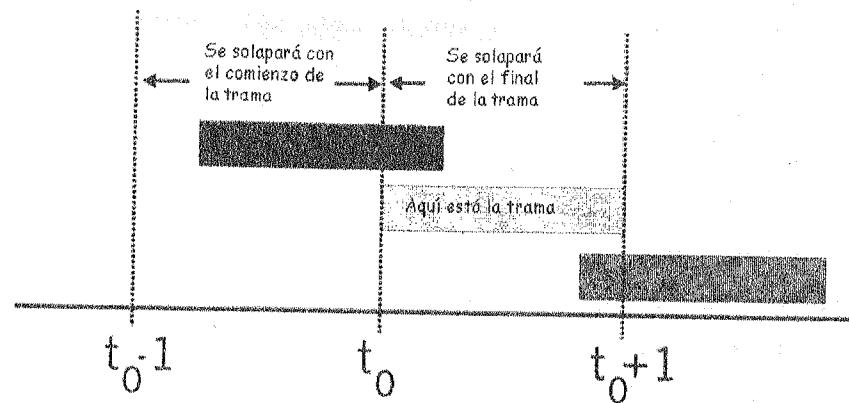


Fig. 7.7 Colisión de tramas

b) ALOHA Dividido o ALOHA con Ranuras

Para mejorar el servicio de Aloha Puro, se definió Aloha Dividido, que es una variación de la primera, con un canal dividido en slots o ranuras de tiempo. El tamaño del slots es igual a la duración de la transmisión de una trama.

Los nodos empiezan a transmitir tramas solo al principio del slot, los nodos están sincronizados de tal manera que cada nodo conoce cuando el slot comienza.

Si dos o más tramas colisionan en un slot, entonces todos los nodos detectan la colisión, aún antes que termine el slot. El nodo retransmite su trama en los siguientes slots con probabilidad p hasta que la trama haya sido transmitida sin colisión. Si no hay una colisión, el nodo no retransmite la trama, sino se prepara para transmitir la siguiente trama.

Ejemplo 7.6

Sean tres nodos que quieren transmitir. Los posibles estados de los slots son: (E) éxito, (C) Congestión, (V) Vacío, mostrar una posible situación en cada uno de los nodos.

Solución

en la figura se muestra.

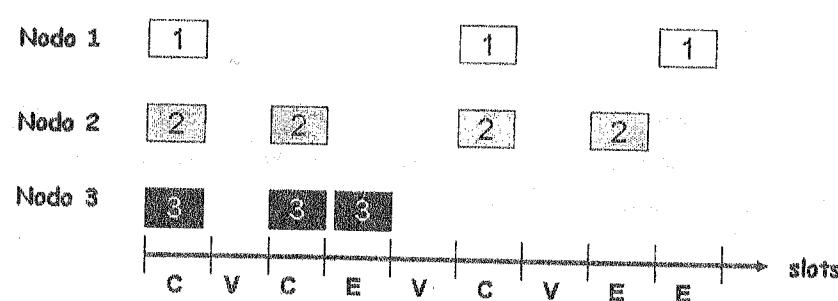


Fig. 7.8 Aloha Dividido

Suponga que N nodos tienen tramas para enviar. Cada uno transmite en el slot con probabilidad p de transmisión exitosa S si:

por un solo nodo: $S = p(1-p)^{N-1}$

por cualquiera de los N nodos

$$S = \text{Prob}(\text{uno solo transmite})$$

$$= Np(1-p)^{N-1}$$

Optimizamos el valor de p como n tal que tienda a infinito

$$= \lim_{n \rightarrow \infty} Nn(1-n)^{N-1}$$

$$= 1/e = 0.37, N \rightarrow \infty$$

Luego, la productividad máxima es 0.37. Es decir, el 37% de estas tramas alcanza el destino con éxito.

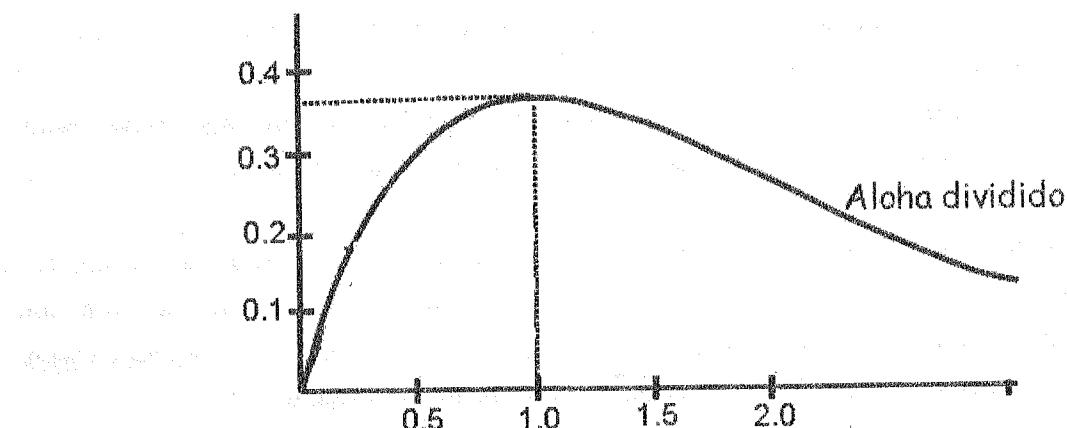


Fig. 7.9 Distribución de tramas Aloha Dividido

c) CSMA (Carrier Sense Multiple Access)

En los protocolos de comunicación humana, cuando el modelador de un seminario otorga la palabra a una persona, debe cuidar que nadie le interrumpa hasta que termine su participación. Si al mismo tiempo dos personas quieren hablar, el modelador solo otorga la palabra a una de ellas.

De manera análoga para reducir la posibilidad de colisiones, se desarrolla el método CSMA donde si el canal escuchado está libre: transmite la trama entera. Si se encuentra ocupado, difiere la transmisión para más tarde, de dos formas:

- CSMA Persistente: reintentar inmediatamente con probabilidad p cuando el canal esté libre (puede causar inestabilidad)

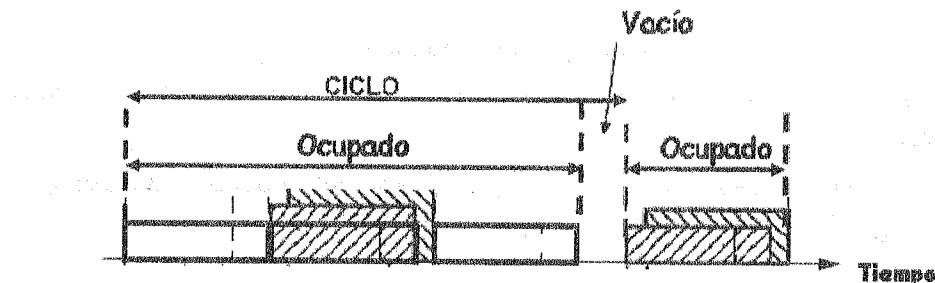


Fig. 7.10 CSMA Persistente

- CSMA No-Persistente: reintentar después de un intervalo s aleatorio

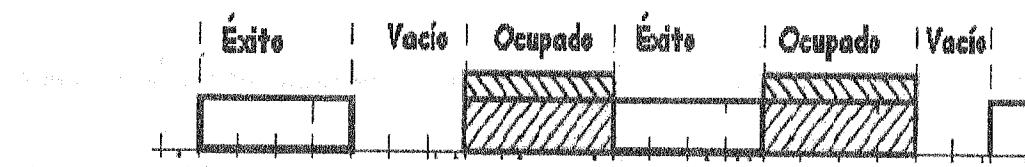


Fig. 7.11 CSMA No-persistente

d) CSMA/CD (Carrier Sense Multiple Access)/(Collision Detection)

Esta técnica mejora a Aloha Dividida en un entorno de una LAN Ethernet donde los nodos están conectados por un canal compartido.

Sus características son:

- La tarjeta de red o adaptador empieza a transmitir en cualquier momento, siempre que ningún adaptador esté transmitiendo.
- Escucha antes de transmitir
- Usa detección de colisiones. Cuando se producen, se cancela la transmisión, reduciendo el no uso del canal.
- Un adaptador espera un tiempo al azar antes de empezar a transmitir. Este tiempo es más corto comparado con el tiempo necesario para transmitir una trama.

7.4.3 Protocolos de acceso controlado

Los nodos consultan unos con otros para determinar cual nodo tiene derecho a enviar. Un nodo no puede enviar, a no ser que haya sido autorizado por los otros nodos.

Este grupo de protocolos, cumple con las siguientes propiedades:

1. Cuando un solo nodo está activo, la cantidad de información procesada por unidad de tiempo (*throughput*) es de R bps.
2. Cuando N nodos están activos, entonces cada nodo tiene un *throughput* de R/N bps
3. Son protocolos libres de conflictos dinámicos.

a) Protocolo de Elección (Polling)

Un nodo es elegido como "nodo maestro", éste invita a nodos esclavos a transmitir un número máximo de tramas según su turno, empezando del primer nodo, luego el siguiente y así sucesivamente de manera cíclica. El nodo maestro determina cuando un nodo ha terminado de enviar, observando la falta de señal en el canal.

Este protocolo elimina las colisiones y los slots vacíos, permitiendo tener mayor eficiencia.

Pero tienen dos desventajas:

Se introduce un tiempo de demora en la elección, el tiempo requerido para notificar que puede transmitir.

Si el nodo maestro falla, todo el canal no es operable.

b) Protocolo de Ficha de Control

También denominado Paso de testigo, los nodos en la red se organizan en un anillo lógico. Es decir, para cada nodo hay un sucesor y un predecesor. Aquí se introduce una pequeña trama de propósito especial o ficha de control (token), que es intercambiada entre los nodos. Cuando un nodo recibe un token del predecesor, se lo queda solo si tiene tramas que transmitir, de otra manera, se reenvía el token al siguiente nodo sucesor.

Este protocolo es descentralizado y tiene una alta eficiencia. Sin embargo, también tiene problemas, como por ejemplo la falla de un nodo puede inhabilitar todo el canal o que un nodo no devuelva el token de manera accidental.

7.5 CONCEPTOS Y TERMINOS CLAVE

Acceso Múltiple por División de Código (CDMA)
Acceso Múltiple por División de Frecuencia (FDMA)
Acceso Múltiple por División de Tiempo (TDMA)
ALOHA Dividido
ALOHA Puro
Código de bloques
Código de redundancia cíclica
CSMA
CSMA/CA
CSMA/CD
Dirección MAC
FCS
Palabra código
Partición del canal
Protocolo de Elección (Polling)
Protocolo de ficha de control
Protocolos de Acceso al Azar
Protocolos de Acceso Múltiple
Protocolos de acceso por turnos
Servicios de la capa Enlace
Técnicas de detección de errores
Trama
Verificación de bit de paridad

7.6 PREGUNTAS DE REPASO

1. El código de paridad par de la siguiente secuencia 10111001 es:
 - A. 101
 - B. 1
 - C. 0
 - D. 11

2. La capa de Enlace se divide en:
 - A. La subcapa de LLC y MAC
 - B. La subcapa MAC
 - C. La subcapa MAC y Control de Error
 - D. No se subdivide en capas

3. El control de acceso al medio utiliza un número para identificar a los equipos conectados físicamente. Este número es:
 - A. El número MAC
 - B. El número IP
 - C. Un número de 48 bits configurado por el administrador de la red.
 - D. Variable dependiente de la norma de cableado.

4. El control de acceso al medio consiste en:
 - A. suministrar el tránsito de datos confiable a través de un enlace físico
 - B. Evitar el acceso de personas no autorizadas
 - C. Colocar un firewall al ingreso de la red
 - D. Control de flujo de paquetes

5. La capa de enlace está implementada en :
 - A. El número IP
 - B. El equipo servidor
 - C. El router principal de la red
 - D. Una tarjeta o adaptador de red.

6. La detección de colisiones de CSMA/CD son difíciles en redes:
 - A. Telefónicas
 - B. Inalámbricas
 - C. Ethernet
 - D. Token Ring

CAPITULO 7: LA CAPA DE ENLACE

7. Cuales son los servicios que brinda la capa de Enlace
 - A. El control de enlace de datos y El control de acceso al medio
 - B. El control de acceso al medio y la seguridad de la red
 - C. El control de acceso de usuarios y el control de acceso al medio
 - D. El enrutamiento y el control de enlace de datos
8. A que se refiere el control de enlace de datos
 - A. Administrar la notificación y detección de errores
 - B. Suministrar tránsito de datos confiable a través de un enlace físico
 - C. Realizar la entrega segura entre dos dispositivos físicamente conectados
 - D. A y C
9. A que se refiere el control de acceso al medio
 - A. Administrar la notificación y detección de errores
 - B. Suministra tránsito de datos confiable a través de un enlace físico
 - C. Realizar la entrega segura entre dos dispositivos físicamente conectados
 - D. A y C
10. La capa de Enlace empaqueta los bits en:
 - A. Datagramas
 - B. Tramas
 - C. Segmentos
 - D. Bytes
11. De cuales tipos pueden ser los canales de comunicación que conectan a los nodos de una red.
 - A. Punto a Punto, Comutado, Abiertos
 - B. Comutado, Punto a Punto
 - C. Compartido, Comutado, Punto a Punto
 - D. Punto a Punto, Multipunto, Cerrado
12. Indicar una característica de Protocolo de Acceso Múltiple
 - A. Delimitar la cantidad de usuarios del canal a compartir
 - B. Realizar el reenvío de las tramas
 - C. Administrar la detección de error
 - D. Determinar cuando un nodo puede transmitir

13. El acceso al azar es una técnica de:
- Detección de errores
 - Acceso múltiple a un canal
 - Elección de trama
 - Acceso al servicio de red
14. En el ALOHA puro, el nodo que transmite una trama que acaba de llegar:
- Sincroniza con el receptor
 - No espera para transmitir otra trama
 - No sincroniza con el receptor
 - Ninguno de los anteriores
15. En el ALOHA Dividido, el nodo que transmite una trama que acaba de llegar:
- Sincroniza con el receptor
 - No espera para transmitir otra trama
 - No sincroniza con el receptor
 - Ninguno de los anteriores

7.7 TALLER

Leer el capítulo 10 de la 1ra. Parte (The data link Layer) del libro Network Essentials de Zacker Craig

1. Sea la siguiente secuencia de bits 11011100010111001 que representa un flujo de datos, y su función generadora $G(x) = x^7 + x^6 + x^4 + x^3 + x + 1$. determinar el Código de Redundancia Cíclica.
2. Sea el código CDMA (1,-1,1,1,-1,-1,1-1) con bit de datos $d_1 = -1$ $d_0 = 1$ Obtener la salida del codificador y los bits de datos que le llegan al receptor. Desarrollar.
3. Sea una red con 5 nodos. Si cada nodo transmite con una probabilidad de 1/5. Hallar la probabilidad de transmisión exitosa para un nodo y para cualquiera de los 5 nodos si se utiliza:
 - a) Aloha Dividido
 - b) Aloha Puro
4. Como se puede evitar que las transmisiones que realizan varias computadoras que están compartiendo el mismo medio de red produzcan colisión de paquetes.

CAPITULO 8 LA CAPA FISICA

Objetivos de Aprendizaje: Al concluir el capítulo, usted será capaz de:

- Describir las señales analógicas y las digitales.
- Establecer las características de los canales de comunicación
- Comprender los problemas en la transmisión de datos y los recursos disponibles para afrontarlos.
- Tener los criterios técnicos para utilizar algún medio de comunicación en el cableado de una red.

8.1 SEÑALES ANALÓGICAS Y DIGITALES

El término "señal" se refiere a un voltaje eléctrico, un patrón luminoso o una onda electromagnética modulada que se desea obtener. Las transmisiones se realizan mediante estas señales electromagnéticas de diferente tipo. Estas señales pueden ser continuas (analógicas) o discretas (digitales).

8.1.1 Señales Analógicas

Se define una señal analógica como aquella en la que la intensidad de la señal varía suavemente en el tiempo, como por ejemplo, el canto de un pájaro que es respondido por otro. En este caso, la señal toma valores continuos a medida que se mueve en forma de una onda de un extremo a otro de la comunicación.

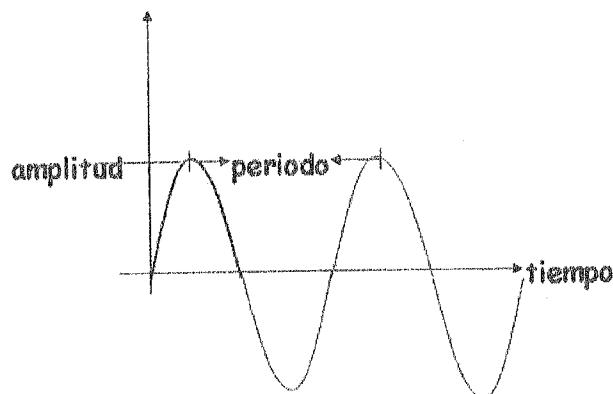


Fig. 8.1 Señal Analógica

Una señal analógica tiene las siguientes características:

- Es ondulatoria.
- Su amplitud o profundidad de la onda
- Su periodo (T). Tiempo necesario para completar un ciclo.
- Su frecuencia es la razón (en ciclos por segundo o Hertzios) a la que la señal se repite. ($f = 1/T$)
- Tiene un voltaje que varía continuamente en función del tiempo.
- Señal capaz de tomar todos los posibles valores en un determinado rango.
- Es típica de los elementos de la naturaleza
- Se refiere a información que es continua .

Ejemplo 8.1

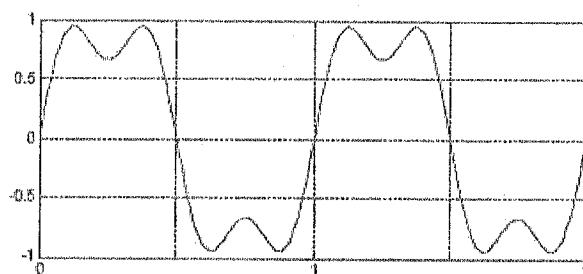
La frecuencia de una señal es de 150 Hertzios. Determinar su periodo.

Solución

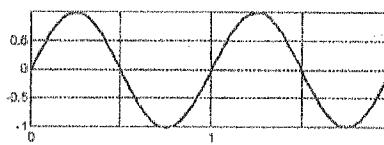
De la ecuación de la frecuencia, despejamos el periodo.

$$T = 1/f = 1/150 \text{ seg} = 0.00667 \text{ seg} = 0.00667 \times 10^{-3} \mu\text{seg} = 6.67 \mu\text{seg}$$

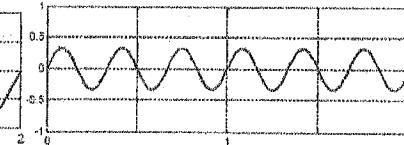
Las señales analógicas pueden ser *simples u onda seno* y *compuestas* formadas por múltiples ondas seno como se muestra en la siguiente figura. Una onda seno no puede ser descompuesta en señales más simples. Una onda seno de frecuencia única, no es útil para transmitir datos; es necesario usar una señal compuesta, por ejemplo en las gráficas siguientes $f(t)$ está compuesta por $g(t)$ y $h(t)$.



$$f(t) = \sin(2\pi f_1 t) + \frac{1}{3} \sin(2\pi(3f_1)t)$$



$$g(t) = \sin(2\pi f_1 t)$$



$$h(t) = \frac{1}{3} \sin(2\pi(3f_1)t)$$

Fig. 8.2 Señales Compuestas

Cuando todas las componentes tienen frecuencias múltiplo de una dada, esta se denomina frecuencia fundamental. El periodo de la señal suma de componentes es el periodo correspondiente a la frecuencia fundamental.

Se denomina *ancho de banda* al rango de frecuencias contenido en una señal compuesta, donde se concentra la mayor parte de la energía de la señal. En otras palabras, es la diferencia entre la frecuencia más alta y la más baja contenidos en la señal.

Ejemplo 8.2

Si se descompone una señal periódica en las siguientes ondas simples 300, 200,700,100,500 Hz.

Determinar su ancho de banda.

Solución

La frecuencia más alta es 700 Hz y la más baja 100 Hz. Luego su diferencia es el ancho de banda:

$$700 - 100 = 600 \text{ Hz}$$

8.1.2 Referencia al Análisis de Fourier

Jean Baptiste Fourier hizo un descubrimiento muy importante en el campo de las matemáticas. Probó que cualquier señal compuesta está constituida por una combinación de señales simples o *armónicos*, con distintas frecuencias, amplitudes y fases que se representa en la siguiente expresión:

$$G(t) = 1/2c + \sum a_n \sin(2\pi nft) + \sum b_n \cos(2\pi nft)$$

donde $f=1/T$ representa la frecuencia fundamental y a_n , b_n son las amplitudes de los diferentes armónicos. Esta expresión se conoce como serie de Fourier.

8.1.3 Señales Digitales

Se define una señal digital como aquella en que la intensidad de la señal se mantiene constante durante un determinado intervalo de tiempo, tras el cual la señal cambia a otro valor constante.

Una señal digital tiene las siguientes características:

- Tienen una amplitud fija
- Puede tomar un número finito de valores, por ejemplo valores binarios.
- La intensidad se mantiene constante durante un intervalo de tiempo, luego del cual la señal cambia a otro valor constante.
- Es típica de la tecnología
- Se pueden aproximar utilizando ondas analógicas

- La tasa de bits, es el número de bits enviados en un segundo, está expresado en bits por segundo (bps).
- La tasa de señal o de pulsos, es el número de elementos de señal enviados en 1 segundo, está expresado en baudios.

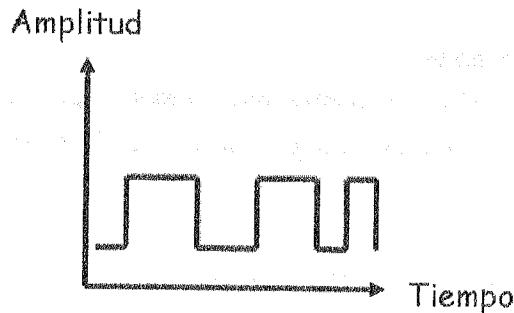


Fig. 8.3 Señal Digital

Ejemplo 8.3

Calcular la tasa de bits para una señal en la cual 15 bits duran 30 microsegundos

Solución

$$\text{Tasa de bit} = 15 \text{ bits} / 30 \text{ (bit}/\mu\text{seg}) = \frac{1}{2} (1/10^{-6}) \text{ bps} = 0,5 \cdot 10^6 \text{ bps} = 500 \text{ kbps}$$

8.2 TRANSMISIÓN DIGITAL

La señalización se logra enviando por ejemplo impulsos eléctricos de cero voltios para el 0 binario y 5 voltios para el 1 binario, se requiere la sincronización a fin de designar cuantos bits estarán representados por un periodo de voltaje continuo. Por ejemplo, sea la secuencia de bits 10100101. Su representación es:

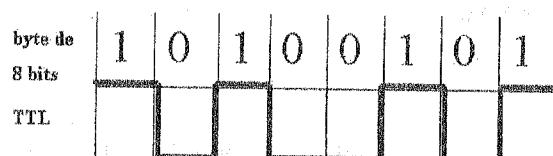


Fig. 8.4 Ejemplo de secuencia de bits

La señal codificada se denominada TTL (Transistor-Transistor Logic)

8.2.1 Codificación Manchester

Un bit "0" representa una señal alta durante la primera mitad del período y baja durante la segunda mitad. Las normas definen al bit "1" como una señal que es baja para la primera mitad del período y alta para la segunda mitad.

8.2.2 Codificación Manchester diferencial

Un bit "1" se representa por la ausencia de un cambio de polaridad al principio del tiempo del bit, y un bit "0" se representa por un cambio de polaridad al principio del tiempo del bit.

Ejemplo 8.4

Codificar la secuencia de bits 10100101 en TTL, Manchester y Manchester Diferencial.

Solución

Estas señales codificadas para el ejemplo se muestran en la siguiente figura:

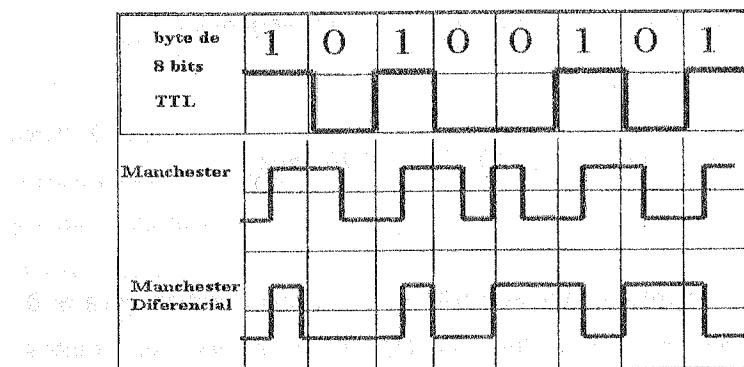


Fig. 8.5 Codificación de Señales

8.3 CARACTERÍSTICAS DEL CANAL

8.3.1 Propagación de la señal

Cuando una tarjeta NIC emite voltaje o pulsos luminosos en un medio físico, ese pulso rectangular, formado por ondas, se desplaza, o se propaga, a través del medio. Propagación significa que un bloque de energía, que representa 1 bit, se desplaza desde un lugar hacia otro. La velocidad a la cual se propaga depende del material que se usa en el medio, de la geometría (estructura) del medio y de la frecuencia de los pulsos. El tiempo que tarda el bit en desplazarse desde un extremo a otro del medio y nuevamente en regresar se denomina tiempo de ida y vuelta, (RTT).

Suponiendo que no se producen más demoras, el tiempo que tarda el bit en desplazarse a través del medio hasta el extremo más lejano es $t = RTT/2$.

Luego la ecuación de la velocidad de propagación en función del desplazamiento (x) y del tiempo de propagación t será:

$$\text{velocidad} = x/t \rightarrow t = x/\text{velocidad}$$

Ejemplo 8.5

Determinar el tiempo de ida y vuelta que tarda en desplazarse un bit que se propaga a 100 metros/seg en una distancia de 15000 Kms. Asuma que la velocidad de propagación en el cable es de $2,4 \times 10^8$ m/s.

Solución

Para el cálculo del tiempo de propagación utilizamos la expresión

$$t = 15000 \times 10^3 \text{ m} / (2,4 \times 10^8 \text{ m/s}) = 15 / (2,4 \cdot 10^2 \text{ s}) = 6,25 \cdot 10^{-2} \text{ s}$$

$$\text{Luego RTT} = t/2 = 6,25 \cdot 10^{-2} \text{ s} / 2 = 3,125 \cdot 10^{-2} \text{ s}$$

8.3.2 V_elocidad de Transmisión

Es el número de elementos de señal o cambios de condición por segundo. Se mide en baudios, que son el número de elementos de señal por segundo que se transmiten.

La velocidad de los datos depende de tres factores:

- El ancho de banda disponible
- Los niveles de señal que se usan
- La calidad del canal (nivel de ruido)

Se han desarrollado dos fórmulas teóricas para calcular la tasa de datos; la de Nyquist para un canal sin ruido y la de Shannon para un canal ruidoso.

a) Canal sin ruido

La fórmula de la tasa de bits de Nyquist define la máxima velocidad teórica para un canal sin ruido en los siguientes términos:

$$\text{Velocidad máxima de datos} = \text{tasa de bits (bps)} = 2 \times \text{ancho de banda} \times \log_2 M$$

Donde M es el número de niveles discretos de señal usados para representar los datos.

Si se incrementa los niveles de la señal, reduce la fiabilidad del sistema.

b) **Canal con ruido**

Si existe ruido, se mide por la relación de Shannon entre la potencia de la señal y la potencia del ruido, o relación señal/ruido. La relación señal-ruido (SR) se define como:

$$SR = \frac{\text{Potencia media de la señal}}{\text{Potencia media del ruido}}$$

Una SNR alta indica que la señal está menos corrompida por ruido,

Una SNR baja indica que la señal está muy corrompida por ruido,

Para expresar SR en decibelios, se recurre a la relación:

$$SNR_{dB} = 10 \log_{10} SR$$

Para determinar la máxima tasa de datos teórica de un canal, se tiene la expresión:

$$\text{Capacidad}_{(bps)} = \text{Ancho de banda} \times \log_2 (1 + SR)$$

En esta expresión, no hay indicación del nivel de señal, es decir, no se puede conseguir una velocidad mayor que la capacidad del canal.

Ejemplo 8.6

Calcular la capacidad del canal de un CD ROM que tiene un ancho de banda de 20 KHz si la razón señal-ruido es 2500.

Solución

$$SNR_{dB} = 10 \log_{10} SR = 10 \log_{10} 2500 = 34 \text{ dB}$$

$$C = 20000 \log_2 (1 + 2500) = 20000 \log_2 (2501) = 20000 \times 11.3 = 226000 = 226 \text{ kbps}$$

Ejemplo 8.7

Sea un canal con un ancho de banda de 3000 Hz y SNR de 20 dB. Cual es la capacidad del canal.

Solución

De la expresión de la capacidad del canal:

$$(C) = \text{ancho de banda} \log_2 (1 + SR) \text{ bps}$$

$$SNR = 10 \log_{10} (SR)$$

$$20 = 10 \log_{10} (SR) \rightarrow SR = 100 \quad C = 19,963 \text{ bps}$$

8.3.3 Ancho de Banda

Este término se puede usar en dos contextos diferentes:

- Como la medida de la cantidad de información (bits) que puede fluir desde un lugar hacia otro, a través de un espacio, en un período de tiempo determinado. Medido en bits por segundo (bps).
- Como el rango de valores de frecuencia que pueden tener las señales a transmitir a través de ese medio de transmisión, ya sean de carácter eléctrico o electromagnético. Medido en herzios.

El ancho de banda tiene las siguientes características:

- Es finito y su demanda crece constantemente. Por muy grande que sea el rango de valores que tenga, éste tiene un límite y cada vez son más usuarios que lo demandan.
- Su uso eficiente puede ahorrar dinero.
- Representa el canal para acceder a Internet. El usuario comprenderá su importancia por la facilidad o dificultad que tenga al acceder a Internet.
- Es un factor del rendimiento de la red, como describimos a continuación.

Al ancho de banda se lo compara analógicamente con el grosor de una tubería, con la capacidad de flujo de una autopista o a la calidad de sonido de un sistema de audio.

8.3.4 El Rendimiento

El rendimiento (throughput) mide lo rápido que se pueden enviar datos realmente a través de una red. El ancho de banda es el factor más importante, pero no el único en su determinación. Por ejemplo para la red Internet además se deberá considerar:

- la hora del día que se conecta,
- el backbone al que está conectado que usará unas rutas específicas de Internet que determinan como se enrutarán los paquetes dentro la red,
- los tipos de datos que se transmiten,
- el procesador y memoria interna del computador,
- la cantidad de usuarios de la LAN que están conectados mientras se descarga un archivo específico.

Por lo mencionado, el rendimiento a menudo es mucho menor que el ancho de banda digital máximo posible del medio que se está usando,

Al diseñar una red, es importante tener en cuenta el ancho de banda teórico. La red no será más rápida que lo que los medios permiten. Al trabajar con redes reales, deberá medir el rendimiento y decidir si éste es adecuado para el usuario.

8.4. PROBLEMAS EN LA TRANSMISIÓN DE DATOS

Un bit en el medio físico puede propagarse (desplazarse) o sufrir una serie de perturbaciones o deterioros en su transmisión que pueden debilitar la señal, interferir con otras señales o ser fuente generadora de errores en la transmisión. Estos son: Atenuación, Reflexión, Ruido y Colisiones.

8.4.1 Atenuación

Atenuación es la pérdida de la fuerza de la señal como, por ejemplo, cuando los cables superan una longitud máxima. En otros términos, es la relación entre la potencia de la señal a la entrada del canal de transmisión y la potencia que tiene esta señal a la salida del canal expresada en decibelios [dB]. Es decir:

$$\text{Atenuación} = 10 \times \log_{10} \frac{\text{Potencia en la entrada}}{\text{Potencia a la salida}} [\text{dB}]$$

Esto significa que una señal de voltaje de 1 bit pierde amplitud a medida que la energía pasa desde la señal hacia el cable. La selección cuidadosa de los materiales y la geometría (la forma y el posicionamiento de los cables) puede disminuir la atenuación eléctrica. Es inevitable que se produzca un cierto nivel de pérdida cuando hay resistencia eléctrica presente. La atenuación también se produce en las señales ópticas, la pérdida de señal es inevitable.

La atenuación puede afectar a una red dado que limita la longitud del cableado de la red a través de la cual se puede enviar un mensaje.

Generalmente un canal presenta distintas atenuaciones a señales de distintas frecuencias, haciendo que determinadas frecuencias apenas se propaguen por el canal.

Esto hace también que el ancho de banda se reduzca a medida que aumenta la longitud del canal, debido a que también aumenta la atenuación de la señal. Por ello, en ocasiones se expresa el ancho de banda del canal por cada 100 m o cada km de longitud.

El límite no viene impuesto por el tipo de cable utilizado que tiene un ancho de banda mucho mayor, sino por los amplificadores que se insertan en la línea para contrarrestar el fenómeno de atenuación de la misma y poder transmitir la señal a larga distancia. Por esto es que en la anterior expresión de la atenuación, si la señal se ha atenuado la expresión es negativa y si se ha amplificado, es positiva.

Ejemplo 8.8

Un canal de transmisión entre dos Equipos de Transmisión de datos consta de 3 secciones. La 1ra introduce una Atenuación de 6 dB, la 2da una atenuación de 12 dB y la 3ra Una Amplificación de 2 dB. Si el nivel de potencia transmitido es de 400 mW Calcular el nivel de potencia de Salida medio del canal.

$$\text{Atenuación Global} = 6 + 16 - 2 = 20$$

$$20 = 10 \log_{10} \frac{\text{P}_{\text{Salida}}}{\text{P}_{\text{Entrada}}} \quad \text{Luego: } 100 = \frac{\text{P}_{\text{Salida}}}{\text{P}_{\text{Entrada}}}$$

$$\text{SRx} = 4 \text{ mW}$$

Una de las formas que existen para resolver el problema es cambiar el medio. Otra de las formas es utilizar un repetidor luego de una distancia determinada. Existen repetidores para bits eléctricos, ópticos e inalámbricos.

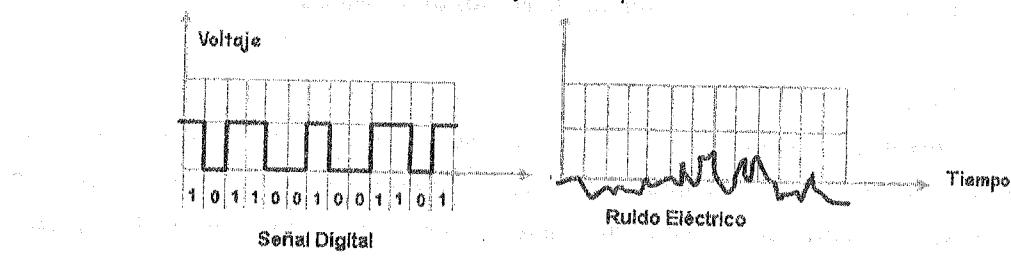
8.4.2 Ruido

Son adiciones no deseadas desde varias fuentes a las señales de voltaje, ópticas o electromagnéticas que se insertan entre el emisor y el receptor, por lo que ninguna señal se produce sin ruido.

Demasiado ruido puede corromper un bit, haciendo que un 1 binario se transforme en un 0 binario, o un 0 en un 1, destruyendo el mensaje. Es el mayor problema en la transmisión de datos. Puede clasificarse en:

- Ruido térmico: producido en todos los componentes electrónicos y en los cables.
- Ruido de intermodulación: debido al medio de transmisión que provoca la presencia de señales electromagnéticas que interfieren.
- Diafonía: producido por la proximidad física de un cable que provoca una inducción magnética de señal.
- Ruido impulsivo: producido por chispas y motores de combustión que producen una señal interferente de un espectro muy grande.

En la siguiente figura, se ilustra el efecto del ruido eléctrico que se produce en una señal digital que se incorpora entre el emisor y el receptor:



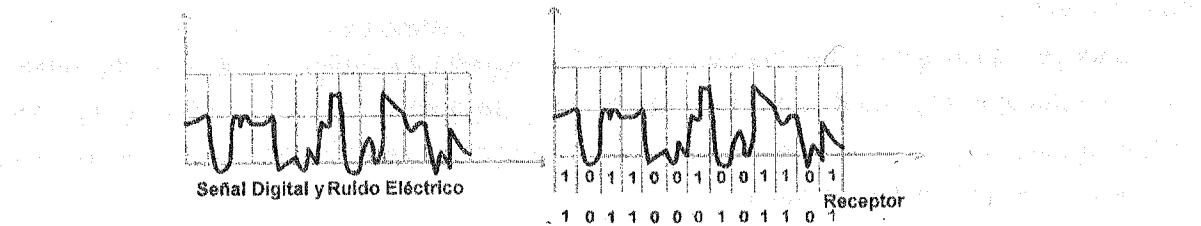


Fig. 8.6 Efecto del ruido eléctrico

8.4.3 Colisiones

Una colisión se produce cuando dos bits de dos computadores distintos que intentan comunicarse se encuentran simultáneamente en un medio compartido. Algunas tecnologías como, por ejemplo, Ethernet, se encargan de un determinado nivel de colisiones, administrando los turnos para transmitir en el medio compartido cuando se produce una comunicación entre hosts. En algunos casos, las colisiones son parte normal del funcionamiento de una red. Sin embargo, un exceso de colisiones puede hacer que la red sea más lenta o pueden detenerla por completo. Por lo tanto, una gran parte del diseño de una red se refiere a la forma de reducir al mínimo y localizar las colisiones.

8.4.4 Dispersión

La Dispersión es cuando la señal se ensancha con el tiempo. Esto se produce debido a los tipos de medios involucrados. Si es muy grave, un bit puede comenzar a interferir con el bit siguiente y confundirlo con los bits que se encuentran antes y después de él, creándose un desfase.

8.5. MEDIOS DE TRANSMISIÓN DE DATOS

Son los recursos que utilizan las redes para transportar los flujos de bits de una máquina a otra. Determina la velocidad de datos y el ancho de banda del canal. Según su naturaleza pueden ser:

- Guiados: Proporcionan un cable conductor, cable trenzado, cable coaxial, fibra óptica
- No guiados o Inalámbricos. Transportan ondas electromagnéticas sin usar un conductor físico. Ejemplo: radio, satélite, infrarrojo, microondas

8.5.1 Cable Coaxial

El cable coaxial consta de un alambre de cobre en su parte central o núcleo. Este se encuentra rodeado por un material aislante. A su vez, el material aislante está recubierto por un conductor que suele presentarse como una malla trenzada. Por último, dicha malla está recubierta por una capa de plástico protector. De este diseño en forma de capas concéntricas es de donde se deriva el nombre.

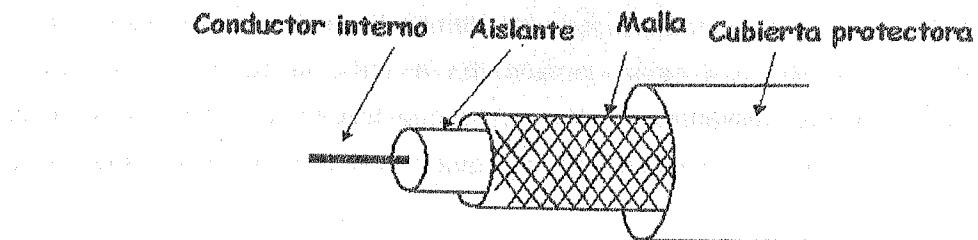


Fig. 8.7 Estructura del Cable Coaxial

El cable coaxial ya dejó de ser el cable más utilizado en cableado de redes. Entre sus características están:

- Bajo costo
- Velocidad de 10 a 100 Mbps
- Longitud máxima del cable de 500 metros.

Los problemas de conexión que tiene el cable coaxial son:

- El ruido eléctrico que interfiere con la transmisión de señales sobre medios de red.
- Su dificultad de manipulación para el cableado.

8.5.2 Cable Trenzado

En su forma más simple, consisten de dos cables de cobre aislados dispuestos en forma de espiral para reducir la interferencia eléctrica con respecto a los pares cercanos que se encuentran a su alrededor. Hay dos tipos de cables trenzados:

El par trenzado con blindaje o STP (shielded twisted-pair) y el par trenzado sin blindaje o UTP (unshielded twisted-pair). De estos, el más utilizado es el UTP de 4 hilos debido a su buen comportamiento y bajo costo. Se encuentra normalizado de acuerdo a la norma Americana TIA/EIA-568-B y a la internacional ISO-11801.

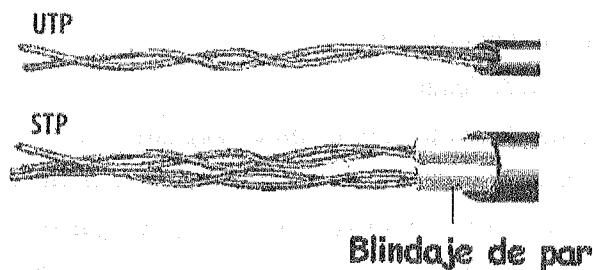


Fig. 8.8 Cable Trenzado

El cable de par trenzado no blindado (UTP) se usa en diversos tipos de redes. Cada uno de los 8 hilos de cobre individuales del cable UTP está revestido de un material aislador. Además, cada par de hilos está trenzado. Este tipo de cable se basa sólo en el efecto de cancelación que producen los pares trenzados de hilos.

Es de fácil instalación y es más económico que los demás tipos de medios para uso de redes. Sin embargo, la ventaja real es su tamaño. Es el más rápido entre los medios basados en cobre. Entre sus desventajas están su susceptibilidad al ruido y la longitud máxima de un cable UTP es de 100 metros sin un equipo adicional como repetidor de la señal.

Los estándares o categorías más utilizadas son:

- Categoría 5: actualmente no reconocido por TIA/EIA. Frecuentemente usado en redes ethernet, fast ethernet (100 Mbit/s) y gigabit ethernet (1000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 100 MHz. Uso: redes LAN.
- Categoría 5e: Extensión de la categoría 5. Minimiza ruido e interferencia magnética. Actualmente definido en TIA/EIA-568-B. Frecuentemente usado en redes fast ethernet (100 Mbit/s) y gigabit ethernet (1000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 100 MHz.
Uso: Redes LAN.
- Categoría 6: actualmente definido en TIA/EIA-568-B. Usado en redes gigabit ethernet (1000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 250 MHz. Uso: redes LAN.

8.5.3 Fibra óptica

El cable de fibra óptica no transporta impulsos eléctricos, a diferencia de otros tipos de medios que usan cables de cobre. Más bien, las señales que representan a los bits se convierten en haces de luz, lo cual es una manera relativamente más segura de enviar datos en relación a las interferencias eléctricas; atenuación más baja.

Un sistema de transmisión óptica tiene 3 componentes:

- el medio de transmisión, es una fibra de vidrio.
- la fuente de luz, es un LED o diodo láser
- el detector, genera un pulso eléctrico cuando recibe un rayo de luz.

El sistema se basa en el principio físico de la refracción. Cuando un rayo de luz pasa de un medio a otro, el rayo se refracta en la frontera entre ambos medios. En general, el ángulo de refracción depende de las propiedades de los medios en contacto, en particular de sus índices de refracción. Si el ángulo de incidencia se encuentra por encima de un determinado valor crítico, la luz se refleja y no sale del medio.

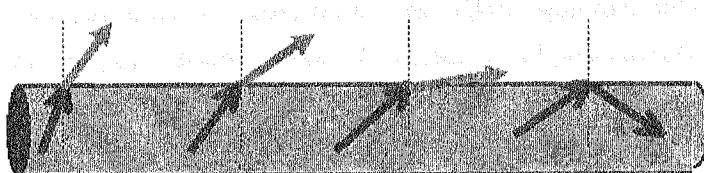


Fig. 8.9 Principio de Refracción

La fibra óptica está compuesta por dos capas de vidrio, cada una con distinto índice de refracción. El índice de refracción del núcleo es mayor que el del revestimiento, razón por la cual, y debido a la diferencia de índices la luz introducida al interior de la fibra se mantiene y propaga a través del núcleo.

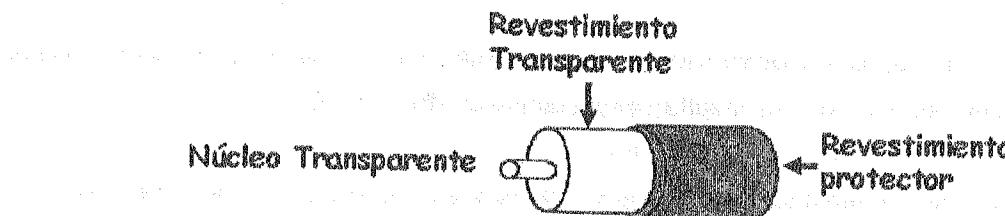


Fig. 8.10 Estructura de la fibra óptica

Dado que cualquier rayo de luz incidente, por encima del ángulo crítico, se reflejará internamente, existirá una gran cantidad de rayos diferentes rebotando a distintos ángulos. A esta situación se la conoce como *fibra multimodo*. Si la luz se propaga en línea recta sin rebotar, se denomina *fibra monomodo*. Las multimodo se usan para distancias cortas (hasta 500 m) y las monomodo para acoplamientos de larga distancia. Debido a que las fibras monomodo son más sensibles a los empalmes, soldaduras y conectores, las fibras y los componentes de éstas son de mayor costo que los de las fibras multimodo.

Las características técnicas de la fibra óptica son:

- Mayor velocidad de propagación de la señal
- Mayor capacidad de transmisión. En la actualidad se pueden hacer transmisiones de hasta 10 Gbps en distancias de 1 km.
- Inmunidad ante interferencias electromagnéticas.
- Menor atenuación. 5 a 20 dB/km a 400 Mhz.
- Mayor ancho de banda.
- Tasas de error menores. 1 error por cada 10^9 bits frente a 1 por cada 10^6 en los cables eléctricos.
- No hay riesgos de cortocircuitos o daños de origen eléctrico.
- Peso mucho menor.
- Se utiliza en redes troncales porque su gran ancho de banda es rentable y en el cableado exterior de una red LAN Fast Ethernet (100 Base-FX) y 1000 Base X.

Sin embargo, también presenta algunas desventajas en relación a otros medios de transmisión:

- La alta fragilidad de las fibras.
- Necesidad de usar transmisores y receptores más caros
- Los empalmes entre fibras son difíciles de realizar, especialmente en el campo, lo que dificulta las reparaciones en caso de rotura del cable.
- No puede transmitir electricidad para alimentar repetidores intermedios.

8.6 MEDIOS NO GUIADOS O INALÁMBRICOS

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

Todas las frecuencias del espectro radioeléctrico pueden ser utilizadas para la transmisión de datos, aunque las microondas resultan especialmente adecuadas.

En aplicaciones de comunicaciones a larga distancia se ha empleado la transmisión por radio de microondas. Las antenas parabólicas se pueden montar sobre torres para enviar un haz de señales a otra antena a decenas de kilómetros de distancia. El sistema es muy usado en transmisiones telefónicas y de video. Cuanto más alta sea la torre mayor es el alcance ya que se propagan fundamentalmente en línea recta.

Las porciones del espectro electromagnético correspondiente a las ondas de radio, microondas, infrarrojo y rayos láser que se muestran en el siguiente cuadro comparativo pueden servir para transmitir información modulando la amplitud, la frecuencia o la fase de las ondas.

ONDAS DE RADIO	MICROONDAS	ONDAS INFRAROJAS Y MILIMETRICAS	RAYOS LASER U ONDAS DE LUZ
Pueden viajar distancias largas y penetrar edificios sin problemas	Se necesitan repetidoras periódicas	No atraviesan los objetos sólidos	No pueden penetrar la lluvia ni la niebla
Omnidireccionales. El Tx y el Rx no tienen que alienarse físicamente	Bidireccionales. Las antenas del Tx y del Rx deben estar muy bien alienados entre sí	El Tx, y el Rx deben estar alienados	Unidireccional.
Requieren de licencia	Requieren de licencia	No requieren de licencia	No requieren de licencia
Usos: comunicaciones interiores y exteriores	Usos: Telefonía de larga distancia, celulares, TV	Uso: Controles remotos, LAN inalámbricas.	Usos: comunicaciones interiores y exteriores.

Cuadro 8.1 Cuadro comparativo de tipos de ondas

En este cuadro el primer ítem (fila) se refiere a la resistencia que ofrecen las ondas a la atenuación de la señal, luego la posición del Transmisor (Tx) y del Receptor (Rx) en la comunicación, en el 3er ítem se encuentra un requerimiento de funcionamiento para los proveedores del servicio en cuanto a si se requiere o no una licencia. Finalmente, los usos que se dan a estos tipos de ondas.

La tecnología inalámbrica también se puede utilizar en la telefonía móvil y en las redes por satélite que son un tipo de comunicación de un punto de la tierra a otro, está constituido por uno o más dispositivos receptor-transmisor (satélites), cada uno de los cuales escucha una parte del espectro, amplificando la señal de entrada y retransmitiendo a otra frecuencia para evitar los efectos de interferencia.

8.7 CONCEPTOS Y TERMINOS CLAVE

- Análisis de Fourier
- Ancho de Banda
- Atenuación
- Cable Coaxial
- Cable Trenzado
- Capacidad del Canal
- Características del Canal 106-109
- Codificación de señales
- Codificación Manchester
- Codificación Manchester Diferencial
- Colisiones
- Comunicación por Satélite
- Dispersión
- Fibra Optica
- Medios de Comunicación
- Medios Inalámbricos
- Problemas en la transmisión de datos
- Propagación de la señal
- Rendimiento de la PC conectada a Internet
- Ruido
- Señales Analógicas
- Señales Digitales
- STP
- Teorema de Nyquist
- UTP
- Velocidad de transmisión

8.8 PREGUNTAS DE REPASO

Cual de las siguientes opciones es una fuente externa de impulsos eléctricos que pueden perjudicar la calidad de las señales eléctricas en un cable ?

- A.Interferencia electromagnética causada por motores eléctricos
- B.Interferencia de la radiofrecuencia causada por motores eléctricos
- C.Impedancia causada por sistemas de radio
- D.Interferencia electromagnética causada por los sistemas de iluminación

2. Como se denomina la condición en que dos bits de dos computadores diferentes que se comunican se encuentran en un medio compartido al mismo tiempo ?

- A.Latencia
- B.Dispersión
- C. Colisión
- D.Obstrucción

3. Cual de las siguientes opciones significa convertir datos binarios en una forma que se pueda transportar a través de un enlace físico de comunicaciones

- A.Codificación
- B.Decodificación
- C.Cifrado
- D.Descifrado

4. Que ocurre con los paquetes que se involucran en una colisión ?

- A.Los paquetes vuelven al lugar de origen
- B.Los paquetes se destruyen bit por bit
- C.Los paquetes siguen viaje hacia el dispositivo destino con sus datos dañados
- D.Ninguna de las anteriores opciones

5. Que se logra mediante el trenzado de los alambres en un cable CAT 5 ?

- A.El cable queda mas delgado
- B.Es más económico
- C.Reduce los problemas de ruido
- D.Permite que 6 pares quepan en el espacio de 4 pares

6. ¿Cómo se denominan todos los materiales de conexión físicos de una red?
- A. Medios de aplicación
 - B. Materiales eléctricos
 - C. Medios de interconexión de red
 - D. Medios de sistema
7. ¿Cuál es una de las ventajas de utilizar cable de fibra óptica en las redes?
- A. Es económico.
 - B. Su instalación es sencilla.
 - C. Es un estándar de la industria y está a la venta en cualquier comercio de artículos electrónicos.
 - D. Proporcionar una velocidad de datos mayor que la de otros cables guiados
8. ¿ Cuál de las siguientes opciones define más correctamente los medios de interconexión de red?
- A. Los cables a través de los cuales pasan los datos
 - B. Los diversos entornos físicos a través de los cuales pasan las señales de transmisión
 - C. Los sistemas informáticos y los cables que forman una red
 - D. Cualquier hardware o software de una red
9. ¿Cuál de las siguientes describe más adecuadamente la atenuación en el medio de transmision?
- A. La señal transmitida llega deformada por la interferencia
 - B. Las señales llegan con menos amplitud
 - C. Las señales se pierden en el medio
 - D. Las señales llegan con ruido
- 10.¿ Cuál es la distancia máxima recomendada para cables UTP categoría 5.
- A. 500 mts
 - B. 2000 mts
 - C. 100 mts
 - D. No hay límite
11. Cual es el tipo de señal que es propio de la naturaleza
- A. Señal Digital
 - B. La transmisión de Datos
 - C. Señal Analógica
 - D. Ninguna de las anteriores

12. Cuales son los factores que intervienen en la propagación de la señal

- A. El material que se usa en el medio
- B. La geometría del medio
- C. la frecuencia de los pulsos
- D. Todos los anteriores

13. La velocidad de datos depende de:

- A. El ancho de banda disponible, los niveles de señal que se usan, la calidad del canal
- B. La frecuencia de los pulsos
- C. Los niveles de señal que se usan
- D. Todos los anteriores

14. Los factores que intervienen en la capacidad de un canal son:

- A. El ancho de banda
- B. La relación señal-ruido
- C. A y B
- D. Ninguno de los anteriores

15. Indicar tres características de las ondas infrarrojas

- A. No atraviesan objetos sólidos, no requieren licencia, el transmisor y el receptor deben estar alienados
- B. No atraviesan objetos sólidos, se necesitan repetidores, requieren licencia
- C. No atraviesan objetos sólidos, se necesitan repetidores, no requieren licencia
- D. No atraviesan objetos sólidos, se necesitan repetidores, unidireccional

8.9 TALLER

1. Sea un canal con una razón de la señal con ruido de 10 dB. Tiene una demora de 15 seg en transferir un archivo de 1 Megabyte. Cual es la tasa de información máxima teórica que se puede obtener.
2. Explique una analogía del ancho de banda (Excluir la analogía con las cañerías o las autopistas).
3. Por que se produce la Latencia. Explicar una causa.
4. Explicar una razón por la cual en la transmisión de datos se elige:
 - a) Cable Coaxial
 - b) Cable UTP
 - c) Cable de Fibra óptica
5. Explique las funciones de una tarjeta de red

CAPITULO 9 SEGURIDAD DE REDES

Objetivos de Aprendizaje: *Al concluir el capítulo, usted será capaz de:*

- *Comprender la importancia de la seguridad de redes*
- *Describir las características de los ataques a redes informáticas*
- *Mostrar las herramientas de una red y sus vulnerabilidades*

9.1 PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA

Según el glosario de la National Security Agency (NSA), el término seguridad es una condición que resulta del establecimiento y mantenimiento de medidas protectivas que aseguran un estado de inviolabilidad de acciones o influencias hostiles. Luego la seguridad informática es el conjunto de medidas protectivas hacia los datos que son procesados por un sistema de computación.

Fenzi (2000) afirma que ningún sistema de computación puede ser completamente seguro, su protección está dirigida a obstaculizar accesos no autorizados al sistema. Esta afirmación la generalizamos al decir que ninguna red de computadoras abierta está inmune de intrusos. Esto lo tomamos como un principio o enunciado a partir del cual desarrollaremos nuestro trabajo.

Cuando ocurre una intrusión la red de computadoras deberá estar provista de varias medidas de defensa o principios de seguridad informática contra ataques a un sistema de computación. Pfleeger (1997) los enuncia: privacidad, integridad, disponibilidad y no repudio que las describimos a continuación:

a) Confidencialidad

La información debe ser leída o copiada únicamente por quienes tienen el derecho o la autoridad de hacerlo. No solo la información global en su conjunto, sino también aquella información a partir de la cual se puede deducir otra de uso confidencial. Para conseguir la confidencialidad de un mensaje, el emisor debe enviarlo cifrado (oculto para personas no autorizadas) y el receptor utilizar una técnica complementaria o descifrado. La Confidencialidad también es conocida como Privacidad.

b) Integridad

La información (datos y programas) debe ser consistente, fiable y protegida contra modificaciones o eliminaciones no deseadas por el propietario de esta información. Por ejemplo, cuando se realizan transacciones financieras por Internet.

c) Disponibilidad

La información debe estar en el momento que el usuario requiera de ella. La falta de disponibilidad no autorizada por el propietario de esa información se denomina denegación de servicio.

d) No repudio

Un emisor no debe ser capaz de negar el envío de un mensaje que efectivamente envió. La carga de la prueba cae sobre el receptor.

9.2 ATAQUES A REDES INFORMÁTICAS

Una red que sufre ataques de intrusos tiene efectos negativos tanto en su funcionamiento normal como un impacto contundente en la organización. Por una parte, el administrador de la red no conoce a ciencia cierta la magnitud del daño producido, la información manipulada o eliminada intencionalmente que finalmente podrá ocasionar la no disponibilidad de los servicios, y por otra parte, el daño a la imagen corporativa de la organización, pérdidas financieras o uso ineficiente de sus recursos.

Los intrusos, crackers o piratas informáticos persiguen diferentes objetivos: el host o la red para participar en un ataque de denegación de servicio, o servirse de un host, comprometerlo para desde ahí poder lanzar otros ataques y ocultar así su verdadera identidad.

Los ataques a una red de computadoras que se han documentado, se remontan a Agosto de 1986 cuando se registra un acceso persistente a los equipos de los laboratorios Lawrence Berkeley en los EEUU y a través de éstos a diferentes lugares. Se tarda mucho tiempo en descubrir que una persona ingresa desde una cabina pública telefónica de Alemania a miles de kilómetros del lugar. Stoll (1988).

En noviembre de 1998, un estudiante de la Universidad de Cornell lanzó un programa conocido como Internet Worm, el cual en 6 horas se difundió entre 3000 y 6000 computadores. Spafford (1989).

A estos ataques a redes informáticas que provienen de usuarios no autorizados que acceden, como señalamos, a hosts de la red desde lugares lejanos valiéndose de malas configuraciones, vulnerabilidades del sistema, deficientes contraseñas o técnicas de ingeniería social Goan (1999) denomina ataques externos.

La amenaza externa de ataques a empresas que han reportado esta situación ha crecido de 1996 a 1998 en un 16% del total de ataques. Redes corporativas supuestamente seguras como las de la CERT, NASA, la CIA, el Pentágono o la de Microsoft han reconocido intromisión en sus sistemas.

La otra forma de vulnerar la seguridad de una red, es a través de un usuario que tiene legítimo acceso, pero que es considerado intruso porque obtiene privilegios adicionales, hace mal uso o daña los recursos del sistema computacional. A este tipo de ataque, Goan (1999) lo denomina ataque interno, que puede llegar a ser más pernicioso e insidioso que el ataque externo.

La amenaza interna también crece, es decir, se han reportado casos en los cuales, los propios empleados de una organización ingresan a información restringida del sistema de computación.

9.3 ESPECTRO DE SEGURIDAD

La seguridad informática puede ser descrita tomando en cuenta el espectro de seguridad del sistema de computación, es decir, la cobertura o alcance que tiene el usuario de un equipo de computación durante su interacción con éste. En principio, como muestra la fig 9.1, nos referiremos al círculo interno del espectro, la seguridad del computador personal, luego a la seguridad de una red local (LAN) y finalmente a la seguridad en el círculo externo, Internet.

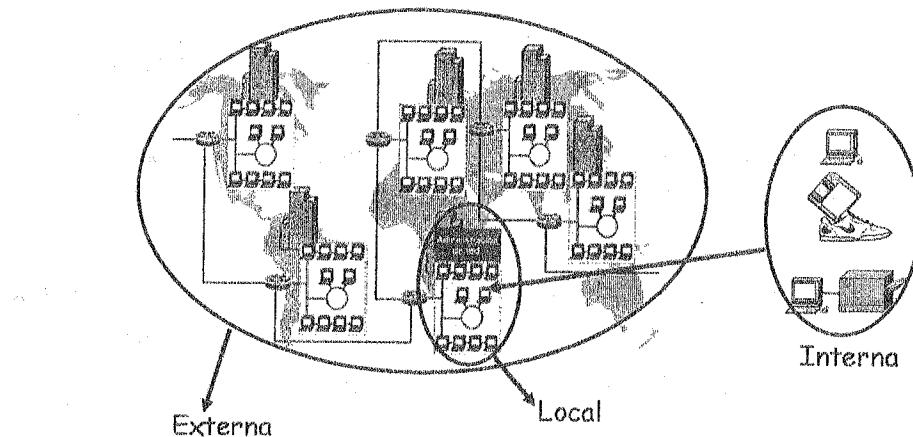


Fig. 9.1 Espectro de Seguridad

9.3.1 Seguridad Interna

Los archivos de datos que se llevan de un computador a otro, a través de medios magnéticos, están expuestos a daños (pérdida de información) debido a la posibilidad de la existencia de virus en otros equipos a los que, se accede. Este escenario se agrava cuando no se cuenta con detectores de virus que alerten de su presencia contagiando al medio magnético y a través de éste a otros computadores personales.

9.3.2 Seguridad Local

A nivel de una red local de computadoras, el ámbito de beneficios y problemas crece, porque se comparte información, bases de datos con otros usuarios, se minimizan los esfuerzos al tiempo de permitir el acceso a cierta información, pero también se va perdiendo la control de esta información. ACM (1997) denomina seguridad perimetral del sistema, a la protección de esta vulnerabilidad.

9.3.3 Seguridad Externa

El círculo externo está referido a la interconexión de muchas redes locales y remotas que tienen diferentes propósitos: académicos, comerciales, institucionales, gubernamentales, etc., es decir, los usos que tiene Internet. En la etapa inicial de Internet, la información circulaba libremente y no existía una preocupación por la privacidad de los datos ni por ninguna otra problemática de seguridad. Con la difusión libre de la información a través de los sitios o páginas en el Internet se abre una puerta al exterior por la que pueden pasar todo tipo de visitantes no necesariamente con buenas intenciones.

9.4 HERRAMIENTAS DE SEGURIDAD

Para proteger los recursos de una red, se aplica una variada tecnología que comprende el uso de: cortafuegos (firewalls), la Criptografía que estudia la conversión de datos en un código secreto o texto cifrado a través de un algoritmo de encriptación para su transmisión sobre una red pública¹, tecnologías biométricas de autentificación , herramientas de software y otros dispositivos con el propósito de controlar el flujo de información desde el exterior de la red, cifrar un mensaje, prevenir posibles ataques, evitar la denegación de servicios o detectar intromisiones a sus sistemas.

No obstante todas estas medidas de protección, los intrusos se valen de las propias herramientas tecnológicos, las adaptan para comprometer la seguridad de aquellos sistemas computacionales que permiten el acceso físico o remoto a sus recursos.

9.4.1 Herramientas de prevención

Los métodos orientados a conexión de red, monitorean las conexiones que se intentan establecer con una red o un equipo en particular, siendo capaces de efectuar una acción en base a métricas como: origen de la conexión, destino de la conexión, servicio solicitado, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador vía correo electrónico . En esta categoría están los cortafuegos (firewalls) y los wrappers.

Una forma de evitar que intrusos penetren a una red local es colocar un Cortafuego o Firewall entre una red que no sea de confianza o red pública (como internet) y la red interna; que controle y restrinja la información que ingrese o sale a o desde equipos de la red local de acuerdo a las políticas de seguridad adoptadas.

Hay dos tipos generales de cortafuegos o combinación de ellos, dependiendo del nivel o capa de la arquitectura de red; a nivel de la capa de Red, están los cortafuegos de filtrado de paquetes o routers y a nivel de la capa de Aplicación los proxies.

Los routers son cortafuego de filtrado de paquetes, tienen la capacidad de definir reglas de acceso, es decir, un conjunto secuencial de condiciones que determinarán si el paquete analizado seguirá (permit) o detendrá (deny) su camino según las direcciones del puerto origen o destino.

Un cortafuegos a nivel de Aplicación o Proxy, actúa como un intermediario entre el cliente y el servidor. En lugar de conectarse directamente con el servidor, una aplicación cliente se conecta con el proxy y le pide información. El proxy abre una conexión con el servidor, envía la petición y continúa para intercambiar información entre el cliente y el servidor (Pitts, 2001).

Los administradores de redes se dieron cuenta que no es suficiente el Cortafuego, Nice (2000), por cuanto no solo existe el riesgo que no se encuentre adecuadamente configurado, sino que los ataques pueden ser internos o tener nuevas técnicas que el Cortafuego no lo detecta.

9.4.2 Herramientas de confidencialidad



Fig. 9.2 Proceso de Encriptación. Fuente (O'Reilly, 1999)

La encriptación se utiliza para asegurar que la información sea sólo visible a quien tiene autorización de verla. Su aplicación es principalmente en las comunicaciones entre dos entidades. Se la realiza a través de herramientas añadidas como por ejemplo GnuPG², Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los certificados digitales tipo X.509. De éstas, la que recomiendan los especialistas es GnuPG por ser más completo, no utiliza el algoritmo patentado de encriptación IDEA, en su lugar soporta ElGamal, DSA, 3DES y MD5 entre otros.

Las funciones hash como SHA-1 (Secure Hash Algorithm) o MD5 (Message Digest Algorithm 5) aplicadas a documentos, generan valores de verificación con resistencia a la colisión, es decir, que no es factible encontrar dos secuencias de caracteres o documentos cuyo valor de hash sea el mismo. El valor de hash representa al documento de forma exacta y unívoca, de manera que aplicando la función hash a un documento modificado, resultase diferente.

9.4.3 Herramientas de integridad

Para poder asegurar la integridad de los datos y archivos, se requiere la habilidad de detectar su manipulación o alteración indeseada (inserción, borrado o sustitución) por algún intruso. Los métodos de autentificación de datos que se utilizan son: la suma de comprobación o checksum y las ya mencionadas funciones hash.

Una herramienta de protección a la integridad de información busca patrones en el registro de Windows y en el cron de Unix, generalmente no emite alarmas sino que genera registros de su trabajo. Baluja (2002).

La herramienta de integridad por excelencia en varias plataformas como LINUX es Tripwire®. Básicamente crea y almacena una suma de comprobación de archivos críticos de alta calidad, de modo que si el archivo o sus atributos cambian, este hecho puede ser detectado.

² GnuPG. Gnu Privacy Guard. Herramienta de seguridad en comunicaciones electrónicas. Es software libre

9.4.4 Herramientas de detección y monitoreo

Las herramientas de detección de intrusos permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, en base a la información con la que han sido previamente alimentados.

El proceso de monitoreo del comportamiento del sistema es realizado por archivos de registro histórico de lo que va sucediendo (log files) como: quien ingresó, que hizo, los archivos que se transfirieron en la red, intentos de usuarios para tener privilegios de root y otra información que permita descubrir la causa de hoyos de seguridad (bugs), la fuente de ataques y tener un panorama del daño causado. Una herramienta del ranking de Focus Security ³ es Maillog View que permite ver los log de mensajes de correo de manera eficiente. Para analizar los logs de Apache o Squirt, se recomienda logcheck. Bajo el entorno Windows Microsoft, el archivo Winlogon.log provee información de registro para eventos de seguridad.⁴

Según Northcutt (2001) una pista de un sistema que se encuentra bajo ataque es el hecho que se produce cuando escribimos un carácter en la consola de este sistema y tarde más de un minuto de mostrarse en pantalla.

Cuando no es posible detener el daño, con estos archivos se debiera reconstruir el sistema, conducir una investigación o dar algún testimonio. Sin embargo, como se encuentran en el sistema, son susceptibles de alteración o eliminación.

Una herramienta de seguridad que detecta los puntos vulnerables del sistema o de la red es el scanner. Los scanners de sistema rastrean hosts locales en busca de puntos vulnerables debido a descuidos en la configuración del sistema, como permisos erróneos para archivos, entradas de UID⁵ erróneas o duplicadas.

Los scanners de red prueban hosts sobre conexiones de red, de forma similar a la que lo haría un intruso. Examinan los servicios y puertos disponibles para detectar las exploraciones de reconocimiento de información en busca de vulnerabilidades conocidas que pueden explotar los atacantes remotos. Ejemplos de scanner de red son: Tiger, ISS (Internet Security Scanner), COPS (Computer Oracle Password and Security), Portsentry y TCP Wrappers.

³ <http://www.securityfocus.com>

⁴ <http://technet.microsoft.com>

⁵ Identificador de usuario en el sistema UNIX

Los scanners de sistema o de red en manos maliciosas son otra forma de ataque, para lo cual se han desarrollado herramientas detectoras de scanners como: IcmpInfo (detector de rastreos/bombas ICMP), scan-detector (detector genérico de rastreos UDP).

Para evitar que los intrusos capturen el tráfico diario de la red, se sugiere instalar un medio seguro para mover archivos, establecer permisos, ejecutar los scripts de la shell, etc. Una herramienta que permite realizar esto es Secure Shell (ssh).

9.5 VULNERABILIDAD DE UNA RED

En general los problemas de seguridad en redes tienen que ver con vulnerabilidades en la función de una red de datos cual es la de transmitir y recibir información desde y a lugares remotos utilizando recursos de hardware y software que como dijimos son susceptibles de ser interceptados por intrusos. Northcutt (2001) señala que los ataques de denegación de servicio y de disponibilidad utilizan tráfico altamente fragmentado para agotar los recursos del sistema.

Estas vulnerabilidades en las redes de datos son violaciones a la privacidad, integridad, disponibilidad o control. Los ataques se producen bajo diversas plataformas de desarrollo, según Anonymous(2000) de los alrededor de 13,000 virus existentes, la mayoría atacan a computadores personales que utilizan el sistema operativo de Microsoft, por el contrario, muy pocos de ellos atacan a sistemas operativos que utilizan UNIX o Linux.

9.5.1 Vulnerabilidad Física

Según Anonymous (2000) la vulnerabilidad física tiene que ver con: la ubicación del servidor y el acceso físico a él, la topología de la red, hardware de la red, acceso físico y robos de los equipos de computación y de comunicación.

Los especialistas en seguridad afirman que si usuarios malintencionados tienen acceso físico, los controles de seguridad son inútiles y los sistemas de computación son vulnerables a ataques in situ.

Para (Mei & Borowski, 2000) la seguridad física es la primera capa de seguridad. En un ambiente de red es mucho más crítico y se recomienda restringir el acceso a la consola de los servidores. Los nodos con inadecuada protección física, son susceptibles a ser vulnerados, es decir, a interferir su tráfico, comprometerla y violar su seguridad.

9.5.2 Virus, Gusanos y Troyanos

Los virus según McAfee (1989) son programas de computación diseñados por intrusos para infectar o adjuntar código dañino a otros programas con copias de sí mismo; en cambio los gusanos son programas que destruyen datos, pero a diferencia de los virus, no se replican a si mismos. Un ataque de los denominados gusanos, usa los recursos del host comprometido para propagarse a otras máquinas conectadas a internet. Estos constantemente desnudan problemas de seguridad en servidores bajo diferentes plataformas o se expanden en equipos cliente a través de archivos adjuntos a correos electrónicos.

Los denominados caballos de Troya o Troyanos son programas alterados con código adicional que emulan realizar funciones normales pero en realidad deshabilitan o sustituyen utilidades legales. Estos programas pueden borrar o modificar archivos de usuarios, transmitir archivos al intruso, instalar programas con privilegios de superusuario, instalar virus u otros caballos de Troya. Para evitarlos, se recomienda instalar software de fuente confiable, no abrir correo no solicitado. El troyano login_trojan.c , es un ejemplo bajo LINUX que emula a /bin/login. Internamente guarda contraseñas en un archivo para un posterior examen que es enviado por correo electrónico al intruso.

A través del comando \$ strings /bin/login | grep "HELO"

Podemos detectar si se encuentra instalado este programa.

Un tipo de ataque de confidencialidad es el denominado "ataque de diccionario" que almacena en un computador todas las palabras de un diccionario u otra lista de posibles contraseñas.

9.5.3 Ataques de Sniffers

Entre las vulnerabilidades de una red, se encuentran herramientas de software desarrolladas por los intrusos maliciosos denominadas sniffers que instalan, a través de programas troyanos, dispositivos de monitorización y analizadores de protocolos ocultos que recogen información de la red desde capturar nombres de usuarios y contraseñas de superusuario hasta grabar todo el tráfico de la red, es decir, colocar la interface de red en modo promiscuo.

En LINUX se han detectado varios sniffers entre los que se incluyen: linsniffer, linuxsniffer, hunt, sniffit cuyas descripciones se encuentran disponibles en Internet.

Los ataques de sniffers son difíciles de detectar porque son programas pasivos que no generan logs y si son exitosos, no utilizan mucha memoria ni espacio en disco. Se recomienda usar los comandos ifconfig e ifstatus que detectan si una interface de red se encuentra o no en modo promiscuo. Otra forma de evitar este tipo de ataques, es utilizar secure Shell (ssh) u otro mecanismo de encriptación de contraseñas.

9.5.4 Ataques de Autentificación (Spoofing)

Cuando los intrusos autentifican una máquina con otra mediante la falsificación de nombres o direcciones de un host confiable se producen los denominados spoofing. Entre las varias técnicas de spoofing se incluyen de: direcciones IP, ARP y DNS dependiendo de la información (paquetes, direcciones o nombres respectivamente) que el host del intruso interfiere entre el intercambio de dos hosts que confían uno del otro. El spoofing de DNS puede evitarse configurando el servidor de manera que éste no responda a consultas recursivas, sino solo a aquellos servidores confiables.

9.5.5 Denegación de servicios

En este tipo de ataques, conocido por sus siglas en inglés como DoS (Denial of Service), un intruso obstruye acceso a la red a los legítimos usuarios de tres formas diferentes: i) sobrecarga de requerimientos de servicio, ii) inundación de mensajes y iii) impedimento de señal. Dependiendo si el ataque obstruye el proceso normal de requerimientos de paquetes de red, si hay un exceso de mensajes al servidor o si hay alguna obstrucción en la transmisión o recepción de la señal respectivamente.

Como ejemplos de este tipo de ataques se encuentran: smurf o bombas de redirección ICMP, inundación SYN, inundación ping o el ataque de red de inundación en masa (Tribe Flood Network, TFN). El ataque smurf, aprovecha la capacidad de ICMP de enviar tráfico a la dirección de difusión. Un host malintencionado crea una petición eco ICMP y la dirige a una dirección de difusión de una red intermedia con un origen IP trampa. El origen IP elegido es el del host objetivo víctima. Si el sitio intermedio permite actividad de difusión en la red enviando la petición eco ICMP, todos sus hosts responden enviando una respuesta eco ICMP a quien piensan que es el remitente o host víctima, consiguiendo que éste se degrade en su funcionamiento.

No es posible protegerse completamente contra los ataques por denegación de servicio. Una estrategia para identificar estos ataques es aislar la red o segmentarla en subredes, monitorear la red y así limitar su efecto en solo partes de la red si el ataque se vuelve a producir nuevamente, aunque no se elimina el problema completamente.

El DDoS (Distributed Denial of Service) es un ataque generado por el esfuerzo coordinado de cientos de computadoras conectadas a internet. Uno de estos ataques lo sufrió recientemente Gibson Research Corporation cuyo servidor fue atacado por 474 PC's bajo plataforma Windows distribuidas en 45 redes conectadas a internet.

9.5.6 La Ingeniería Social

En este caso, el intruso obtiene información valiosa (cuenta bancaria, contraseñas) de otra persona, usuario legítimo, quien por descuido a través de una conversación, agenda, llamada telefónica, encuestas o cualquier otro medio pierde o involuntariamente revela esta información.

Las relaciones sociales de los actores de sistemas de información, en reuniones, sala de computadoras o en la gerencia de una empresa, como en cualquier área de trabajo, facilitan las tareas. Sin embargo también se constituyen en otra fuente de vulnerabilidad interna de una red, por lo que se requiere añadir procesos de autentificación.

9.6 VULNERABILIDAD DEL MODELO TCP/IP

El modelo TCP/IP de internet es una representación de la actividad de intercambios de información que se producen entre hosts de una red. A nivel de la capa de Aplicaciones o de interfase directo con el usuario, los protocolos más importantes son :FTP, SMTP, HTTP y TELNET.

Los servidores de red asociados a los mencionados protocolos respectivamente son: Transferencia de Archivos, Correo Electrónico, Páginas Web y Conexión Remota. Además mencionamos al Servidor de Nombres de Dominio (DNS), que según Northcutt (2001) es probablemente uno de los objetivos más comunes de los esfuerzos de un intruso por tratar de vulnerarlo. En el siguiente cuadro se resumen algunas vulnerabilidades de protocolos de este modelo.

PROTOCOLO	VULNERABILIDAD
TCP	Instalación de puerta trasera en el servidor
IP	Enmascaramiento en la fragmentación de datagramas
ICMP	No ofrece garantías sobre la respuesta al informador
FTP	Falta de privacidad de sus sesiones, ya que no se encuentra cifrado
HTTP	Riesgo de escucha de información sensitiva
SMTP	Acceso al servidor de correo para enviar correo basura (spam)
TELNET	Saturación de memoria en el programa <i>telnetd</i> para obtener acceso a la cuenta de superusuario.

Cuadro 9.1 Vulnerabilidades de algunos protocolos TCP/IP

Ante estas vulnerabilidades, se recomienda mantener actualizadas las versiones de estos protocolos porque generalmente se incluyen parches a las vulnerabilidades detectadas en las versiones anteriores. También el administrador de la red deberá estar actualizado y mantenerse informado, por ejemplo, se publican en internet boletines de información donde se describe el problema, la plataforma, el daño y la solución a aplicar, es decir, los parches necesarios.

9.7 CONCEPTOS Y TERMINOS CLAVE

- Archivos de registro histórico
- Arquitectura de los IDS
- Ataque Mitnick
- Ataques a redes informáticas
- Ataques de Autentificación
- Ataques de Sniffers
- Ataques externos
- Ataques internos
- Clasificación de los IDS
- Cortafuegos
- DDoS
- Denegación de servicio
- Espectro de seguridad
- Función hash
- GnuPG
- Herramientas de confidencialidad
- Herramientas de detección y monitoreo
- Herramientas de integridad
- Herramientas de Prevención
- Herramientas de Seguridad
- Ingeniería Social
- Intrusos
- Localización de un IDS
- Principios de Seguridad Informática
- Problemas de seguridad de DNS, FTP, http, ICMP, IP, SMTP, TCP, TELNET
- Proceso de Encriptación
- Scanner
- Sistemas de Detección de Intrusos
- Smurf
- TCPDUMP
- Virus
- Vulnerabilidad de una red
- Vulnerabilidad del modelo TCP/IP
- Vulnerabilidad Física

9.8 PREGUNTAS DE REPASO

1. Cual de las siguientes opciones define con más precisión la Confidencialidad
 - A. Certificar que la comunicación es con quien se desea
 - B. Privacidad de la información
 - C. Intercambio seguro de información
 - D. Consistencia y protección de la información

2. Cual de las siguientes opciones define con más precisión la Integridad
 - A. Certificar que la comunicación es con quien se desea
 - B. Privacidad de la información
 - C. Intercambio seguro de información
 - D. Consistencia y protección de la información

3. Cual de las siguientes opciones define con más precisión el principio de No repudio
 - A. El receptor no debe ser capaz de negar el envío de un mensaje
 - B. El emisor no debe ser capaz de negar el envío de un mensaje
 - C. Intercambio seguro de información
 - D. Consistencia y protección de la información

4. Cual de las siguientes opciones define con más precisión la Denegación de Servicios
 - A. Una vulnerabilidad
 - B. Un ataque al protocolo tcp
 - C. Deshabilitar el acceso a un particular recurso de las víctimas
 - D. Un ataque de autentificación

5. Un Cortafuegos se coloca:
 - A. Entre la red pública y la red interna
 - B. Al interior de la red interna
 - C. Fuera de la red pública
 - D. Entre los servidores locales

6. Un cortafuegos a nivel de paquetes es el:
 - A. Proxy
 - B. Hub
 - C. Router
 - D. Switch

7. ¿Cuál es una de las acciones que debe tomar un Administrador de red para prever que su red no sea atacada
- A. Revisar el hardware de la red
 - B. Nunca instalar un servicio que no necesita
 - C. Ninguna acción
 - D. Responder al ataque
8. ¿Cuál de las siguientes opciones es una vulnerabilidad del password o contraseña
- A. Tener una aplicación que no es necesaria
 - B. Que el nombre se encuentre en un diccionario
 - C. Que el nombre sea menos de 6 caracteres
 - D. Que el nombre sea difícil de recordar
9. ¿Cuál de las siguientes opciones es un ataque al protocolo HTTP
- A. Crear un enlace con información maliciosa
 - B. Crear una petición de eco para un host víctima
 - C. Solicitar información inocente, pero la respuesta contiene datos corruptos
 - D. Escucha de información sensitiva del usuario
10. ¿Cuál de las siguientes opciones es una vulnerabilidad del protocolo ICMP
- A. Crear un enlace con información maliciosa
 - B. Crear una petición de eco para un host víctima
 - C. Solicitar información inocente, pero la respuesta contiene datos corruptos
 - D. Crear un programa que revele la identidad del usuario
11. En que tipo de red, el riesgo de vulnerabilidad es mayor a las demás
- A. Una LAN sin conexión a Internet
 - B. Una LAN con conexión a Internet
 - C. Una WAN
 - D. Una red con solo dos equipos
12. A que se denomina seguridad perimetral
- A. A la seguridad dentro de la red LAN
 - B. A la seguridad fuera de la red LAN
 - C. A la seguridad de la WAN
 - D. A la seguridad de cualquier red

13. Un cortafuegos a nivel de aplicación es el:

- A. Hub
- B. Proxy
- C. Router
- D. Switch

14. Para que se utiliza la encriptación

- A. Ocultar la información a todos los usuarios de la red
- B. Hacer visible la información a los intrusos
- C. Codificar cualquier información
- D. Asegurar que la información sea sólo visible a quien tiene autorización de verla

15. Las funciones Hash permiten:

- A. Encriptar la información
- B. Generar valores de verificación con resistencia a la colisión
- C. Generar números aleatorios
- D. Asegurar que los intrusos no ingresen a la red

9.9 TALLER

1. Discuta en el grupo el concepto de Seguridad y elaborar sus conclusiones
2. Discuta en el grupo los correos "spam" y las estrategias para controlarlos
3. Cual es la situación de la seguridad de las redes locales a nivel nacional. Describa algún caso concreto utilizando la matriz FODA (Fortalezas Oportunidades Debilidades y Amenazas)
4. Para cada uno de los principios de seguridad discutir en el grupo ejemplos.

CAPITULO 10 REDES WLAN

Objetivos de Aprendizaje: Al concluir el capítulo, usted será capaz de:

- Describir las normas aplicables a las redes inalámbricas
- Mostrar la arquitectura WLAN
- Conocer los avances en relación al futuro de las redes WLAN

10.1 INTRODUCCIÓN A LAS REDES WLAN

La importancia del acceso a Internet para host móviles es cada vez mayor por las nuevas aplicaciones como: acceso móvil a información, comunicaciones multimedia en tiempo real, juegos en red, trabajo corporativo y otras.

Las redes WLAN constituyen una alternativa a las redes LAN para lugares donde el cableado es difícil o imposible por tratarse de áreas con edificaciones antiguas y protegidas o áreas educativas donde no es adecuado una instalación de una LAN. Además son baratas en su instalación y pueden ser configuradas en una variedad de topologías para satisfacer la necesidad de la aplicación específica.

Los equipos de computación actuales que utilizan medios de comunicación fijos, como fibra óptica o cable UTP, también ofrecen la posibilidad de una conexión inalámbrica, es decir, sin utilizar los medios fijos mencionados.

Muchos de los fabricantes de computadoras y equipos de comunicación como son los PDAs (Personal Digital Assistants), modems y otros dispositivos están introduciendo aplicaciones soportadas en las comunicaciones inalámbricas.

Una WLAN es una red de área local inalámbrica, es decir, utiliza ondas de radio en lugar de cableado para la transmisión de datos en un edificio, oficina o en su domicilio. Está constituida por un conjunto de equipos tales como:

- Estaciones móviles (MS) como: computadores personales de bolsillo, Laptops, PDAs y otros conectados a través de dispositivos de comunicación
- Computadoras de escritorio provistas de tarjetas ISA
- Puntos de Acceso (AP) de alcance local (edificio o campus) que utilizan ondas de radio en zonas geográficas limitadas sin necesidad de tendido de cable entre ellos.

Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y video. La gran ventaja de esta tecnología es que ofrece movilidad al usuario y requiere una instalación muy sencilla. En cambio entre sus desventajas están su baja velocidad y vulnerabilidad a ataques de intrusos.

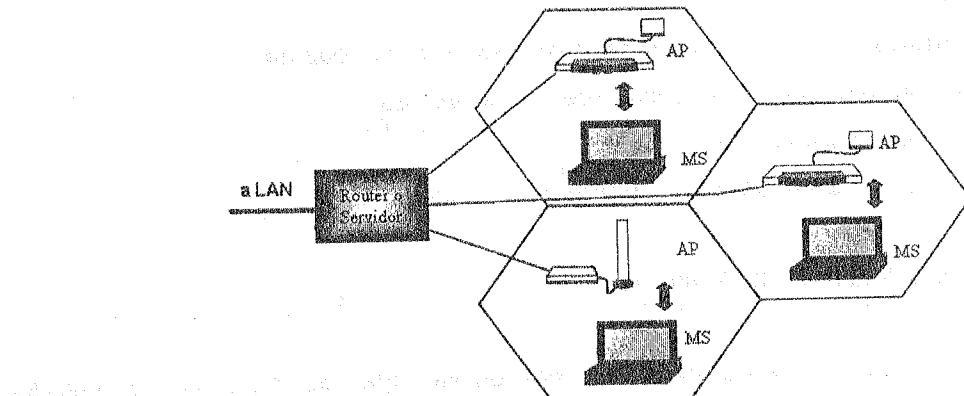


Fig. 10.1 Red Local Inalámbrica (WLAN)

10.2 ESTANDARIZACIÓN DE TECNOLOGÍAS WLAN

Las redes WLAN cumplen con los estándares genéricos aplicables al mundo de las LAN cableadas (i.e. IEEE 802.3 o equivalentes) pero necesitan una normativa específica adicional que defina el uso de los recursos radioeléctricos.

El primer estándar de WLAN lo generó el organismo IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) en 1997 y se denomina IEEE 802.11. Desde entonces varios organismos internacionales han desarrollado una amplia actividad en la estandarización de normativa de WLAN y han generado un abanico de nuevos estándares.

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación, todas las cuales utilizan los mismos protocolos.

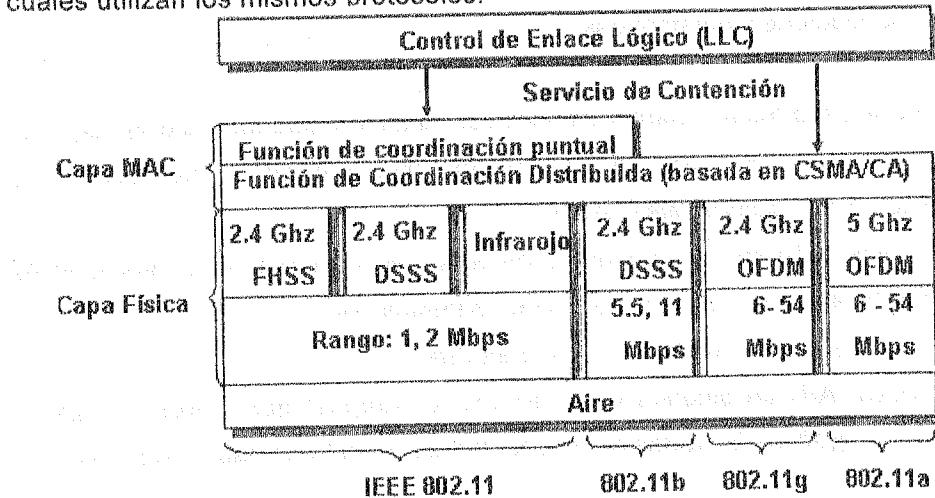


Fig. 10.2 Estructura del Estándar 802.11

a) La Norma IEEE 802.11

Esta norma conocida comercialmente como WI-FI o Wireless Fidelity, es el estándard básico para las redes WLAN que ofrece un rango de 1 a 2 Mbps. Su propósito es proveer un sistema de conectividad inalámbrica, que estandariza el acceso a bandas de frecuencia para comunicación de area local. Los beneficios de este estándar son: su compatibilidad, no requiere licencia o permiso para operar ni se necesita cableado para conectar los equipos del usuario.

b) La Norma IEEE 802.11b

La tasa de datos (de 1 a 2 Mbps) del estándar original 802.11 es muy lento para soportar la mayoría de los requerimientos de las empresas, por lo que la IEEE ha lanzado la norma 802.11b para transmisiones de 5,5 Mbps y de 11 Mbps que promete abrir nuevos mercados para la WLAN en empresas grandes, en pequeñas oficinas y para el hogar con rendimientos comparables a la norma Ethernet. Es decir, que estas especificaciones solo afectan a la capa Física como se observa en la anterior figura.

c) La Norma IEEE 802.11g

Similar a la norma 802.11b, es compatible con ésta, aunque la técnica de modulación que utiliza es OFDM o Multiplexación por División de frecuencias ortogonal. Su rendimiento llega a 54 Mbps, al igual que la 802.11b, opera en la banda de frecuencia de 2.4 Ghz.

d) La Norma IEEE 802.11a

Usa la banda de 5 Ghz con una tasa entre 6 a 54 Mbps. La banda se divide en sub-bandas para disminuir los efectos de interferencia. Si las sub-bandas se utilizan de forma aleatoria, la seguridad también puede ser mejorada.

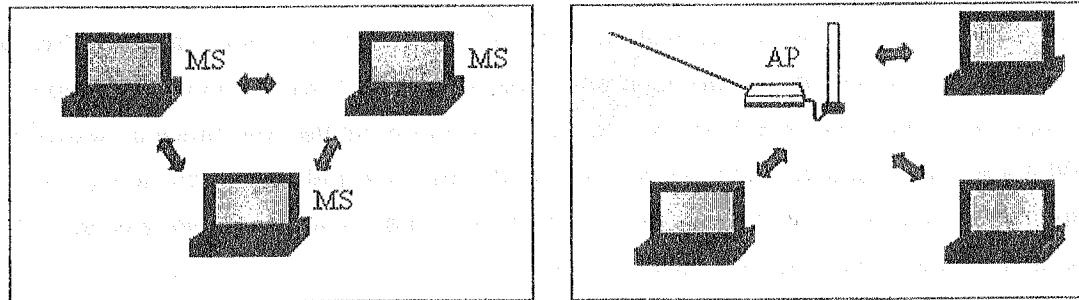
Es necesario mencionar que parte de la información transmitida en el aire es específica de la transmisión radio(cabeceras, codificación, etc..) y por lo tanto no forma parte de la capacidad útil para el usuario. Es decir que los valores de velocidad máxima de 11 Mbps ó de 54 Mbps no son equivalentes al concepto de velocidad aplicado en las redes LAN cableadas.

10.3 ARQUITECTURA WLAN

Una red inalámbrica de área local WLAN 802.11 define dos tipos de servicios: el conjunto de servicios básicos (BSS) y el conjunto de servicios ampliado (ESS).

10.3.1 Conjunto de servicios básico (BSS)

Un BSS es el bloque constructivo de una WLAN, compuesto de estaciones o nodos inalámbricos móviles o fijas y una estación base opcional, conocida como punto de acceso (AP). Un BSS sin un AP se denomina red ad hoc, un BSS con un AP se denomina red con infraestructura.



a) Red ad hoc

b) Red con Infraestructura

Fig. 10.3 Tipos de arquitecturas BSS

En una arquitectura tipo *ad hoc* la red está aislada y no se puede utilizar para enviar datos a otros BSS. Las estaciones móviles (MS) escuchan todo el tráfico, es decir, se pueden localizar unas a otras. No tiene conexión a una red fija y resulta útil allí donde previamente no existe o no se requiere infraestructura cableada (Hoteles, aeropuertos). Se reutiliza el canal, evitando que los puntos de acceso sobre un canal DSSS no se solapen con un canal utilizado por su punto de acceso vecino.

Una arquitectura con Infraestructura, consta de al menos un AP. Está conectado a la infraestructura de red cableada y un conjunto de estaciones finales inalámbricas. Se utiliza cuando se quiere conectar una red WLAN a una red cableada. Es el modo más adoptado. El AP utiliza todos los canales, no hay necesidad de configurarlos.

10.3.2 Conjunto de servicios ampliado (ESS)

Un ESS es un conjunto de dos o más BSS con AP que forman una sola subred. Teniendo en cuenta que la mayoría de las WLAN tendrán la necesidad de conectarse a las LAN cableadas corporativas, por ejemplo, una LAN Ethernet, éste será el modo de operación generalmente adoptado. La siguiente figura muestra un ESS.

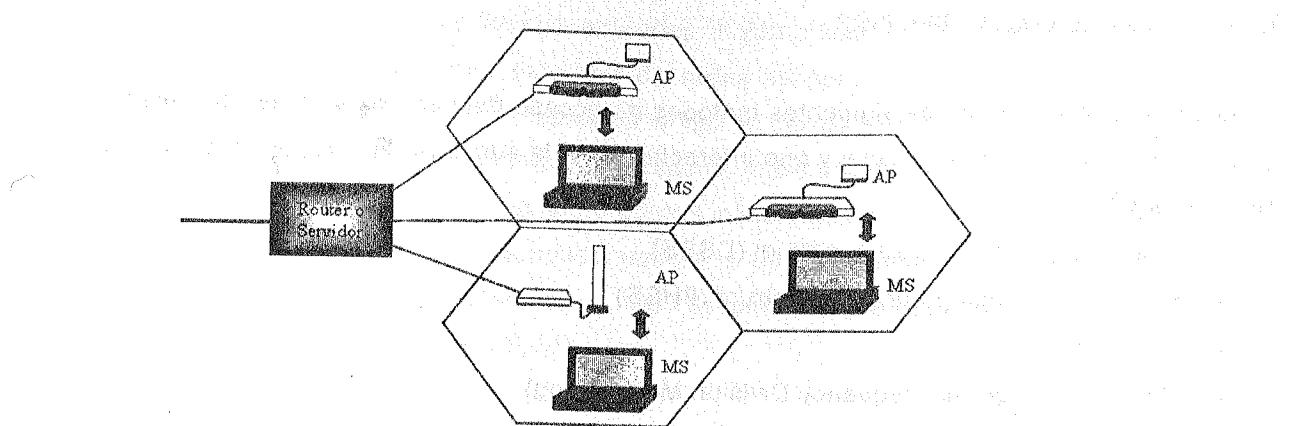


Fig. 10.4 Arquitectura ESS

Cuando se conectan los BSS, las estaciones situadas dentro del BSS pueden comunicarse entre sí, sin utilizar un punto de acceso (AP). Sin embargo, la comunicación de dos estaciones que se encuentren en diferentes BSS es a través de sus AP's. En el modo ESS las circunstancias y problemas son similares a los de un sistema celular, porque hay una competencia por el uso del canal entre los AP's.

10.4 PROTOCOLOS WLAN

Las normativas específicas para las redes WLAN como la familia 802.11, definen el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos) y de forma detallada los protocolos de la capa física (PHY) y de la subcapa de Control de Acceso al Medio (MAC) que regulan la conexión vía ondas de radio. Las capas superiores no se ven afectadas como muestra la siguiente figura.

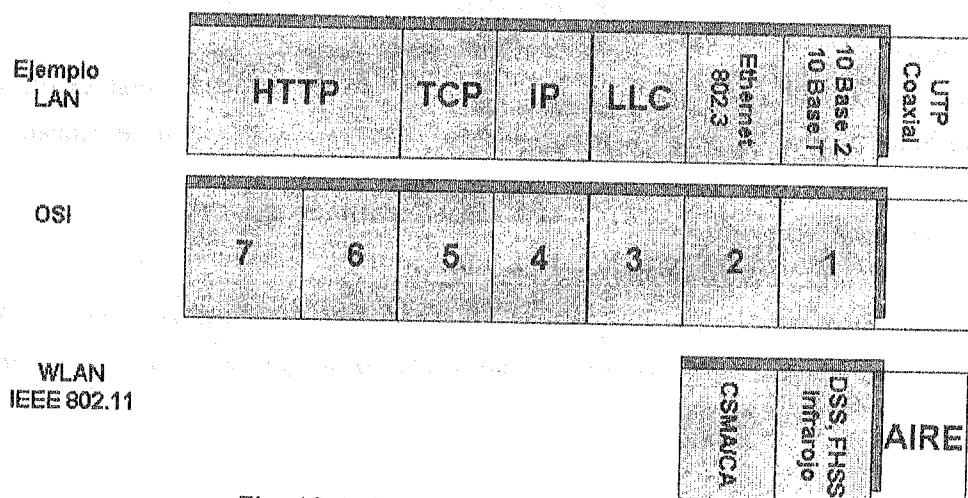


Fig. 10.5 Protocolos WLAN

10.4.1 Protocolos de la capa física

El estándar 802.11 define los siguientes métodos de acceso físico o técnicas de transmisión que corresponden a la capa Física y que interactúan con la subcapa de Control de Acceso al Medio o MAC:

- Direct Sequence spread spectrum (DSSS),
- Frequency Hopping spread spectrum (FHSS)
- Infrarrojo y
- OFDM (Orthogonal Frequency Division Multiplexing).

Las características de estos métodos se resumen en la siguiente tabla:

CARACTERÍSTICA	MÉTODO DE ACCESO DSSS - FHSS	Infrarojo
Frecuencia	2.4 - 2.4385 GHz 5.725 - 5.825 GHz	3×10^{14} Hz
Cobertura máxima	30 - 250 m, 4500 m ²	10 - 25 m
Requerimiento de línea de vista	No, pero en la práctica las ondas de radio penetran solo una pared de concreto.	Sí
Potencia de transmisión	DSSS: 1 - 100 mW FHSS: 10 - 100 mW	N/A
Uso entre edificios	Possible con antena	Possible
Velocidad	DSSS: 11 Mbit/s FHSS: 2 Mbit/s	2 Mbit/s

Tabla 10.1 Protocolos de la capa Física de una WLAN

10.4.2 Protocolos de MAC

La norma 802.11 define dos subniveles MAC: la función de coordinación distribuida y la función de coordinación puntual. La primera utiliza CSMA/CA como el método de acceso.

a) CSMA/CA Carrier Sense Multiple Access)/(Collision Avoidance)

En las redes inalámbricas, gran parte de la energía se pierde en la transmisión. La señal recibida tiene muy poca energía, lo cual es un inconveniente en la detección efectiva de las colisiones.

Es necesario evitar las colisiones en redes inalámbricas debido a que las colisiones no pueden ser detectadas. Para este tipo de redes se desarrolló el protocolo CSMA/CA con especificaciones IEEE 802.11, donde si el canal permanece vacío por un tiempo igual o mayor a un parámetro denominado IFS (Espacio entre tramas) entonces el nodo inalámbrico que está listo para acceder al canal de control inicialmente sensa el canal para determinar si está o no ocupado, si está ocupado espera a que se encuentre inactivo, si está vacío transmite y la trama será recibida en el nodo destino siempre que ninguna otra transmisión la interfiera para no causar una colisión.

b) Función de Coordinación Puntual

Es un método de acceso opcional por muestreo libre de contención centralizada, que se puede implementar en una red con infraestructura. El AP realiza el muestreo sobre aquellas estaciones que sean capaces de ser muestreadas. Las estaciones se muestrean una detrás de otra, enviando cualquier dato que tengan al AP.

10.5 SEGURIDAD EN WLAN

En cuanto a seguridad, 802.11 utiliza encriptación y autentificación. La encriptación lo realiza mediante el algoritmo WEP (Wired Equivalent Privacy), permite que la encriptación se ajuste a 256 bits, 128 bits, 64 bits o deshabilitada. Cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red, y para controlar los accesos se programa ESSID, también conocido como WLAN Service Area ID, en cada punto de acceso.

Existen diferentes opciones para realizar el proceso de autentificación. Para las WLAN en topologías ad-hoc, la autentificación puede ser en "Open System" o con "Shared Key". En un Open System, cualquier terminal cliente puede solicitar la autentificación y el terminal que recibe esta solicitud puede otorgar la autentificación a las estaciones que se encuentran en su lista de usuarios definidos. En un sistema Shared Key, solamente las estaciones que comparten una clave secreta pueden ser autenticadas. Para las topologías en modo infraestructura, la autentificación se resuelve mediante un diálogo entre el cliente y el punto de acceso.

Y más allá del Nivel 2, emplea los mecanismos de seguridad propios de todas las tecnologías LAN 802, como login al sistema operativo de red, estando abierto además a la encriptación avanzada IPsec (IP Security), entre otras alternativas. Estas tecnologías de mayor nivel pueden ser usadas para crear redes seguras de extremo a extremo que incluyan tanto redes cableadas como inalámbricas.

Algunos fabricantes han desarrollado extensiones propietarias de las normas de seguridad (sobre 802.11) para implementar el cambio de claves periódicamente pero el inconveniente es que todos los dispositivos de la red WLAN deben ser suministrados en ese caso por el mismo fabricante. La tendencia más reciente es sin embargo emplear el estándar 802.1x como base sólida del mecanismo de autenticación y autorización. Estos atributos de seguridad que se han descrito operan a nivel físico y de enlace. Pero existen otras vías de añadir más seguridad al sistema WLAN a otros niveles, tales como jugar con las direcciones MAC de los clientes (nivel 2) o construir VPNs entre el cliente y el servidor correspondiente (nivel 3), con lo que en la práctica puede decirse que la parcela de seguridad está suficientemente consolidada.

10.6 EL FUTURO DE LAS REDES INALÁMBRICAS

Los fabricantes de WLANs migraron de la banda de 900 MHz a la banda de 2,4 GHz para mejorar la velocidad de información.

Este patrón, iniciado con IEEE 802.11b continúa al abrirse el estándar IEEE 802.11a en la banda de 5,7 GHz operando con una velocidad de datos de hasta 54 Mbit/s. Esta banda de 5,7 GHz promete otras mejoras en velocidad, permitiendo en el futuro romper la barrera de los 100 Mbit/s.

Otras tecnologías para redes inalámbricas también han emergido paralelamente a las definidas por la IEEE 802.11x, tales como Bluetooth, HomeRF, LMDS (Local Multipoint Distribution Service). También, la entrada de nuevos protocolos, lenguajes y esquemas de seguridad ha sido de gran importancia en el avance de las redes inalámbricas tales como WAP (Wireless Application Protocol), WML (Wireless Markup Language), WEP (Wired Equivalent Privacy), entre otros.

La opción WLAN se convierte así en una alternativa de acceso en los denominados Hot Spots, entornos públicos o semipúblicos, donde reside temporalmente una apreciable cantidad de personas con necesidad de establecer, al mismo tiempo, comunicaciones de voz y/o datos.

En el futuro, no solo se verán aplicaciones de las redes inalámbricas para grandes empresas, sino en las próximas redes de tercera generación Sistema Universal de Telecomunicaciones móviles (Universal Mobile Telecommunications System - UMTS) que es una de las tecnologías usadas por los móviles de tercera generación (3G, también llamado W-CDMA). Sucesor de GSM.

Así, la integración de WLAN y de 3G se presenta, junto con la utilización por los ISPs para facilitar el acceso a alta velocidad a Internet, como las opciones de más futuro. Por ejemplo, la limitación del bajo rango de transmisión de datos de 3G (2 Mbps) se puede superar cuando esté disponible una cobertura de WLAN. Similarmente, cuando el usuario sale de la pequeña área de cobertura de WLAN, se puede manejar la del sistema 3G.

Con la integración de WLAN como un acceso más a las redes de los operadores de nueva generación, tanto fijos como móviles, los usuarios de WLAN serán tratados sin ninguna diferenciación respecto del resto de usuarios de redes fijas o celulares, salvo los problemas de roaming si nos movemos a una gran velocidad, puesto que las células WLAN cubren 50 m. En consecuencia, WLAN puede verse como un complemento a UMTS, más que como una amenaza.

Otra solución de comunicación inalámbrica para redes de área metropolitana que ya se ofrece en nuestro medio es el WiMAX o Worldwide Interoperability for Microwave Access (Interoperabilidad mundial para acceso por microondas). Es una norma de transmisión de datos usando ondas de radio, que está conforme con los estándares de acceso inalámbrico IEEE 802.16.

En comparación con el estándar 802.11 (WiFi), la cobertura de WiMAX puede alcanzar hasta 50 Kms para estaciones fijas y hasta 15 Kms, para estaciones móviles aunque su uso sea similar. WiMAX opera con frecuencias con y sin licencia.

10.8 PREGUNTAS DE REPASO

1. Indicar los componentes de una red WLAN
 - A. Puntos de Acceso AP, Estaciones Móviles, PC con tarjeta ISA
 - B. Puntos de Acceso AP, routers, Laptops
 - C. Estaciones Móviles, Puntos de Acceso AP, Hubs
 - D. Puntos de Acceso AP, Pc con tarjeta ISA, Switch
2. Cual es el alcance de un Punto de Acceso AP
 - A. Regional
 - B. Nacional
 - C. Local
 - D. Cobertura Amplia
3. Indicar una desventaja de la red WLAN
 - A. Difícil instalación
 - B. Baja velocidad
 - C. No ofrece movilidad a sus usuarios
 - D. Todas las anteriores
4. Que tipo de normas son aplicables a las redes WLAN
 - A. Las que utilizan las redes LAN
 - B. Las que utilizan las redes WAN
 - C. Las que utilizan las redes LAN con una normativa adicional
 - D. Las que utilizan las redes MAN con una normativa adicional
5. Cual es el estándar que utilizan las redes inalámbricas
 - A. IEEE 802.3.
 - B. IEEE 802.5.
 - C. IEEE 802.11
 - D. Ninguna de las anteriores
6. Cual es el rango de la norma WI FI
 - A. De 1 a 10 Mbps
 - B. De 10 a 100 Mbps
 - C. De 1 a 2 Mbps
 - D. Mas de 10 Mbps

7. A cuales capas del modelo TCP/IP afectan las normativas de redes inalámbricas
- A. Capa de Aplicación
 - B. Capa de Transporte
 - C. Capa de Red
 - D. Capa Física
8. Indicar un tipo de servicio de las redes WLAN
- A. conjunto de servicios básicos
 - B. conjunto de servicios locales
 - C. Conjunto de servicios metropolitanos
 - D. Ninguno de los anteriores
9. Como se denomina el servicio BBS que utiliza un punto de acceso
- A. Red Ad Hoc
 - B. Red con infraestructura
 - C. Red ESS
 - D. Ninguno de los anteriores
10. Que tipo de red inalámbrica es adecuada para un hotel
- A. Red Ad Hoc
 - B. Red con infraestructura
 - C. Red ESS
 - D. Ninguno de los anteriores
11. Que tipo de red inalámbrica es adecuada cuando se quiere conectar una WLAN a una red cableada
- A. Red con infraestructura
 - B. Red Ad Hoc
 - C. Red ESS
 - D. Ninguno de los anteriores
12. Como está conformado el conjunto de servicios ampliado
- A. Un BBS con un AP
 - B. Dos o mas ESS con un AP
 - C. Un ESS
 - D. Dos o mas BBS con un AP

13. Indicar una característica de los protocolos de la capa Física de una red inalámbrica

- A. Velocidad
- B. Ancho de banda
- C. Conectividad
- D. Atenuación

14. Cual es el tratamiento de las colisiones en las redes inalámbricas:

- A. Rápidamente se las detecta
- B. No se las detecta
- C. Depende de la velocidad
- D. Depende del protocolo

15. Que aspectos de seguridad toma en cuenta el estándar que utiliza las redes inalámbricas

- A. Autentificación
- B. Encriptación
- C. AyB
- D. Ninguna de las anteriores

10.8 TALLER

1. Indicar 3 características fundamentales de las redes WLAN
2. Explicar por que las redes WLAN son más vulnerables que las redes LAN
3. Describir que se requiere para instalar una red WLAN
4. Explicar 3 diferencias de las redes LAN y las redes WLAN

CAPITULO 11 TECNOLOGIA VoIP

Objetivos de Aprendizaje: Al concluir el capítulo, usted será capaz de:

- Conocer las características de la tecnología VoIP
- Mostrar los agentes implicados en una telefonía IP
- Describir los protocolos utilizados para VoIP
- Establecer los requerimientos para implementar una comunicación utilizando esta tecnología

11.1 LA TELEFONÍA TRADICIONAL

El desarrollo del acceso a Internet por un canal de banda ancha, así como el uso de nuevas tecnologías como los avanzados sistemas inalámbricos, ha revolucionado el tráfico de voz de la red telefónica tradicional pública o PSTN a redes alternativas utilizando el protocolo IP como lo es voz sobre IP o VoIP.

La idea de hacer audible la voz a grandes distancias lo inicia Alexander Bell en el siglo XIX con transmisiones sobre un hilo de hierro y comunicación punto a punto inicialmente con conmutación manual, luego a través de una central telefónica y de ésta hacia otras centrales mediante una conexión entre canales los usuarios se comunican a través de una red de interconexión.

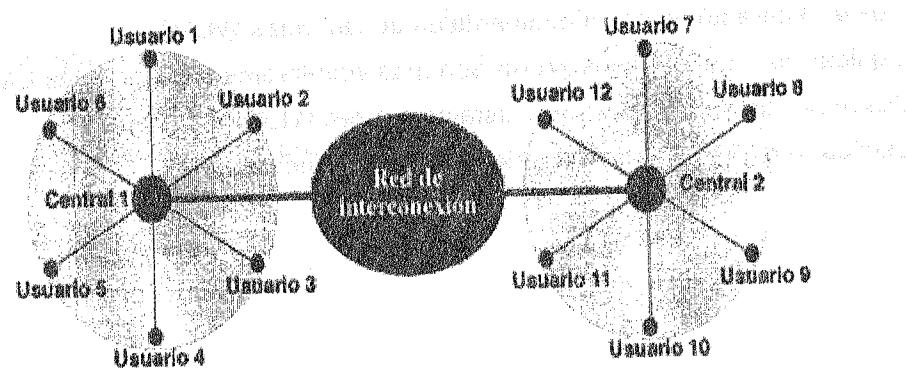


Fig. 11.1 Conexión entre canales

La llamada que sale de una de las centrales tiene que llegar hasta la central donde está la persona o teléfono destino. Este sistema ya realiza la multiplexación por división de tiempo TDM, donde se hace necesaria la multiplexación del enlace troncal entre centrales y no es posible realizar un mallado total.

Las características principales de la telefonía tradicional son:

- Recursos ocupados durante toda la duración de la llamada.
- Los precios varían en base al tiempo de uso (tiempo de ocupación del circuito dedicado).
- La distancia importa (más circuitos, y sobre todo de operadoras distintas).
- Diseñado para "solo voz".
- Sector totalmente regulado.
- Garantía de disponibilidad.

11.2 FUNDAMENTOS DE VOIP

La tecnología de VoIP está teniendo rápida expansión, causando cambios significativos en la forma en que los servicios de comunicación de voz son realizados. Según (Ahuja, 2004) se constituirá en la futura autopista para redes de telecomunicación.

El servicio VoIP es mucho más económico que el servicio tradicional de teléfonos fijos y en algunos casos, incluso gratuito. Otra ventaja importante de VoIP es su gran portabilidad. Puesto que se basa en la red mundial de Internet, los usuarios no están limitados a una ubicación física específica a la hora de obtener los servicios como el acceso a los mensajes del buzón de voz a través de Internet.

Según el diccionario de Internet Newton, se define la voz sobre IP (VoIP) como: "La tecnología usada para transmitir conversaciones de voz sobre una red de datos usando el protocolo IP. Esta red de datos puede ser la Internet o una Intranet corporativa o administrada por un proveedor de servicios Internet".

La historia de Voz sobre IP comienza en la década de los años 90 cuando investigadores de instituciones educativas y corporativas tomaron interés en la transmisión de voz y video sobre redes IP, especialmente en intranets corporativas y en la Internet. Esta tecnología es comúnmente referida como VoIP y es en términos simples, el proceso de dividir el audio o video en pequeños pedazos o paquetes, transmitiendo estos paquetes sobre una red IP y reensamblándolos en el otro extremo de tal forma que dos personas puedan comunicarse usando audio y video.

Por supuesto que hay mucho más que decir acerca de VoIP que solo envía/recibe paquetes de audio/video sobre la Internet. Un aspecto importante se refiere al protocolo de comunicación que utilizan las computadoras para intercambiar información y permitir que ésta fluya entre los dispositivos de comunicación. O el formato que tiene el contenido de los paquetes.

VoIP no está limitada a computadoras de escritorio. Esta tecnología está implementada en una variedad de dispositivos de hardware, incluyendo: teléfonos IP, adaptadores o interfaces de terminales análogas / terminales IP, puertas de enlace o gateways, servidores de aplicaciones IP. En resumen, un gran número de dispositivos que pueden habilitar el servicio de comunicaciones IP con varias soluciones, algunas de las cuales permite el uso del aparato telefónico tradicional con interface a la red IP.

Con la tecnología VoIP, la voz está integrada con otros servicios como: buscador de personas, reuniones virtuales a nivel individual y de empresas, traducción de idiomas en tiempo real, video conferencias multipunto, chat de voz, central de llamadas con acceso desde navegadores web, teléfonos IP o solo teléfonos de voz, central de llamadas que incluyen mensajes SMS y otros.

En relación al funcionamiento de VoIP, se simplifica en los sgtes pasos (Asterik, 2005):

- Paso 1: Los dos comunicantes se registran en el servidor VoIP con sus teléfonos (Hardphones, Softphones).
- Paso 2: El equipo del emisor pregunta por el equipo del receptor.
- Paso 3: El servidor VoIP devuelve datos de contacto al emisor (puertos, direcciones IP).
- Paso 4: Se establecen comunicación entre los interlocutores.

Todo ello utilizando un protocolo determinado: SIP, IAX2, H323, MGCP.

11.3. DISPOSITIVOS DE HARDWARE Y SOFTWARE

Los dispositivos de hardware o software implicados en esta tecnología son:

- Teléfonos IP: Físicamente, son teléfonos normales, con apariencia tradicional. Incorporan un conector RJ45 para conectarlo directamente a una red IP en Ethernet. No pueden ser conectados a líneas telefónicas normales. Ejemplos son: SNOM 360, Sipura 841.
- Adaptadores análogicos IP: Permiten aprovechar los teléfonos analógicos actuales, transformando su señal analógica en los protocolos de VoIP.
- Softphones: La telefonía por Internet, también conocida como "softphone", son aplicaciones que permiten utilizar el ordenador como si se tratara de un teléfono. Son programas que permiten llamar desde el ordenador utilizando tecnologías VoIP. Ejemplos son: Skipe, GoogleTalk, X-Lite o WengoPhone
- Centralitas IP: Centralitas de telefonía o PBX que permiten utilizar de forma combinada la tecnología VoIP (mixtas) o exclusivamente IP (puras). Algunas de sus funcionalidades más interesantes son: la transferencia de llamadas, música en espera, registro de llamadas en BD, buzón de Voz por Mail, llamada en espera, salas de Conferencia, Pickup de llamadas, identificador de llamadas, Buzón de Voz personal y otras.

En resumen, un gran número de dispositivos que pueden habilitar el servicio de comunicaciones IP con varias soluciones, algunas de las cuales permite el uso del aparato telefónico tradicional con interface a la red IP.

11.4 TELEFONÍA IP

La telefonía IP realiza el transporte de las llamadas telefónicas a través de la red Internet, sin importar si es a través de los dispositivos de telefonía tradicional, computadoras personales con multimedia o terminales dedicadas.

Para este propósito, los agentes implicados son:

- Usuarios VoIP: Utilizan tecnologías VoIP para realizar llamadas.
- Proveedores de VoIP: Su principal servicio es el de hacer de pasarela hacia la red telefónica pública (conocida como PSTN/POTS) a costes muy reducidos. Las llamadas entre usuarios de un mismo proveedor son gratuitas, en algunos casos existen 'prefijos' para saltar entre redes de proveedores conocidos.
- Carriers de VoIP: Venden sus rutas VoIP a los proveedores, son 'mayoristas' de minutos IP.
- Terminadores VoIP: Venden sus líneas para llamar a telefonía tradicional a los proveedores de VoIP.
- Integradores de Soluciones VoIP: Conectan centralitas a VoIP, servidores dedicados para servicios adicionales, conexiones CRM -> VoIP, Softphones.

La relación de los agentes implicados se muestra en la siguiente figura:

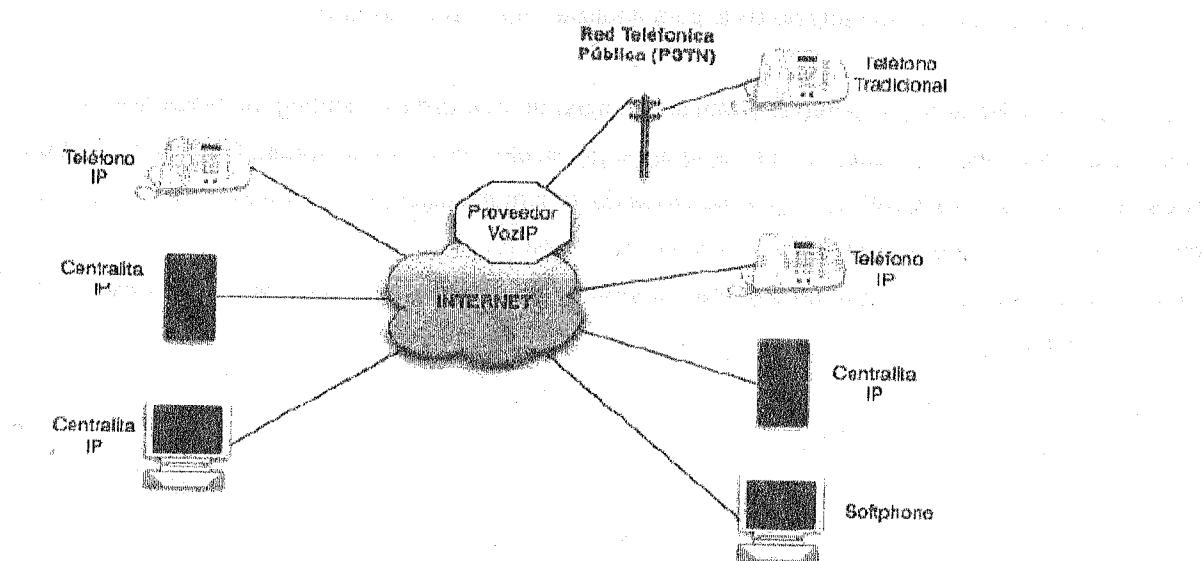


Fig. 11.1 Telefonía IP

11.5 ESTÁNDARES DE VoIP

Dos de los protocolos más populares utilizados para la comunicación VoIP son el protocolo de inicio de sesión (SIP) y H.323. Aunque el primero que apareció fue H.323, SIP se considera más fácil de implementar y usar.

11.5.1 Protocolo de Inicio de Sesión (SIP)

Protocolo de aplicación diseñado por el IETF¹, establece, gestiona y finaliza una llamada (voz sobre IP), texto o en general sesión multimedia. Se utiliza para crear sesiones entre dos personas, entre varias o sesiones de multienvío. Utiliza un servicio de transporte confiable o no confiable, es decir, los protocolos TCP y UDP. La distribución de contenido multimedia a través del internet se basa en el protocolo de transporte de tiempo real RTP y el Protocolo de control de transporte de tiempo real RTCP. Ambos se colocan entre UDP y el programa de aplicación.²

Los mensajes SIP son codificados en formato de texto ASCII, como consecuencia, son mensajes grandes y poco adecuados cuando es crítico el ancho de banda o la demora. Cada mensaje tiene una cabecera y un cuerpo. La cabecera describe la estructura del mensaje, las capacidades del que llama, el tipo de medio, etc.

En una sesión SIP entre el equipo Transmisor y el Receptor se utilizan tres fases:

1. Establecimiento. A través del envío de los mensajes INVITE para iniciar la sesión y ACK de confirmación
2. Intercambio de audio y
3. Cierre. Enviendo el mensaje BYE para finalizar una sesión sencilla.

Para una comunicación con teléfonos convencionales, un número de teléfono identifica al emisor y otro número identifica al receptor. En cambio, el protocolo SIP es más flexible, pues acepta otros tipos de formatos para identificar a los extremos de la comunicación, por ejemplo: una dirección de correo electrónico, una dirección IP o un número de teléfono.

Si el receptor está al otro lado del terminal, la sesión SIP se denomina sencilla y se representa en la siguiente figura:

¹ The Internet Engineering Task Force

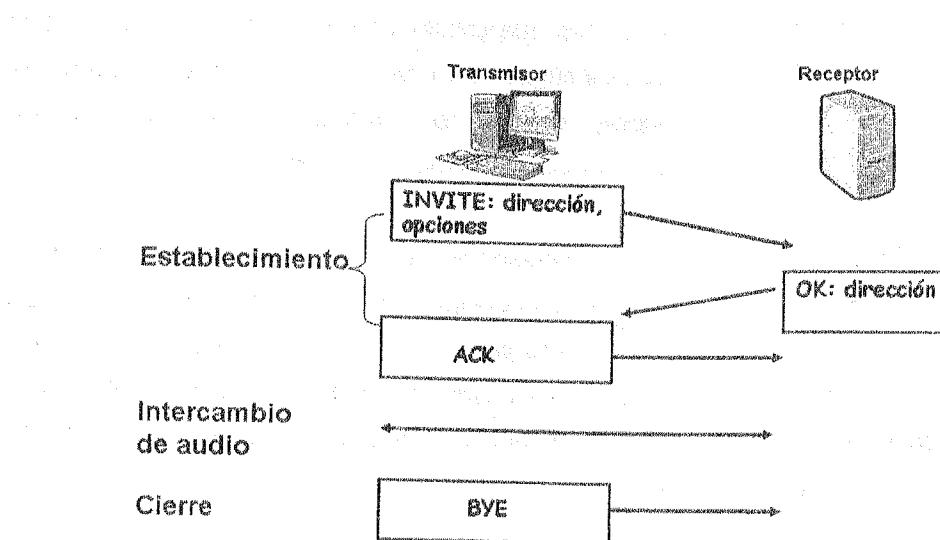


Fig. 11.2 Sesión sencilla SIP

Sin embargo, en una situación real, el receptor puede estar en otra terminal o incluso no tener una dirección IP fija (si utiliza DHCP). Para ello se añaden uno o más servidores proxy SIP.

Servidor Proxy SIP

Es una aplicación intermedia que actúa tanto como servidor y cliente, generando mensajes SIP a nombre del cliente que generó el mensaje original. Los mensajes pueden ser respondidos o encaminados a otros servidores, el proxy los interpreta, re-escribe o traduce los mensajes antes de encaminarlos.

Un mismo servidor puede funcionar como Proxy entrante y saliente de un dominio

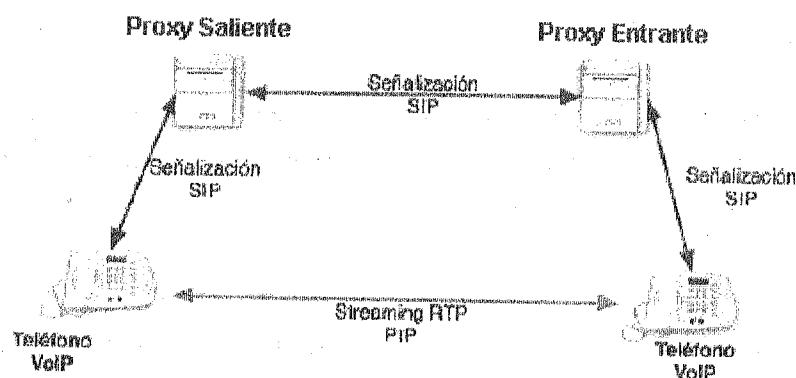


Fig. 11.3 proxys SIP

SIP tiene un mecanismo, similar al utilizado en DNS, que encuentra la dirección IP del terminal en el que se encuentra el receptor. Para realizar este seguimiento, SIP utiliza el concepto de registro. SIP define algunos servidores como registradores. En cualquier momento un usuario se registra en al menos un servidor de registro; este servidor conoce la dirección IP del receptor.

Cuando un transmisor desea comunicarse con un receptor, el transmisor puede utilizar la dirección de correo electrónico en lugar de la dirección IP en el mensaje INVITE, el mensaje va a un servidor Proxy, éste envía un mensaje de búsqueda (no forma parte de SIP) a algún servidor de registro. Cuando el servidor Proxy recibe un mensaje de respuesta del servidor de registro, el servidor Proxy toma el mensaje INVITE de transmisor e inserta la nueva dirección IP descubierta del receptor. Este mensaje es enviado al receptor.

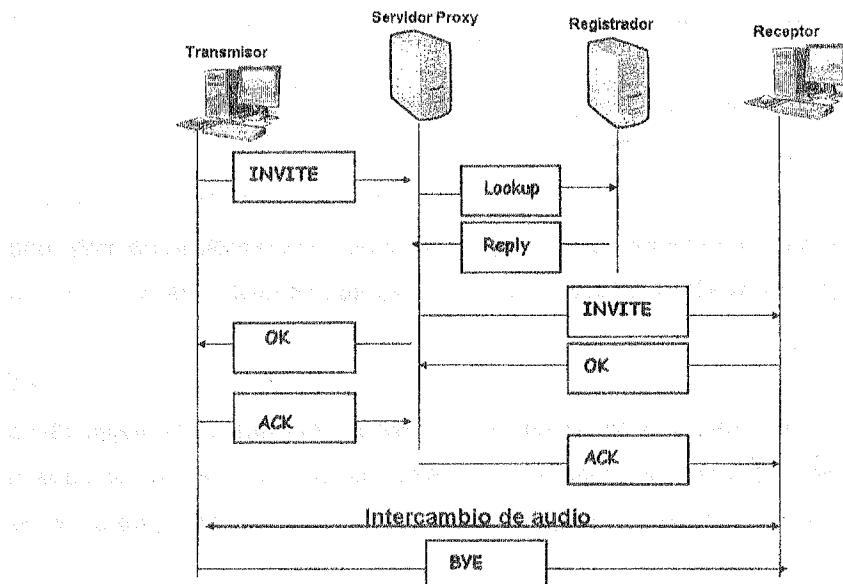


Fig. 11.4 Comunicación transmisor/receptor SIP

11.5.2 Protocolo H.323

H.323 es un estándar definido por la ITU² mediante el cual, se establece la comunicación multimedia sobre redes IP que incluye audio, video y datos. Sus mensajes están codificados en formato binario por máquinas con decodificadores como Ethereal.

La primera versión de H.323 (1996) se define como *Sistemas y equipos videoteléfonicos para redes de área local que proporcionan una calidad de servicio no garantizada*" se cambió en la versión 2 por *coherencia con la ampliación de su alcance*.

Al igual que el protocolo SIP, tiene ambos servicios de transporte: el confiable TCP y el no confiable UDP. Para la distribución de contenido multimedia en Internet, también utiliza los protocolos RTP y RTCP.

La comunicación multimedia punto a punto entre dos puntos extremos H.323, empieza con el procedimiento de establecimiento de la comunicación y termina con el procedimiento de terminación de la llamada. La llamada está formada por el conjunto de canales fiables y no fiables entre los puntos extremos. Una llamada puede producirse directamente entre dos puntos extremos o puede implicar a otras entidades H.323 tales como un controlador de acceso sencillo o multipunto (MC).

Los elementos de una arquitectura H.323 son:

- Las terminales. Puntos extremos de la red que proveen comunicación de audio, video y datos a otra terminal H.323.
- Gateways o Pasarelas. Conecta Internet a la red PSTN telefónica u otra red H.323.
- Gatekeepers. Proveen traducción de dirección, control de acceso, gestión de ancho de banda y otras operaciones de administración.
- Unidades de control multipunto (MCU). Permite que tres o más terminales participen en una conferencia multipunto.

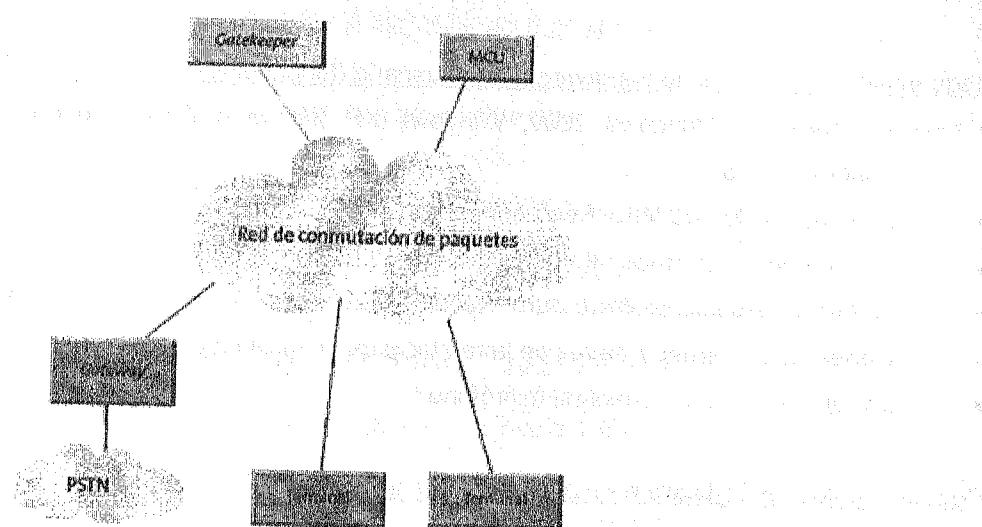


Fig. 11.5 Arquitectura H.323

11.6 CARACTERÍSTICAS DE EQUIPOS Y SOFTWARE DE COMUNICACIÓN PARA VOIP

En este apartado, vamos a definir alguna de las características de hardware y software que requiere una institución con red local instalada y con intenciones de implementar el servicio de VoIP para sus funcionarios con el propósito que el servicio telefónico sea eficiente para la gestión administrativa de la institución.

11.6.1 Para comunicación dentro de la institución

El funcionario de la institución que desee efectuar llamadas, deberá recurrir a su computadora provista de micrófono y parlantes que reemplazarán al aparato telefónico tradicional. El servicio es gratuito.

Las llamadas externas a la institución, no son gratuitas porque se requiere de un proveedor de VoIP para la interface de comunicación con la red telefónica tradicional.

a) Uso de Softphones

El servicio de VoIP que ofrecen Google Talk o Skype para este caso es gratuito.

Requerimientos mínimos de Hardware para el usuario (funcionario)

- PC corriendo Windows 2000, Windows XP (Home o Pro), Windows Server 2003 o Windows Vista.
- Procesador de 400 Mhz. Recomendable 1 Ghz
- 128 MB en RAM. Recomendable 256 MB en RAM
- 15 MB de espacio en disco duro. Recomendable 30 MB
- Conexión a Internet a través de la red local de la institución
- Tarjeta de sonido, parlantes, micrófono

Requerimientos de Software para el usuario (funcionario)

En el caso de Google Talk, suscripción gratuita a correo Gmail, descargar e instalar el software en español (1.3 MB) de esta dirección: <http://www.google.com/talk/intl/es/index.html>

Si se usa Skype, también el software está en español y es gratuito, descargarlo de esta dirección: <http://www.skype.com/intl/es/download/skype/>

b) Uso de una Centralita de VoIP

En el núcleo de la red local de la institución, deberá instalarse un servidor Proxy provisto de una centralita o PBX para VoIP. Una referencia se muestra en la sgte. figura:

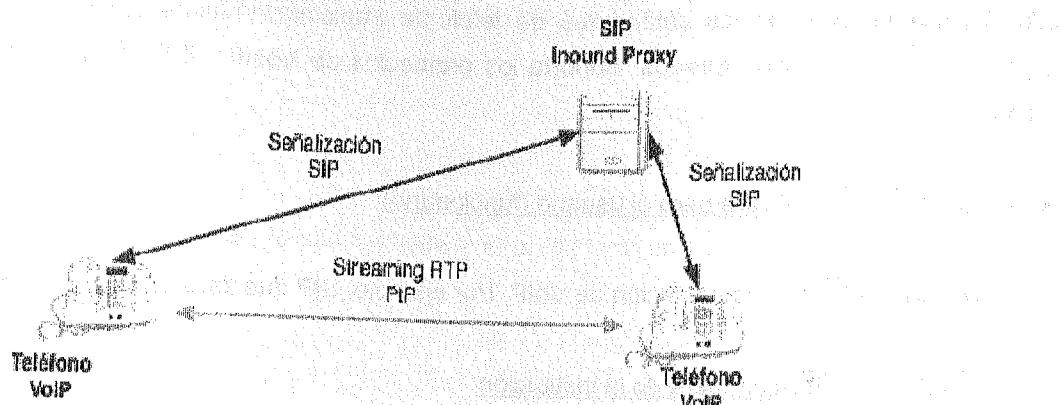


Fig. 11.6 Comunicación con centralita para VoIP

Requerimientos mínimos de Hardware para la administración de la red local de la institución.

Para el Servidor, se tiene el siguiente cuadro comparativo de dos marcas prestigiosas y recomendables.

COMPARACION DE SERVIDORES IBM Y HP

Modelo Variable	IBM X Series 255	HP Proliant DL 580 G3
Procesador	Xeon MP de 4 vías hasta 2 Ghz	Xeon MP de 4 vías hasta 2, 6 Ghz
Memoria	Hasta 12 GB Chipkill™ Memory	Hasta 4 GB
Almacenamiento interno	SATA hasta 640 MB SCSI hasta 1 TB	SATA hasta 640 MB SCSI hasta 1.2 TB
Slots de expansión	(7) 5 NHP PCI-X 2 HP PCI-X o NHP PCI-E	(8) 3.3 Volt PCI-X I/O Slots: (6) 64-bit / 100 MHz PCI-X, (2) 64-bit / 100 MHz PCI-X
RAID	Opcional RAID-4	Hot RAID

Cuadro 11.1 Requerimientos mínimos de Hardware para el usuario

Si la conexión es de la centralita al equipo del usuario, éste deberá tener los mismos requerimientos mínimos que del caso anterior, además de tarjeta de red. También es posible utilizar teléfonos IP que son aparatos telefónicos con la misma apariencia física que los teléfonos tradicionales. Utilizan tecnologías VozIP y normalmente permiten realizar ciertas funcionalidades avanzadas como la llamada en espera. Un modelo compatible con Asterisk es IAXy™.

Requerimientos de Software para la administración de la red local.

Una centralita o PBX para VoIP de software abierto con versiones comerciales, <http://www.digium.com> muy recomendable es Asterisk que corre bajo plataforma Linux. Trabaja con prácticamente todos los estándares de telefonía tradicional: Líneas analógicas y Líneas digitales: E1, T1, accesos básicos. Soporta los protocolos de VoIP: SIP, IAX2, MGCP, Cisco Skinny.

Requerimientos de Software para el usuario (funcionario)

Un protocolo cliente de comunicación de VoIP. Por ejemplo, SIP que tiene una versión libre.

11.6.2 Para comunicación fuera de la institución

El funcionario que desee comunicarse con algún teléfono de la red pública local, nacional o internacional tendrá las sgtes. Opciones:

a) Uso de Softphones.

El servicio de VoIP que ofrecen Google Talk o Skype para este caso No es gratuito.

Requerimientos mínimos de Hardware para el usuario (funcionario)

Los mismos para el caso anterior, pero además se requieren adaptadores telefónicos y gateway para la interface o pasarela hacia la red telefónica.

Un ejemplo de gateway para utilizarse con el servicio Skype es el modelo DPH-50U, permite recibir llamadas procedentes de teléfonos ordinarios y Skype en el mismo teléfono. Los adaptadores para este servicio, (modelo Zonet Sky-USB).

b) Uso de una Centralita de VoIP

Los requerimientos de hardware y software tanto para el funcionario como para la administración de la red local, son los mismos que para la comunicación dentro de los predios de la institución. La forma de operar para una centralita Asterisk, cuando un usuario marca un número es la siguiente:

- Si el número empieza por 0, llamar al destino utilizando un proveedor externo.
- Si el número tiene 3 cifras y empieza por 1, llamar a un determinado usuario de la centralita.
- Si cuando llamamos a ese usuario, no contesta en 60 segundos, reproducir un mensaje de alerta.

11.7 CONCEPTOS Y TERMINOS CLAVE

Adaptadores analógicos IP

Características de equipos y software de comunicación para VoIP

Centralitas IP

Dispositivos de Hardware y Software

Funcionamiento de VoIP

Fundamentos de VoIP

Protocolo H.323

Protocolo SIP

Requerimiento de software para la administración de la red local con VoIP

Servidor Proxy SIP

Servidores para VoIP

Softphones

Telefonia IP

Telefonia Tradicional

Teléfonos IP

11.8 PREGUNTAS DE REPASO

1. Indicar dos características de la telefonía tradicional
 - A. Garantía de disponibilidad, diseñado con perspectivas futuras a utilizarse en telefonía móvil
 - B. Sector regulado, no garantiza la disponibilidad
 - C. Recursos ocupados durante toda la duración de la llamada, diseñado para solo voz
 - D. Ninguno de los anteriores
2. En la telefonía VoIP, porque se dice que los usuarios no están limitados a una ubicación física específica
 - A. VoIP es móvil
 - B. VoIP está basada en Internet
 - C. Porque los usuarios pueden cambiar su número
 - D. Porque los usuarios disponen de varios teléfonos
3. Sobre que tipo de red puede operar VoIP
 - A. Una intranet corporativa, Internet
 - B. Internet, ARPANET
 - C. Red Simplex
 - D. Ninguna de las anteriores
4. En que tipo de dispositivos se puede implementar la tecnología VoIP
 - A. PC's
 - B. Teléfonos IP
 - C. aparato telefónico tradicional
 - D. Todos los anteriores
5. Indicar un protocolo de comunicación a nivel de Aplicación que utiliza VoIP
 - A. H323
 - B. 802.11
 - C. RIP
 - D. HTTP
6. Que se denomina el dispositivo que permite utilizar el ordenador como si fuera un teléfono
 - A. VoIPphone
 - B. Softphone
 - C. PCphone
 - D. Adaptador analógico IP

7. Que dispositivo permite aprovechar los teléfonos analógicos actuales, transformando su señal en los protocolos de VoIP.
 - A. VoIPphone
 - B. Softphone
 - C. PCphone
 - D. Adaptador analógico IP
8. Indicar las fases del protocolo de comunicación Inicio de Sesión (SIP)
 - A. Establecimiento, intercambio de audio y cierre
 - B. Establecimiento, transmisión y cierre
 - C. Gestión y cierre
 - D. Establecimiento y gestión
9. Cual es el formato de los mensajes SIP
 - A. Comprimido gzip
 - B. Texto EBCDIC
 - C. Texto ASCII
 - D. Código encriptado
10. Que tipos de formatos acepta SIP para identificar a los extremos de la comunicación.
 - A. Número telefónico
 - B. Dirección de email
 - C. Dirección IP
 - D. Todos los anteriores
11. Que tipo de comunicación se puede establecer con el protocolo H323
 - A. Texto
 - B. Multimedia
 - C. Voz
 - D. Sonido
12. Indique dos elementos de una arquitectura H323
 - A. Teléfono, terminal
 - B. Unidades de control multipunto, controlador
 - C. Terminal, gateways
 - D. Terminal, unidad móvil

13. Cuales son las opciones de comunicación VoIP al interior de una institución

- A. Hardphones
- B. Softphones
- C. Uso de centralita VoIP
- D. B y C

14. Indicar una aplicación softphone

- A. Skype
- B. Youtube
- C. Picasa
- D. Mozilla

15. En que dispositivo de hardware se instala una centralita VoIP

- A. Servidor Principal
- B. Servidor Proxy
- C. Una terminal
- D. Un router

11.9 TALLER

1. Comparar en por lo menos 5 criterios la telefonía tradicional con la telefonía IP
2. Se desea instalar VoIP en una institución mediana con alrededor de 100 empleados
 - a. Justificar el método a seguir y
 - b. Explicar las características de hardware y software que se requieren.
3. Investigar los requerimientos para obtener los servicios de Skype y de Google Talk y compararlos.
4. Comparar los protocolo SIP y H323

A1.1 Red Ethernet

El término Ethernet se refiere a la familia de redes LAN desarrolladas bajo la norma IEEE 802.3. Esta incluye a la original 10 Mbps, 100 Mbps Fast Ethernet, 1000 Mbps Gigabit Ethernet y 10 Gigabit Ethernet. En la siguiente figura se muestra una clasificación de éstas.

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbps	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbps	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbps	Fibra óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100Mbps	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex(hub) y Full Duplex(switch)
100BaseTX	100Mbps	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex(hub) y Full Duplex(switch)
100BaseFX	100Mbps	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	1000Mbps	4 pares trenzado (categoría 5UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseSX	1000Mbps	Fibra óptica (multimodo)	560 m	Estrella. Full Duplex (switch)
1000BaseLX	1000Mbps	Fibra óptica (monomodo)	5000 m	Estrella. Full Duplex (switch)

Fig. A.1 Tecnologías Ethernet

Ethernet usa el sistema de comunicación broadcast para la transmisión de tramas de datos entre los hosts localmente distribuidos (Metcalfe, 1976).

En la figura que se muestra a continuación, se muestra la idea básica del concepto de Ethernet. Las estaciones antes de transmitir deberían detectar si el canal ya estaba en uso, en cuyo caso esperarían a que la estación activa terminara.

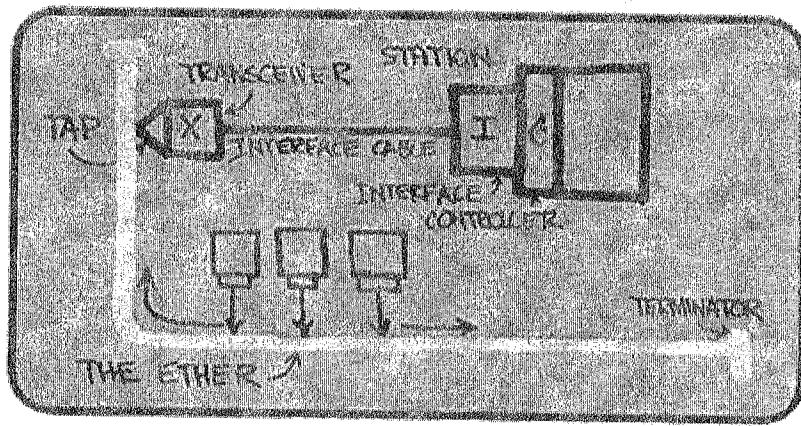


Fig. A.2 Un dibujo del concepto de Ethernet (1976) por R. Metcalfe tomado de Charles Spurgeon's Ethernet Web Site.

Además, cada estación mientras transmitiera estaría continuamente vigilando el medio físico por si se producía alguna colisión, en cuyo caso se pararía y retransmitiría más tarde.

El “Ether” es el medio físico por donde va la señal. Este protocolo de comunicación se conoce como Acceso Múltiple con Detección de Portadora y Detección de Colisiones, o más brevemente CSMA/CD (Carrier Sense Multiple Access / Collision Detect).¹ Actualmente las redes Ethernet no necesariamente tienen como método de acceso a CSMA/CD.

A1.2 Red Token Ring

En esta red que está desarrollada bajo la norma IEEE 802.5, todos los nodos de la LAN (hosts y routers) están organizados en una topología tipo anillo. Cuando un nodo obtiene el “token” (objeto virtual) y envía una trama, la trama se propaga a lo largo del anillo secuencialmente, creando un canal broadcast virtual. El nodo que envía la trama tiene la responsabilidad de eliminar la trama del anillo. Este anillo es lógico y no físico respecto a como los hosts están conectados a un hub o switch central. Los usuarios son parte del anillo, como se muestra en la figura.

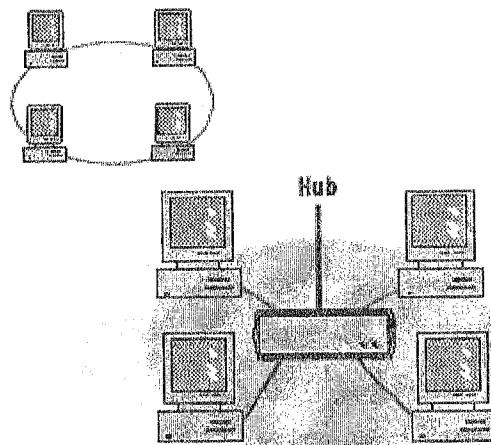


Fig. A.3 Token Ring con topología anillo y cableado estrella

Esta tecnología soporta rangos de transferencia entre 4 a 16 Mbps.

¹ Este protocolo lo describiremos en el capítulo de la capa Física

A1.3 Red FDDI

Las redes FDDI (Fiber Distributed Data Interface) fueron diseñadas para redes LAN geográficamente más grandes o Areas Metropolitanas que cubren varios kilómetros. Describe a redes de alta velocidad (100 Mbps) con topología de doble anillo, envío de token a cientos de hosts y uso de cable de fibra óptica como backbone de una red.

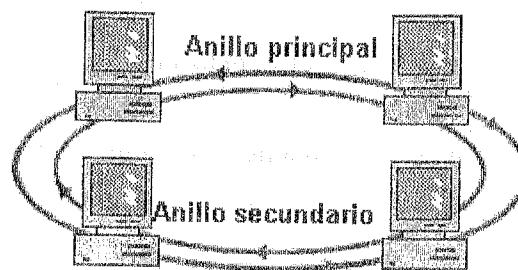


Fig. A.4 Red FDDI con anillo dual

Generalmente el tráfico fluye solo en el anillo principal, pero si éste falla, automáticamente se reconfigura la red y fluye sobre el anillo secundario en sentido contrario.

BIBLIOGRAFIA

1. Ahuja Sudhir. VoIP What is it good for?. Revista QUEUE Septiembre 2004. pp 49-55.
2. APNIC 24 Plenary Session: "The Future of IPv4," September 2007.
<http://www.apnic.net/meetings/24/program/plenaries/apnic/>
3. [AT&T,2005] AT&T Network Design and Consulting Division. USA 2005
4. [Asterisk, 2005] The Future of Telephony. Jim Van Meggelen, Jared Smith & Leif Madsen – O'Reilly
5. Cisco Networking Academic Program. Cisco Press. 2000
6. Douglas Comer. Redes globales de información con internet y TCP/IP. Prentice Hall, México 1996.
7. Fenzi, K., 2000: Linux Security HOW TO v1.1.1, 17 March 2000
8. Fletcher. Exploring Quizzing in Macromedia Captivate. [en linea] 2007; 11(20) p:1-9. Disponible en:
<http://www.adobe.com/devnet/captivate/articles/quiz.html>
9. Forouzan Behrouz. Transmisión de datos y redes de comunicaciones. 4ta Edición Mc Graw Hill. 2007
10. Gallardo Portanda Ramiro. Estrategias de utilización de las TIC para el docente de la UMSA. [en linea] 2004; p:1-8 . Disponible en:
<http://www.haciaelcongreso.umsa.bo/images/stories/presentaciones/estrategiasdeutilizaciondelasticparaeldocente de la umsa lic ramiro gallardo 261007.pdf>

11. Goan, T., 1999: A Coap on the Beat:Collecting and Appraising Intrusion. Communication of the ACM. July 1999. Vol 42 No. 7
12. Huidobro Joé Manuel. El auge de las redes inalámbricas(WLAN).Revista Antena de Telecomunicación. Diciembre 2002.
13. Huston Geoff. TCP Performance, The Internet Protocol Journal Vol 3, Número 2, June 2000.
14. International Data Corporation (IDC) Disponible en <http://www.idc.com>
15. Kurose & W. Ross. Computer Networking A top down approach. Ed. Adison Wesley. 2004.
16. McAFFEE John. Computer Viruses, Worms, Data Diddlers, Killer Programs and other Threats to Your System. Ed. ST. MARTIN PRESS New York 1989
17. McQuerry Steve. Interconexión de dispositivos de red Cisco. Ed. Cisco Press. Madrid, 2001.
18. Mei M.,& Borowski B., 2000: Introducción a la seguridad y al trabajo en red con linux, ACM, 2000
19. Metcalfe Robert, and David R. Boggs. "Ethernet: Distributed Packet Switching for Local Computer Networks," Communications of the Association for Computing Machinery, Vol19/No 7, July 1976.
20. Minguet Jesús. Informática Fundamental. 2da Edición. Editorial Universitaria Ramón Areces 2008
21. Mohanty S. A new architecture for 3G and WLAN integration and inter-system handover management. Wireless Netw (2006) 12:733–745
22. Nice, D., 2000: Why Firewalls Are not Enough,disponible: <http://www.networkice.com/Library/firewalls.htm>.

23. Northcutt S., Novak J., 2001: Detección de Intrusos 2da. Edición. Ed. Prentice Hall. 2001
24. Pfleeger, Ch.,1997: Security in Computing, Prentice Hall New York 1997.
25. Rodriguez Adolfo. TCP/IP Tutorial and Technical Overview. IBM Disponible en <http://www.redbooks.ibm.com>
26. Spafford E. 2000. Data collection mechanisms for intrusion detection systems. CERIAS Technical Report 2000-08. Purdue University. June 2, 2000.
27. R. Steinmetz and K. Wehrle, P2P Systems and Applications, Springer Lecture Notes in CS, 2005.
28. Northcutt Stephen, Guía Avanzada Detección de intrusos. 2da. Edición . Prentice Hall, Madrid 2001
29. Charles Spurgeon's Ethernet Web Site. Disponible en: <http://www.ethermanage.com/ethernet/ethernet.html>
30. The Internet Protocol Journal. Disponible en <http://www.cisco.com>
31. Tim Berners-Lee, Robert Cailliau, Jean-François Groff, and Bernd Pollermann. World-Wide Web: The Information Universe. ELECTRONIC NETWORKING, Vol. 2, No. 1, Spring 1992, pp. 52-58. © 1992 Meckler
32. Zacker Craig. Networking Essentials. Ed. Digital Think 1999.

