

Módulo II: Redes de Datos

Autores: Juan Carlos Caldera Palma
Wilberth Elieser Suazo Sequeira

Coordinador: Msc. Ing. Marlon Ramírez

ÍNDICE

UNIDAD 1. INTRODUCCIÓN A REDES DE DATOS	3
1.1 INTRODUCCIÓN	3
1.2 TIPOS DE REDES DE DATOS	6
1.2.1 REDES ENTERPRISE	9
1.3 TOPOLOGÍAS DE REDES DE DATOS.....	10
1.3.1 TOPOLOGÍAS LÓGICAS.....	11
1.3.1.1 Topología Punto a Punto.....	11
1.3.1.2 Topología multi - acceso.....	12
1.3.1.3 Topología de anillo	15
1.3.1.4 Topología de malla.....	16
1.3.1.5 Topología de árbol jerárquico	17
1.3.2 TOPOLOGÍAS FÍSICAS.....	17
1.3.2.1 Topología de estrella.....	18
1.3.2.2 Topología de árbol jerárquico	19
1.4 REDES INALÁMBRICAS	19
1.4.1 CATEGORÍAS DE REDES INALÁMBRICAS.....	20
1.4.2 SEGURIDAD EN REDES INALÁMBRICAS.	21
1.4.2.1 WEP	21
1.4.2.2 WPA.....	23
1.5 LA RED COMO PLATAFORMA MULTISERVICIOS.....	24
1.6 TECNOLOGÍAS DE PROCESAMIENTO EN LA RED.	26
1.7 BREVE RESEÑA SOBRE ELEMENTOS DE UNA RED DE DATOS	28
1.8 ASPECTOS IMPORTANTES DE UNA RED DE DATOS	30
1.8.1 TOLERANCIA A FALLAS	30
1.8.1.1 Sistemas conmutados por circuitos vs Sistemas conmutados por paquetes.....	31
1.8.1.2 Jitter.....	33
1.8.1.3 Latencia.....	34
1.8.2 ESCALABILIDAD	35
1.8.3 CALIDAD DE SERVICIOS.....	36
1.8.3.1 QoS y Aplicaciones.....	37
1.8.3.2 Mantener el servicio activo acorde a su prioridad.....	38
1.8.3.3 Técnicas para alcanzar buena calidad de servicio.....	39
1.8.4 SEGURIDAD	42

1.8.4.1	Redes Virtuales Privadas.....	44
1.8.4.2	Firewalls.....	46
1.9	IMPORTANCIA EN TELEFONÍA	48
1.10	TÉRMINOS	49
1.11	PREGUNTAS DE CONTROL.	50

UNIDAD 2. ARQUITECTURA DE UNA RED DE DATOS **55**

2.1	INTRODUCCIÓN	55
2.2	ESTRUCTURA DEL MODELO DE REFERENCIA OSI	56
2.2.1	INTRODUCCIÓN.....	56
2.2.2	CAPAS DEL MODELO OSI	58
2.2.2.1	Capa física.....	58
2.2.2.2	Capa de enlace de datos.	58
2.2.2.3	Capa de red.....	62
2.2.2.4	Capa de transporte.....	63
2.2.2.5	Capa de sesión.....	64
2.2.2.6	Capa de presentación.....	64
2.2.2.7	Capa de aplicación	65
2.2.3	FUNCIONAMIENTO DEL MODELO OSI.....	66
2.2.3.1	Des-encapsulamiento de datos.	68
2.2.4	NORMALIZACIÓN EN EL MODELO OSI.....	69
2.2.5	PARÁMETROS Y PRIMITIVAS DE SERVICIO.....	70
2.3	MODELO TCP/IP	71
2.3.1	¿QUÉ ES TCP/IP?	71
2.3.2	TCP/IP EN EL MUNDO.....	72
2.3.3	FACTORES IMPORTANTES DE TCP/IP	72
2.4	PREGUNTAS DE CONTROL.	74

UNIDAD 3. PROTOCOLOS DEL MODELO TCP/IP **77**

3.1	CAPAS DEL MODELO TCP/IP	77
3.1.1	CAPA FÍSICA.....	77
3.1.1.1	NIC.....	77

3.1.1.2	Estándar V.24.....	79
3.1.1.3	Estándar Ethernet.....	82
3.1.1.4	Estándares relacionados.....	84
3.1.2	CAPA DE ACCESO A LA RED.....	85
3.1.2.1	Direccionamiento de tramas.....	85
3.1.2.2	Dispositivos de capa de enlace.....	88
3.1.2.3	Protocolos de enlace.....	94
3.1.2.4	Tecnologías de capa de enlace de datos.....	97
3.1.2.5	HLDC.....	97
3.1.2.6	PPP.....	100
3.1.2.7	Frame Relay.....	102
3.1.2.8	ATM.....	105
3.1.3	CAPA DE INTERNET.....	106
3.1.3.1	Router.....	106
3.1.3.2	Protocolo de red IPv4.....	111
3.1.3.3	Protocolo IPv6.....	112
3.1.3.4	Direccionamiento.....	115
3.1.3.5	Enrutamiento.....	121
3.1.3.6	Protocolo de enrutamiento OSPF.....	129
3.1.3.7	Protocolos externos de pasarela.....	131
3.1.3.8	Protocolo de Gateway externo- BGP.....	132
3.1.4	CAPA DE TRANSPORTE.....	133
3.1.4.1	Protocolos orientados a la conexión.....	133
3.1.4.2	Protocolo no orientado a la conexión.....	134
3.1.4.3	Protocolo TCP y UDP.....	134
3.1.4.4	Protocolo RTP y RTCP.....	143
3.1.5	CAPA DE APLICACIÓN.....	147
3.1.5.1	Servicios de capa de Aplicación de TCP/IP.....	147
3.1.5.2	Servidores.....	148
3.2	PREGUNTAS DE CONTROL.....	159
 <u>UNIDAD 4. MPLS.....</u>		<u>163</u>
4.1	INTRODUCCIÓN.....	163

4.2 ENCABEZADO MPLS DEL PAQUETE	165
4.3 COMPONENTES DE MPLS	167
4.4 OPERACIÓN DE UNA RED MPLS.	168
4.5 CREACIÓN DE ETIQUETAS.	169
4.6 DISTRIBUCIÓN DE ETIQUETAS.....	170
4.6.1 PROTOCOLO DE DISTRIBUCIÓN DE ETIQUETAS - LDP	170
4.6.2 MODOS DE ANUNCIO DE ETIQUETA	170
4.6.3 PROCEDIMIENTO DE DISTRIBUCIÓN DE ETIQUETA	171
4.7 UNIDADES DE DATOS DE PROTOCOLO LDP.....	173
4.7.1 MENSAJES DE EMPAREJAMIENTO.....	173
4.7.1.1 Mensaje Hello.	173
4.7.1.2 Mensaje de inicialización.....	174
4.7.1.3 Mensaje de notificación	175
4.7.2 MENSAJES DE DISTRIBUCIÓN DE ETIQUETAS.....	176
4.7.2.1 Mensaje de dirección.....	177
4.7.2.2 Mensaje de asignación de etiquetas.	177
4.7.2.3 Mensaje de solicitud de etiqueta.	179
4.7.2.4 Mensaje de liberación de etiqueta.	180
4.7.2.5 Mensaje de retiro de etiqueta	180
4.8 CLASIFICACIÓN DE ETIQUETAS	180
4.9 INTERCAMBIO DE ETIQUETAS MPLS	181
4.9.1 ENVÍO DE PAQUETES ETIQUETADOS	181
4.9.2 ENVÍO DE PAQUETES SIN ETIQUETAR.	181
4.9.3 LÍNEAS DE ETIQUETA CONMUTADA	182
4.10 VENTAJAS DEL ETIQUETADO.	182
4.11 CALIDAD DE SERVICIO.....	183
4.12 SERVICIO TELEFÓNICO IMPLEMENTADO EN REDES MPLS.	184
4.13 PREGUNTAS DE CONTROL.	186
<u>ABREVIATURAS.....</u>	<u>187</u>
<u>BIBLIOGRAFÍA.....</u>	<u>188</u>

Unidad I

Introducción a Redes de datos.

Objetivos General:

- Brindar al estudiante una visión general del entorno e importancia del estudio de redes de datos.

Objetivos Específicos:

- Señalar los tipos de redes de datos y sus topologías
 - Mencionar los distintos servicios de una plataforma multiservicios.
 - Identificar los parámetros importantes en el funcionamiento de una red de datos.
 - Determinar los diferentes componentes de una red de datos.
-

Unidad 1. Introducción a Redes de datos

1.1 Introducción

Los orígenes de las redes de datos se remontan a principios del siglo XIX en Francia y Suecia donde se desarrolló la primera red de telecomunicaciones. El sistema resulto ser muy ingenioso, consistía en una serie de molinos con espejos a sus lados (Ver Figura. 1-1), permitiendo reflejar la luz a larga distancia con patrones conocidos por ambos extremos. A este sistema se le conoció como telégrafo óptico. Y esta es la primera muestra de una red de datos. (Universidad Nacional Autonoma de Mexico).

Durante el siglo XX la tecnología clave fue la obtención, procesamiento y la distribución de la información. Entre otros acontecimientos, vimos la instalación de redes mundiales de telefonía, la invención de la radio y la televisión, el nacimiento y crecimiento sin precedentes de la industria de la computación, así como el lanzamiento de satélites de comunicación.

En el año de 1937, George Steblitz desarrollo su modelo K de computadora, para esta fecha existía una carrera por el diseño y construcción de un sistema de procesamiento de datos. Steblitz crea su computador a base de conglomerados y otras piezas de materiales “basura” o desperdicios, pero capaz de resolver ecuaciones complejas. Si bien este sistema no marco una línea importante en el desarrollo de una arquitectura de computadoras, como lo son las arquitecturas Harvard y John Von Newman. Sin embargo, si abrió un nuevo capítulo en la historia de la comunicación de datos; mientras Steblitz trabajaba en los laboratorios Bell el 11 de septiembre de 1940, logra transmitir un problema a su “calculador numérico complejo” en New York, con el uso de una máquina de telégrafo y recibe el resultado correcto. (GoldenInk)

Las redes de computadoras progresaron en gran medida en poco tiempo. Durante las dos primeras décadas de su existencia, los sistemas de computación tenían una estructura centralizada, por lo general, todo el equipo de cómputo se colocaba en una sala grande e independiente del resto de la empresa. Las compañías o universidades medianas apenas llegaban a tener un o dos computadoras, en tanto que las instituciones grandes tenían, cuando mucho una docena.

Al unir los sistemas de computadoras y de comunicación, los primeros se vieron fuertemente afectados en cuanto a su organización. El concepto de “centro de cómputo” colocado en una habitación donde los usuarios o trabajadores llevaban su información a ser procesada es obsoleto. Este modelo antiguo en el cual una computadora se encargaba de manejar todo el procesamiento de una empresa se reemplaza por un modelo que interconectan varias computadoras de menor capacidad para realizar el mismo trabajo. Se dice que dos computadoras están interconectadas si pueden intercambiar información. A

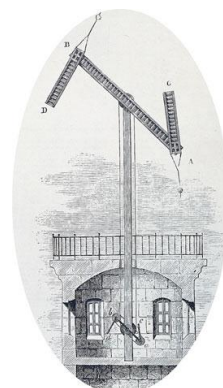


Figura. 1-1
Telégrafo Óptico

estos sistemas se les denomina redes de computadoras las cuales puede tener distintos tamaños y formas.

Es primordial aclarar que internet y Web no son una red de computadoras. El internet no es una red única, sino una red de redes, y Web es un sistema operativo distribuido que se ejecuta sobre Internet. El sistema distribuido aparece ante sus usuarios como un sistema consistente y único. Un ejemplo de sistema distribuido es World Wide Web. En una red de computadoras no se tiene esta consistencia o software de operación. Las máquinas de la red pueden utilizar sistemas operativos distintos y esto deberá ser completamente transparente para los usuarios. Por lo tanto, se puede observar que la principal diferencia entre Internet y sistema distribuido radica en el software. (Tanenbaum, 2003)

En la actualidad, muchas compañías tienen una cantidad considerable de computadoras. Una empresa podría tener computadoras separas para supervisar producción, controlar inventarios y hacer nómina. Pero a fin de recolectar información sobre el estado de toda la empresa surge la necesidad de conectar todos los equipos. Esto resalta como aspecto importante la compartición de recursos.

El objetivo de compartir recursos en una empresa es hacer que todos los programas, el equipo y en especial los datos que se procesan en cada ordenador estén disponibles para todos lo que se conecten a la red, independientemente de la ubicación física del recurso y del usuario.

En las compañías más pequeñas, es posible que todas las computadoras estén en una sola oficina o en un solo edificio, pero en las más grandes, las computadoras y los empleados pueden estar dispersos en docenas de oficinas y plantas en varios países. En estos casos, los datos están almacenados en computadoras de gran tamaño llamados servidores. Los empleados pueden acceder a estos “servidores” de forma remota. Este conjunto se conoce como modelo cliente-servidor. (Tanenbaum, 2003)

Otra aplicación de una red de computadoras en una empresa es hacer uso de esta como un medio de comunicación entre los empleados. Muchas de las empresas y universidades utilizan cuentas de correo electrónico a fin de mantener una comunicación diaria entre los empleados o docentes, respectivamente. Con una red es fácil que dos o más personas que trabajan a distancia escriban en conjunto un informe. Si un empleado hace un cambio a un documento en línea, los demás pueden ver el cambio de inmediato, en vez de esperar una carta durante varios días. Un ejemplo de esto es el programa TeamViewer el cual permite comunicar 2 ordenadores a través del escritorio desde cualquier lugar con acceso a Internet, de tal forma que los miembros manipulen u observen los cambios realizados en tiempo real.

Un nuevo uso de las redes es el trámite de compra y venta por parte de las compañías. Una compañía constructora puede hacer uso de este medio para comprar materiales provenientes de una empresa que se sitúa en otro país.

En el periodo de los noventa se dio un gran salto en el desarrollo de las redes caseras, específicamente en los años 1997 y 1998. El cable modem resulto ser la primera opción, sin embargo solo unos miles aceptaron el nuevo servicio en el primer año. Luego en 1999 surgió una nueva tecnología conocida como DSL, sin embargo su aceptación fue mucho menor a la de cable modem. El servicio de Internet satelital incluso en la actualidad no ha sido aceptado por la mayoría de la población debido al costo de este. (Company, 2010)

En cuanto a aplicaciones domésticas, el mercado de las computadoras inicialmente no perseguía el crear computadoras personales en gran volumen. Inicialmente se pensaba que solo se le daría uso a las computadoras en los hogares para el procesamiento de texto y juegos, pero en los últimos años esto ha cambiado radicalmente. La razón más importante en la actualidad puede ser el acceso a internet.

Algunos de los usos más comunes de internet por parte de usuarios domésticos son:

- Acceso a información remota
- Comunicación de persona a persona
- Entretenimiento interactivo
- Comercio electrónico

El acceso a la información remota se puede llevar a cabo por varios motivos. Puede ser que el usuario navegue en la red buscando información o solo diversión. Muchos de los periódicos, por ejemplo, la prensa y el nuevo diario poseen páginas de internet que se actualizan a diario permitiendo así que los lectores puedan informarse diariamente.

La comunicación de persona a persona a proporcionado la respuesta del siglo XXI al teléfono del XIX. Millones de personas utilizan a diario el correo electrónico, y de igual forma muchas utilizan los servicios de mensajes instantáneos. Como parte de las aplicaciones que se llevan a cabo en la comunicación de persona a persona, es el uso del internet como plataforma para realizar llamadas telefónicas, telefonía con video y la radio por internet.

El comercio electrónico se da a nivel de los hogares brindando el servicio de compra de materiales, muebles, equipos electrodomésticos o cualquier otra cosa que necesitare. Por ejemplo, las aerolíneas venden boletos de viaje desde sus páginas de internet de tal forma que el cliente puede realizar la compra con mucha facilidad desde la comodidad de su hogar u oficina, confirmar la reservación para lo cual normalmente el viajero debe estar 3 horas en el aeropuerto antes de su partida, e imprimirlo para su uso en el aeropuerto.

1.2 Tipos de redes de datos

¿Que es una red de datos?

Una red de datos consiste en 2 o más “hosts” que son interconectados de forma que puedan compartir recursos, tales como impresoras o archivos. Esto quiere decir que exista comunicación entre los hosts que pueden ser dos o más. El host¹ puede ser conectado a la red a través de cables, líneas telefónicas o cualquier otro medio de transmisión. (University of South Florida)

Existen algunos tipos de redes de datos, como por ejemplo:

Las **redes de Área Local** también conocidas LAN²_i (Ver Figura. 1-2), esta es una red delimitada a una pequeña área geográfica.³ En términos de medición de distancia, una red LAN no abarca más del área cubierta por una milla de diámetro. (University of South Florida)

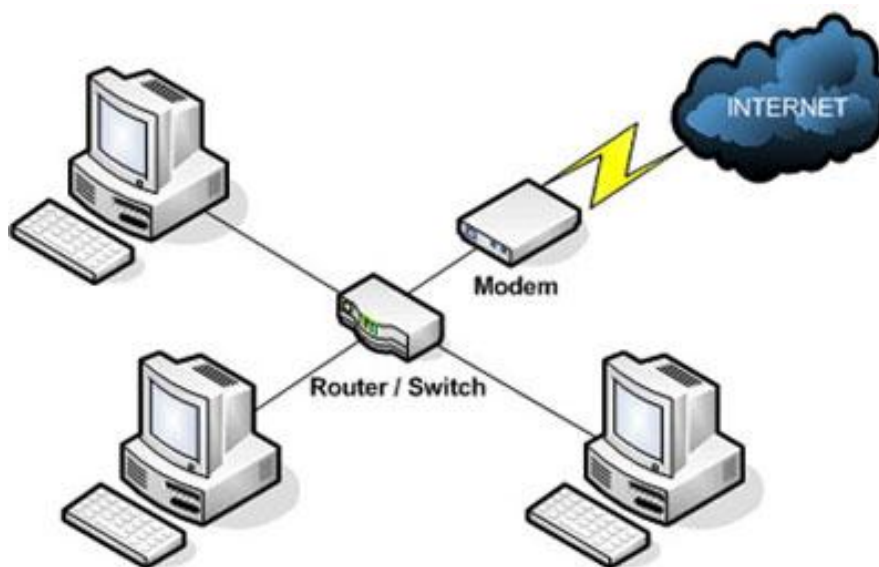


Figura. 1-2 Ejemplo de red LAN

En una red LAN la configuración más común es que uno de sus ordenadores sea programado como servidor de archivos (Ver Figura. 1-3). Este servidor almacena todos los softwares que controlan la red. Las computadoras conectadas a este servidor se les conocen como estaciones de trabajo. (University of South Florida)

¹ Se hace referencia a host como cualquier dispositivo que permita al usuario conectarse a una red de datos o hacer uso de esta. Un host puede ser un teléfono, computadora, impresora IP, etc.

² LAN = Local Area Network – Red de área local

³ Por pequeña área geográfica se entiende un laboratorio, escuela o un edificio.

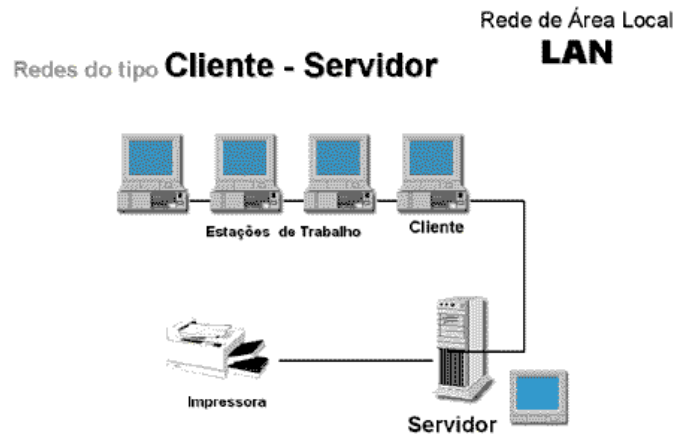


Figura. 1-3 Configuración Cliente-Servidor de una red LAN

En muchas redes LAN, los cables con usados para conectar las computadoras. Esto se hace utilizando cables UTP y conectores RJ-45. Estos terminales se introducen en el puerto Ethernet de la tarjeta de red. Esta parte de las conexiones físicas se abarcaran más adelante.

Antes de avanzar a redes WAN⁴_{ii} es necesario mencionar las redes de área metropolitana, o bien MAN⁵_{iii}, estas presentan una cobertura desde unos kilómetros hasta unos cientos de kilómetros y una velocidad de transmisión de Kbps a Gbps (Ver Figura. 1-4), sirve como *backbone* para conectar varias redes LAN. Puede proveer acceso a una red pública de área amplia. (GS Comunicaciones, 1999)

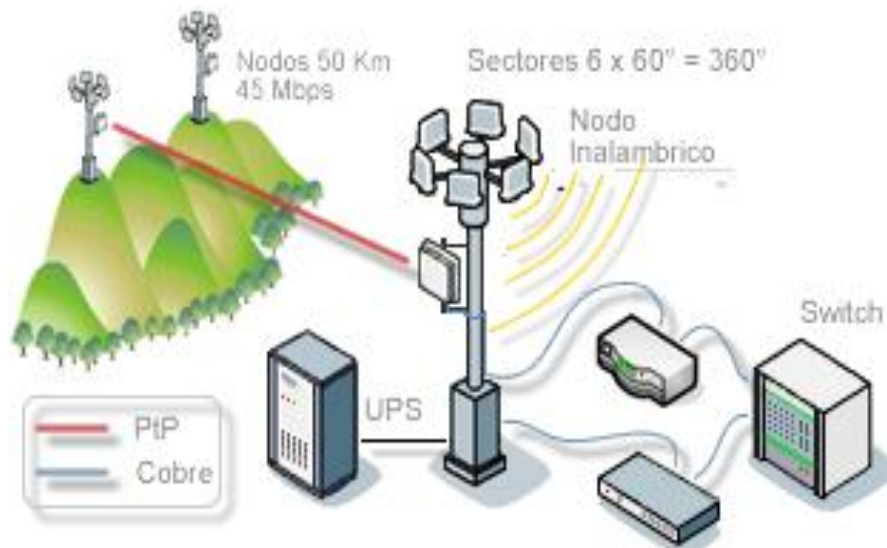


Figura. 1-4 Ejemplo de red MAN

⁴ WAN = Wide Area Network – Red de Área Amplia

⁵ MAN = Metropolitan Area Network – Red de Area Metropolitana

Las **redes de Área amplia** también conocidas como WAN, permite la conexión de grandes áreas geográficas (Ver Figura. 1-5). Para ilustrar mejor esta red, supongamos que se tiene una empresa y esta posee distintos edificios, como podría ser el caso de una cadena de bancos. En la actualidad si depositamos el dinero en la sucursal de un banco, tenemos la facilidad de retirarlo en esta o cualquier otra sucursal. Esto se debe a la existencia de base de datos que almacenan nuestros estados de cuenta pero para que los registros de todas las sucursales se actualicen a los depósitos o retiros que se realicen en otro edificio es necesaria la comunicación entre ellos y es en este punto donde se usan las redes WAN.

En cada banco existe una red LAN, pero estas redes se conectan entre sí a través de redes WAN compartiendo los archivos e información de cada usuario.

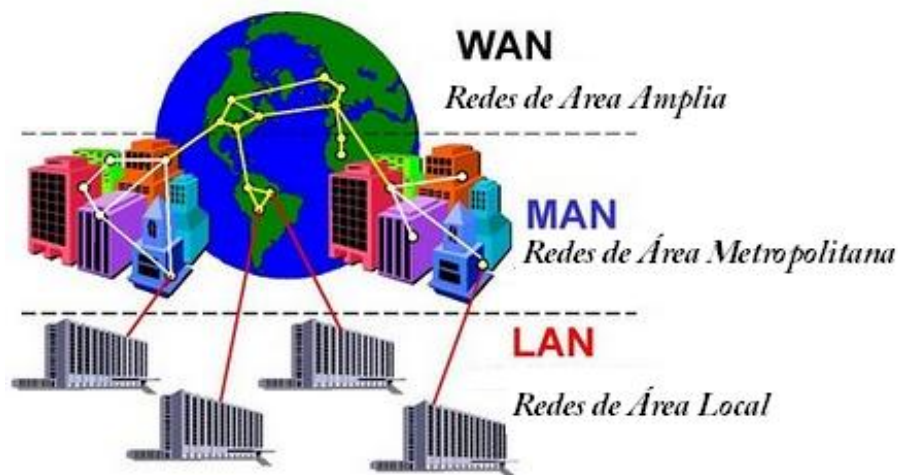


Figura. 1-5 Clasificación de Redes

En algunos casos las empresas deben utilizar a proveedores de servicios de telecomunicaciones para interconectar las redes locales que existen en cada una de sus sucursales. En estas situaciones los protocolos o reglas de comunicación en la red WAN están dados por los proveedores de dicha red, sin embargo en los extremos LAN, las reglas las establece el administrador de red.

La red WAN más grande y conocida es aquella que llamamos Internet pues esta no es más que la interconexión de un sin número de redes LAN, ya sean las redes LAN de nuestros hogares o las redes LAN de grandes empresas que brindan servicios de correo electrónico como Hotmail y Yahoo, empresas de venta e incluso LAN para redes sociales como Facebook.

También existen otros conceptos que se deben tomar en cuenta, como:

- **Internetwork:** Malla global de redes interconectadas pertenecientes a organizaciones públicas o privadas. Internet como tal es una de estas internetworks. (CISCO, 2008)
- **Intranet:** Se refiere a conexiones privadas de redes LAN y WAN que pertenezcan a organización. En este caso los miembros o empleados de la organización son los únicos que pueden acceder a esta red o los servidores que se encuentren en ella. (CISCO, 2008)

1.2.1 Redes Enterprise

El diseño, instalación y operación de redes de computadoras es vital para el funcionamiento de las organizaciones modernas. El término red Enterprise surge cuando se necesita interconectar las redes de organizaciones y los elementos que conectan estas.

El concepto de red Enterprise surge en la industria ya hace más de 10 años, definiéndose como una red de computadoras que resulta de interconectar las distintas redes existentes a lo largo de una organización. El objetivo principal de esta red es facilitar la computación empresarial, en la que los usuarios, a través de una organización, sean capaces de comunicarse entre sí y acceder a datos, servicios de procesamiento, aplicaciones y otros recursos, sin importar donde están localizados. (GS Comunicaciones, 1999)

La meta es brindar a las organizaciones una mejor comunicación para que satisficieran las necesidades de la computación empresarial a un costo razonable. La compatibilidad es un factor clave en la provisión de conectividad entre todos los usuarios y recursos en la red empresarial.

Bloques de construcción de una Red Enterprise.

La creación de una red Enterprise consiste en interconectar redes individuales, de tal manera que constituyen una red global. Generalmente las redes pequeñas utilizan tecnología de conectividad LAN y tecnología WAN.

El proceso de implementación constituye en primera instancia la identificación de redes existentes de una organización dentro de 2 categorías que se denominan: redes departamentales que utilizan tecnología LAN para interconectar los sistemas y las redes tradicionales que utilizan tecnología WAN para conectar los mainframes o estaciones de trabajo a grupos de terminales. (GS Comunicaciones, 1999)

1.3 Topologías de redes de datos

La forma en que opera una red está en dependencia de la estructura, arquitectura lógica, conexiones físicas, softwares de red y características de los dispositivos que le integran. Es importante saber que existen dos enfoques para el estudio, diseño e implementación de una red. Siendo estos las topologías lógicas de una red y la topología física. (Ver Figura. 1-6)

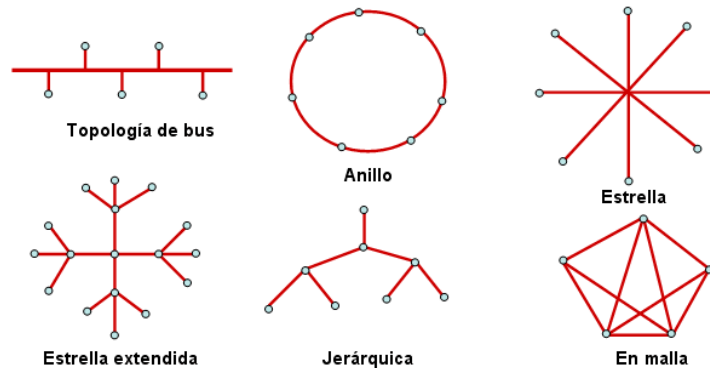


Figura. 1-6 Ejemplo topologías lógicas y físicas.

En esta parte, nos enfocaremos en el estudio de las topologías lógicas y físicas de los distintos tipos de redes. Las topologías lógicas no necesariamente representan la verdadera conexión física entre los dispositivos, que conforma la topología física. (Ver Figura. 1-7)

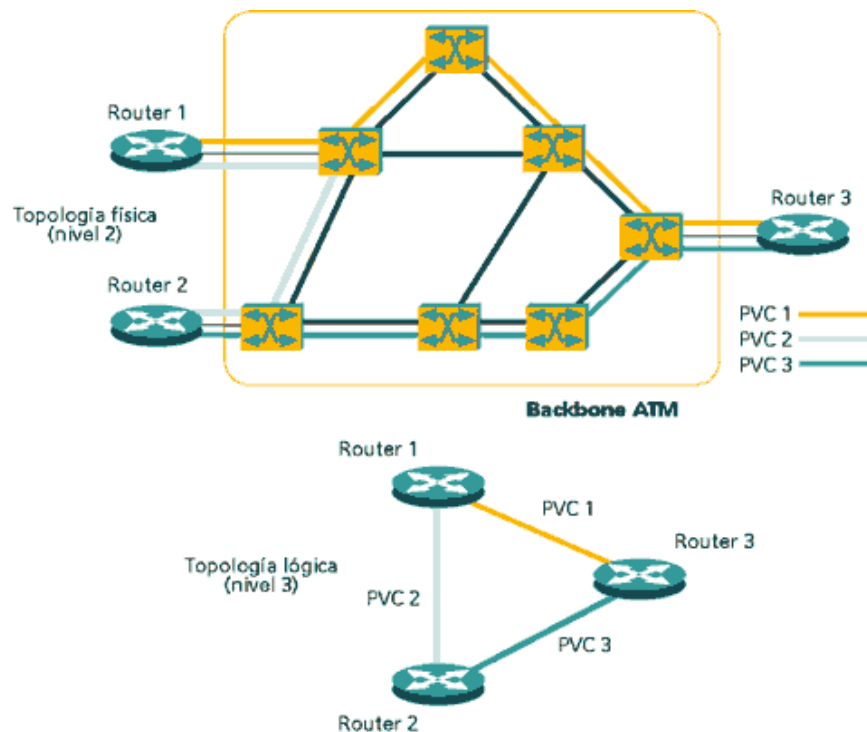


Figura. 1-7 Topologías Físicas y lógicas de una misma red de datos.

1.3.1 Topologías lógicas

Las topologías lógicas muestran de una forma estructurada el cómo se transfieren los paquetes de datos de un nodo hacia otro nodo en la red. Las conexiones son virtuales, lo que indica que una línea puede ser en la topología física una serie de elementos de red. Es en esta parte donde surge la necesidad de ocupar métodos de control a acceso al medio para evitar “colisiones” de paquetes de datos. (CISCO, 2008)

1.3.1.1 Topología Punto a Punto

Hemos decidido desarrollar la topología punto a punto (point to point) (Ver Figura. 1-8 (a)), debido a su gran presencia en el mercado. Esta topología es fundamental para el desarrollo de cualquier red, pues alguna de las redes que se mencionan más adelante como la red estrella está constituida de varias redes punto a punto.

Esta topología constituye la unión o conexión de dos nodos directamente, es por ello que la estructura es de fácil análisis. Los punto de transmisión y recepción son únicamente 2. El número de receptores y transmisores puede variar según el tipo de comunicación que se establezca. Si la comunicación es half-duplex (Ver Figura. 1-8 (b)), únicamente se puede existir un transmisor y receptor por trama de datos que se envíe. En el caso de comunicación full-duplex (Ver Figura. 1-8 (c)), ambos extremos o nodos pueden transmitir y recibir datos de forma simultánea.

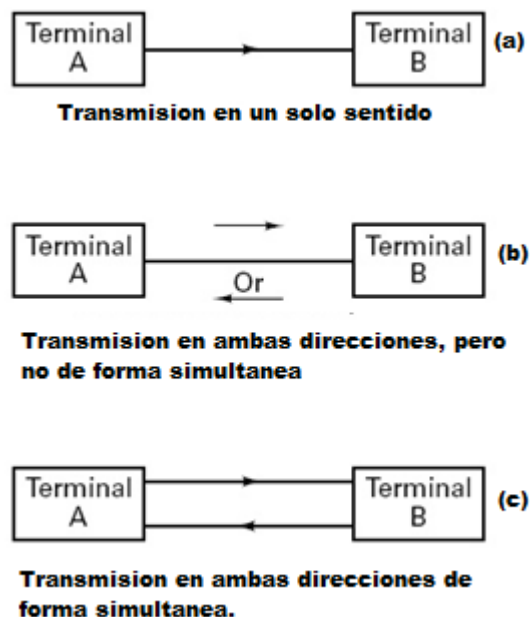


Figura. 1-8 Ejemplos de modos de transmisión entre nodos.

El sistema full –duplex tiene la ventaja de no presentar colisiones en el medio pues para que esta comunicación suceda son necesarios dos medios o líneas de transmisión

separadas. Esta parte de colisiones se valora al desarrollar la capa de enlace de datos en la Unidad III.

1.3.1.2 Topología multi - acceso

Una topología multi – acceso o bien de “bus”, es aquella que utiliza un solo medio o “bus común” para la transmisión de datos a varios nodos o hosts (Ver Figura. 1-9). Un host envía una trama a todos los ordenadores o dispositivos conectados, pero solo el terminal al que corresponden los datos hará uso de ellos (CISCO, 2008). El paquete de datos contiene una dirección física y lógica que identifica a que ordenador le corresponde.

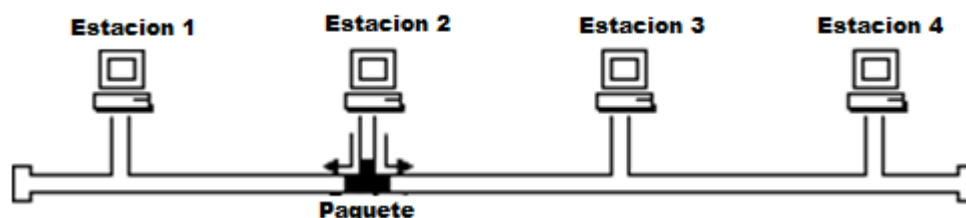


Figura. 1-9 Funcionamiento lógico de una topología tipo bus.

Surge aquí una pregunta, si todos los usuarios hacen uso del mismo medio para transmitir ¿qué pasaría si dos o más usuarios transmiten de manera simultánea?! Es por ello, se necesita de un mecanismo para evitar estas “colisiones” o para prevenirlas. Este tema se mencionara brevemente en este segmento, pues se desarrollara al estudiar las funciones que realiza la capa de enlace de datos en el modelo OSI.

1.3.1.2.1 Detección de colisiones

CSMA/CD⁶ es un sistema que permite la comunicación en topologías tipo bus, disminuyendo el número de colisiones en el medio. La siguiente figura muestra el proceso que se implementa. Cada host está equipado con una tarjeta de red, esta tarjeta tiene la opción de medir el nivel de voltaje en la línea o medio. Antes de que se envíe un dato, el host debe chequear si se está transmitiendo una trama. Si la línea está en uso por otro host, este deberá esperar su turno para transmitir (Ver Figura. 1-10).

⁶ CSMA/ CD = Carrier Sense Multiple Access/ Collision Deteccion – Acceso múltiple por detección de portadora/ Detección de Colisión

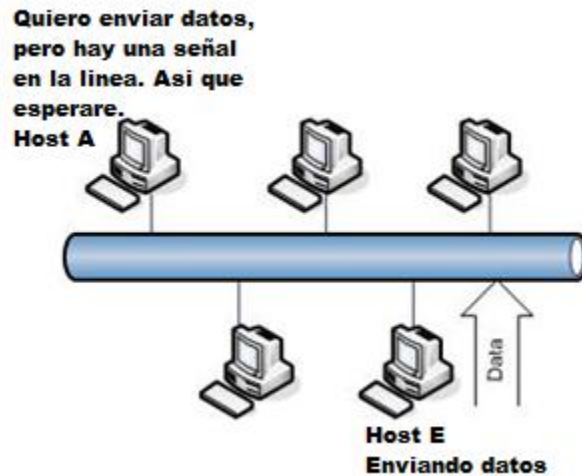


Figura. 1-10 Primer paso en el envío de tramas en una topología de acceso múltiple.

Sin embargo aun con este sistema es posible que se generen colisiones en la línea. Supongamos que la línea está libre y dos hosts realizan una detección por portadora de manera simultánea (Ver Figura. 1-11 (a)). En este punto ambos hosts proceden a enviar sus datos al mismo tiempo (Ver Figura. 1-11 (b)), lo que genera una colisión. La tarjeta una vez que ha transmitido los datos procede a detectar si el nivel de voltaje no se ha incrementado por encima de los normal (Ver Figura. 1-11(c)), pues un aumento significa que los voltajes de dos o más señales se han superpuesto (CISCO, 2008). A continuación la Figura. 1-11 demuestra de manera gráfica el procedimiento de detección de portadora cuando sucede una colisión.

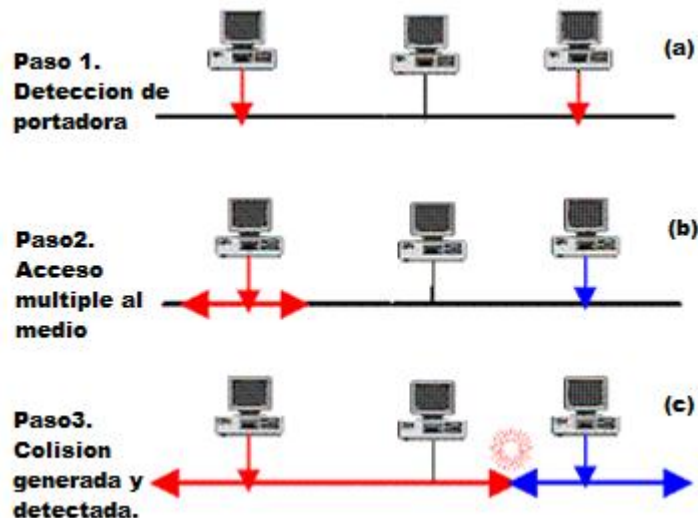


Figura. 1-11 Ejemplo de ocurrencia de colisión utilizando CSMA/CD

Si esto sucede los host involucrados deberán esperar un tiempo antes del próximo intento de transmitir sus tramas (Ver Figura. 1-12). Este tiempo se asigna de forma aleatoria. Las formas tradicionales de Ethernet implementan este método.

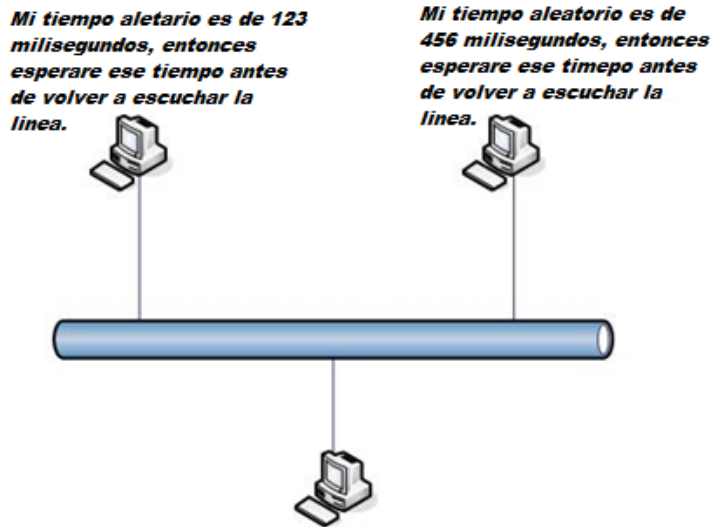


Figura. 1-12 El tiempo de espera luego de una colisión es diferente en cada PC.

1.3.1.2.2 Prevención de colisiones

En este caso sobresalen las siglas CSMA/CA⁷, el host al igual que en el caso anterior monitorea el medio o línea de transmisión en busca de la presencia de una señal, pero si no la encuentra notifica a los otros dispositivos conectados a la red de sus intenciones de enviar una trama. Luego se procede a enviar la trama de datos. La Figura. 1-13 muestra un ejemplo de este método de acceso al medio.

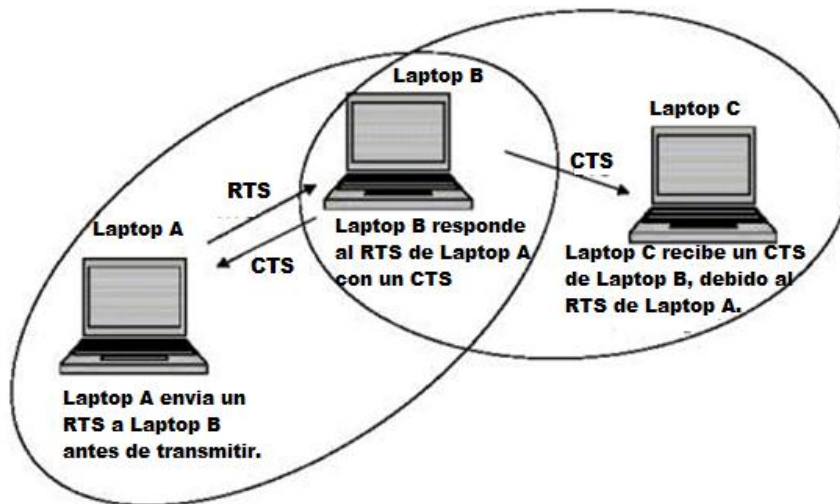


Figura. 1-13 La transmisión inalámbrica implementa CSMA/CA

⁷ CSMA/CA =Carrier Sense Multiple Access/ Collision Avoidance - Acceso múltiple por detección de portadora/ Anticolisión

El host A avisa al host B de sus intenciones de enviar datos, luego el host B envía una respuesta confirmando esta solicitud y envía un aviso al host C para que no envíe datos mientras se da la transferencia entre A y B.

RTS_{vi} son las siglas de Request to Send o “Pregunta para enviar” y CTS_{vii} “Clear to Send” que tiene la función de despejar la línea para la transferencia clara de los datos.

1.3.1.3 Topología de anillo

En esta topología el conjunto total de hosts o nodos se conectan virtualmente como un anillo o lazo (Ver Figura. 1-14), cada nodo recibe una trama por turno. Si la trama que llega a un nodo no está direccionada a este, el nodo transfiere la trama al siguiente nodo. El anillo permite implementar un mecanismo de control de acceso al medio conocido como “token passing”⁸.

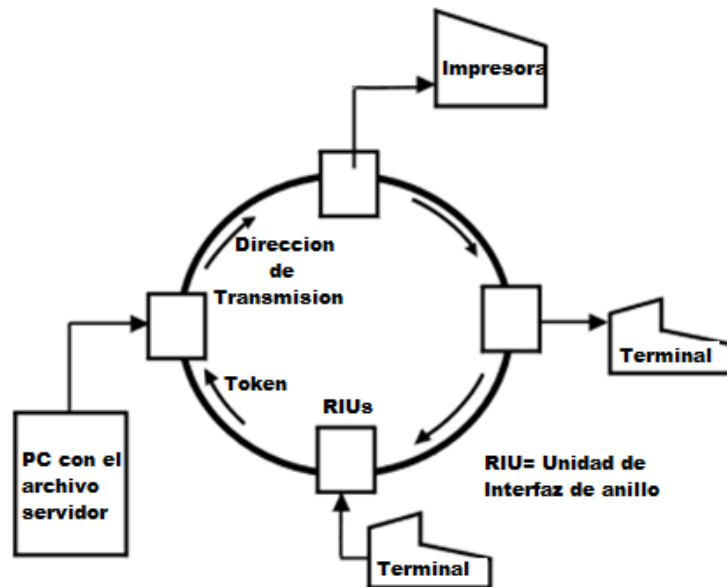


Figura. 1-14 Conexiones lógicas de terminales implementando una topología de anillo.

El token passing se basa en el envío de paquetes de información que contienen la dirección de destino y la información que se envía al nodo. Cuando la información que se entrega la información, el paquete es libre y puede ser usado por otra estación de trabajo. (GS Comunicaciones, 1999)

Los nodos son los encargados de eliminar o sacar del medio una trama, pues si el nodo reconoce al destinatario de la trama como si mismo este ya no procede a transferirle al

⁸ Token passing = Paso de tokens

siguiente host. Cada host es encargado de regenerar la señal o trama con la desventaja que si un nodo falla todo el sistema se ve afectado.

La información pasa dentro de un anillo en un solo sentido, por lo cual el riesgo de colisiones es nulo.

1.3.1.4 Topología de malla

Esta topología presenta una gran cantidad de redundancias, pues se crean enlaces punto a punto y dedicados entre cada dispositivo de la red (Ver Figura. 1-15). Por lo cual, es capaz de seguir operando con sus otros terminales en caso de una falla. Sin embargo, estas redundancias incrementan el monto de inversión para instalar la red.

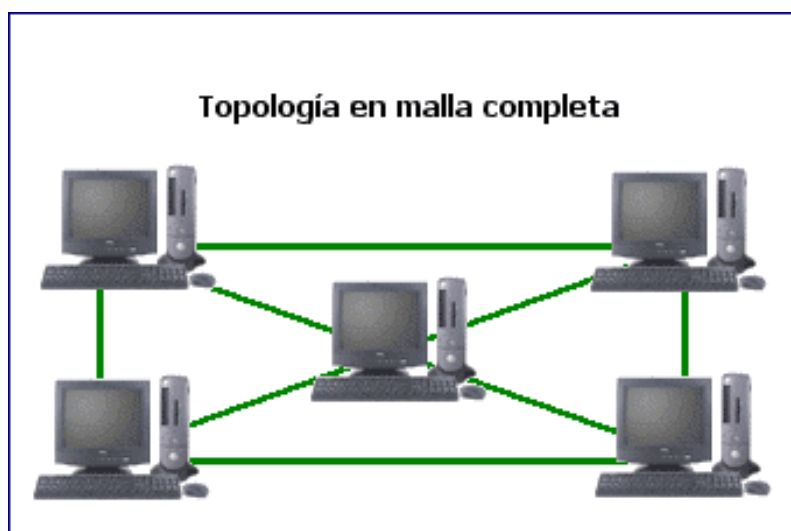


Figura. 1-15 Ejemplo de topología en malla.

Como parte del análisis si se tuvieran “n” dispositivos el número de líneas o medios físicos de interconexión total, estará dado por la ecuación $n(n-1)/2$.

El sistema tiene las ventajas de disminuir el tráfico que se transporta a través de cada línea, puesto que cada conexión solamente transporta los datos de comunicación entre dos puntos. Esto disminuye el número de colisiones que se pueden generar en relación a cierto periodo de tiempo.

Finalmente, esta topología brinda una mayor seguridad o privacidad a cada usuario. Esto se genera al restringir el número de usuarios que pueden ver los datos que son transportados por una línea. Es decir, solamente el receptor de dicho paquete de datos está en la capacidad de examinar el paquete de datos incluso para la revisión de dirección de destino.

1.3.1.5 Topología de árbol jerárquico

Es formada por segmentos de una red o subredes que estarán en dependencia de los tipos de elementos que ocupen en la construcción de la misma (Kevin Vergara, 2007). Como su nombre lo menciona, esta topología posee la estructura de un árbol invertido, donde la raíz del árbol representa el punto central de conexión a internet.

La Figura. 1-16 es un ejemplo de una red que implementa una topología lógica de árbol jerárquico.



Figura. 1-16 Conexión entre ordenadores de forma jerárquica.

En este caso, se tiene una red global y dos subredes. Este sistema es el más utilizado para el diseño de redes a nivel de empresas, pues permite mantener un orden en caso de aumentar el número de ordenadores en la red.

Cuando se estudie el proceso de diseño de redes IP, se utilizara este tipo de topología.

1.3.2 Topologías físicas

Las topologías físicas no siempre tienen la misma forma que una topología lógica, es por esto que a continuación procedemos a mostrar las implementaciones físicas de las topologías más comunes. En algunos casos 2 topologías lógicas pueden llegar a tener la misma estructura física.

La diferencia entre las topologías físicas y lógicas es que las primeras se basan en las características en su hardware y las segundas se basan en las características internas que se desean tengan en su software de red.

1.3.2.1 Topología de estrella

En esta topología existe un enlace punto a punto entre cada host y un concentrador central, que comúnmente se llama hub. A diferencia de la red malla, los hosts no están conectados entre sí y por ende no permite el tráfico directo entre dispositivos (Ver Figura. 1-17).

El hub actúa como un intercambiador, este concentrador recibe los datos de un host y los envía a todos los otros dispositivos conectados a este. Sin embargo, esto aumenta el tráfico y disminuye la eficiencia del sistema pues solo puede realizar una función a la vez (receptor o transmisor). (CISCO, 2008)

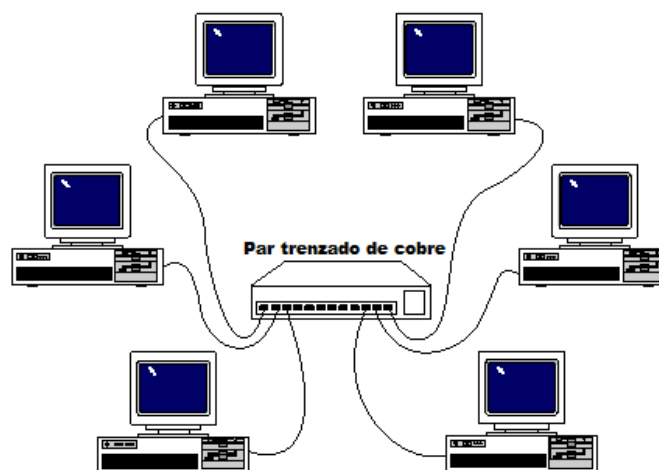


Figura. 1-17 Conexión física de una red usando topología de estrella.

Para mejorar la red los diseñadores han reemplazado el concentrador central por un switch (Ver Figura. 1-18). Este switch permite el intercambio de datos de una forma más eficiente, cada línea puede estar enviando datos y el switch se encargará que los datos se transmitan únicamente por la línea a la que está conectado el destino.



Figura. 1-18 Implementación de una red de estrella con un switch.

1.3.2.2 Topología de árbol jerárquico

En la práctica una topología de árbol jerárquico posee segmentos y cada segmento es en realidad una configuración en estrella (Ver Figura. 1-19). (Ureña Poirier & Rodriguez, 2005)

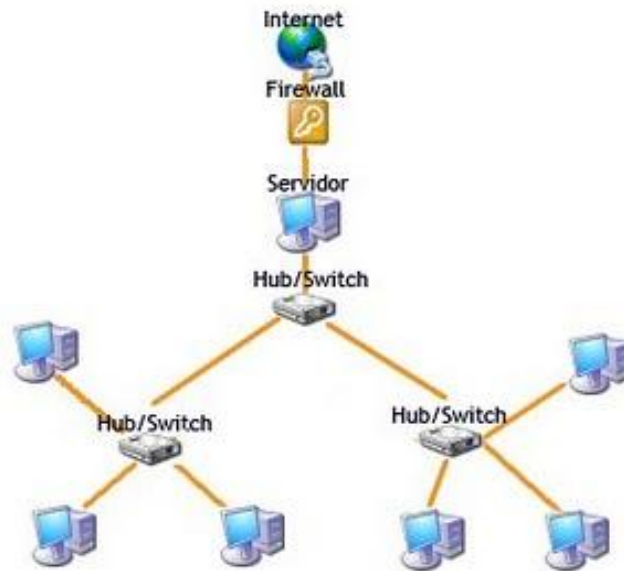


Figura. 1-19 Topología física de una red en configuración de árbol jerárquico.

Por lo tanto las características presentadas en la sección anterior son similares para cada una de los segmentos del árbol. A este tipo de topología se le denomina como “estrella extendida”.

1.4 Redes inalámbricas

Una **red inalámbrica** es, como su nombre lo indica, una red en la que dos o más terminales (por ejemplo, ordenadores portátiles, agendas electrónicas, etc.) se pueden comunicar sin la necesidad de una conexión por cable.

Con las redes inalámbricas, un usuario puede mantenerse conectado cuando se desplaza dentro de una determinada área geográfica. Por esta razón, a veces se utiliza el término "movilidad" cuando se trata este tema.

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar. Hay muchas tecnologías diferentes que se diferencian por la frecuencia de transmisión que utilizan, y el alcance y la velocidad de sus transmisiones.

Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya se encuentren a unos metros de distancia como a varios kilómetros. Asimismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente como pasa con las redes cableadas. Tampoco hay necesidad de agujerear las paredes para pasar cables ni de instalar portacables o conectores. Esto ha hecho que el uso de esta tecnología se extienda con rapidez.

Por el otro lado, existen algunas cuestiones relacionadas con la regulación legal del espectro electromagnético. Las ondas electromagnéticas se transmiten a través de muchos dispositivos (de uso militar, científico y de aficionados), pero son propensos a las interferencias. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y la potencia de transmisión que se permite a cada categoría de uso.

Además, las ondas hertzianas no se confinan fácilmente a una superficie geográfica restringida. Por este motivo, un hacker puede, con facilidad, escuchar una red si los datos que se transmiten no están codificados. Por lo tanto, se deben tomar medidas para garantizar la privacidad de los datos que se transmiten a través de redes inalámbricas.

1.4.1 Categorías de redes inalámbricas

Por lo general, las redes inalámbricas se clasifican en varias categorías, de acuerdo al área geográfica desde la que el usuario se conecta a la red (denominada *área de cobertura*). La Figura. 1-20 muestra la clasificación de la redes inalámbricas según el área de cobertura que estas tienen:

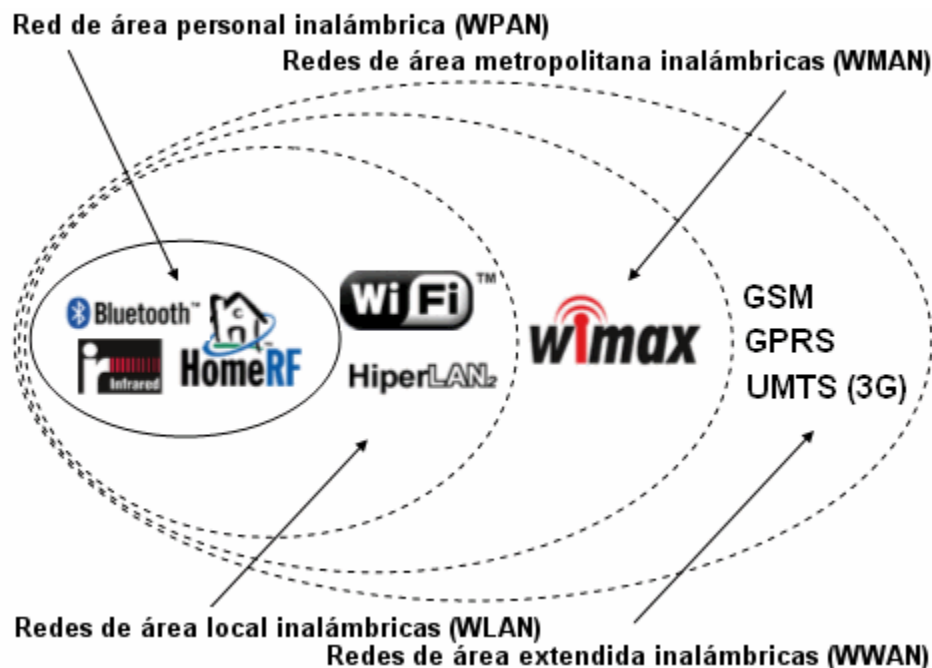


Figura. 1-20 Redes inalámbricas según área de cobertura.

1.4.2 Seguridad en redes Inalámbricas.

El avance tecnológico en medios de comunicación inalámbrica ha proporcionado nuevas expectativas de futuros para facilitar flexibilidad y movilidad al momento de comunicarnos. En el año 2002 demostró ser la mejor manera de realizar conectividad de datos en edificios sin necesidad de cablearlos.

Sin embargo, como toda tecnología presenta riesgos, que debido al optimismo inicial y en la adopción no se observaron los riesgos que podrían surgir con la utilización de un medio de transmisión tan “compartido” como son las ondas de radio.

Existen 4 tipos de redes inalámbricas, las basadas en tecnología BlueThooth, la IrDa⁹ viii, la HomRF y la WECA¹⁰. La primera de ellas no permite la transmisión de grandes cantidades de datos entre ordenadores de forma continua y la segunda tecnología, estándar utilizado por los dispositivos de ondas infrarrojas Home RF y Wi-Fi están basadas en las especificaciones 802.11 de Ethernet Inalámbrica y son las que utilizan actualmente tarjetas inalámbricas. (Universidad de Valencia, 2009)

La topología de redes inalámbricas consta de dos elementos clave, las instalaciones cliente y los puntos de acceso. La comunicación puede realizarse directamente entre estaciones cliente a través de los puntos de acceso. El intercambio de datos solo es posible cuando existe una autenticación entre las estaciones clientes y el punto de acceso y se produce la asociación entre ellos. Al comienzo se lleva a cabo un intercambio de mensajes de autenticación que periódicamente se repite a fin de comprobar el estado actual de un usuario en la red.

EL uso del aire como medio de transmisión de datos mediante la propagación de radio ha proporcionado nuevos riesgos de seguridad. La salida de estas ondas de radio fuera del edificio donde está ubicada la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible a la empresa y a la seguridad informática de la misma.

La posibilidad de comunicarnos entre estaciones clientes directamente, sin pasar por el punto de acceso permitiría atacar directamente a una estación cliente, generando problemas si esta estación cliente ofrece servicios TCP/IP o comparte ficheros. Existe también la posibilidad de duplicar las direcciones IP o MAC de estaciones cliente legítimas.

1.4.2.1 WEP

El protocolo Web es un sistema de encriptación estándar propuesto por el comité 802.11, implementada en la capa MAC y soportada por la mayoría de los vendedores de

⁹ IrDa = Infrared Data Association – Asociación de datos Infrarrojos.

¹⁰ WECA es la asociación de Wi-Fi.

soluciones inalámbricas. WEP comprime y cifra los datos que se envían a través de las ondas de radio.

Con WEP, la tarjeta de red encripta el cuerpo y el CRC de cada trama 802.11 antes de la transmisión utilizando el algoritmo de encriptación RC4 proporcionado por RSA Security. La Estación receptora, sea un punto de acceso o una estación cliente es la encargada de desencriptar la trama. (Universidad de Valencia, 2009)

Como parte del proceso de encriptación, WEP prepara una estructura denominada “seed” obtenida tras la concatenación de la llave secreta proporcionada por el usuario de la estación emisora con un vector de inicialización (IV) de 24 bits generada aleatoriamente. La estación cambia el IV para cada trama transmitida.

A continuación, WEP utiliza “seed” en un generador de números pseudoaleatorios que produce una llave de longitud igual al payload de la trama más un valor para chequear la integridad (ICV) de 32 bits de longitud. (Universidad de Valencia, 2009)

El ICV es una checksum que utiliza la estación receptora para recalcularlo y compararlo con el enviado por la estación emisora para determinar si los datos han sido manipulados durante su envío. Si la estación receptora recalcula un ICV que no concuerda con el recibido en la trama, esta queda descartada e incluso puede rechazar al emisor de la misma.

WEP especifica una llave secreta compartida de 40 o 64 bits para encriptar y desencriptar, utilizando encriptación simétrica

Antes de que tome lugar la transmisión, WEP combina la llave con el payload/ICV a través de un proceso XOR a nivel de bit que producirá el texto cifrado. Incluyendo el IV sin encriptar sin los primeros bytes del cuerpo de la trama. (Tanenbaum, 2003)

La estación receptora utiliza el IV proporcionado junto con la llave del usuario de la estación receptora para desencriptar la parte del payload del cuerpo de la trama.

Cuando se transmiten mensajes con el mismo encabezado, el principio de cada payload encriptado será el mismo si se utiliza la misma llave. Tras encriptar los datos, el principio de estas tramas será el mismo, proporcionando un patrón que puede ayudar a los intrusos a romper el algoritmo de encriptación. Esto se soluciona utilizando un IV diferente para cada trama.

La vulnerabilidad de WEP reside en la insuficiente longitud del Vector de Inicialización (IV) y lo estáticas que permanecen las llaves de cifrado, pudiendo no cambiar en mucho tiempo. Si utilizamos solamente 24 bits, WEP utilizara el mismo IV para paquete diferentes, pudiéndose repetir a partir de un cierto tiempo de transmisión continua. Es a partir de entonces cuando un intruso puede, una vez recogiendo suficientes tramas, determinar incluso la llave compartida.

En cambio 802.11 no proporciona ninguna función que soporte el intercambio de llaves entre estaciones. Como resultado, los administradores de sistema y los usuarios utilizan las

mismas llaves durante días o incluso meses. Algunos vendedores han desarrollado soluciones de llaves dinámicas distribuidas.

A pesar de todo, WEP proporciona un mínimo de seguridad para pequeños negocios o instituciones educativas, sin o esta deshabilitada, como se encuentra por defecto en los distintos componentes inalámbricos.

1.4.2.2 WPA

WPA es la abreviatura de Wifi Protect Access que significa Acceso de protección Wi-Fi, y consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP. También se le conoce con el nombre de TSN¹¹.

WPA utiliza TKIP¹² para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización. En general WPA es TKIP con 8021X. Por lo demás WPA funciona de una manera parecida a WEP pero utilizando claves dinámicas, utiliza el algoritmo RC4 para generar un flujo de bits que se utilizan para cifrar con XOR y su vector de inicialización (IV) es de 48 bits. La modificación dinámica de claves puede hacer imposible utilizar el mismo sistema que con WEP para abrir una red inalámbrica con seguridad WPA. (dns.bdat.net)

Además WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema o simplemente utilizar una contraseña compartida para identificarse.

Es el sistema más simple de control de acceso tras WEP, a efectos prácticos tiene la misma dificultad de configuración que WEP, una clave común compartida, sin embargo, la gestión dinámica de claves aumenta notoriamente su nivel de seguridad. PSK se corresponde con las iniciales de PreShared Key y viene a significar clave compartida previamente, es decir, a efectos del cliente basa su seguridad en una contraseña compartida.

WPA-PSK usa una clave de acceso de una longitud entre 8 y 63 caracteres, que es la clave compartida. Al igual que ocurría con WEP, esta clave hay que introducirla en cada una de las estaciones y puntos de acceso de la red inalámbrica. Cualquier estación que se identifique con esta contraseña, tiene acceso a la red. (Tanenbaum, 2003)

Las características de WPA-PSK lo definen como el sistema, actualmente, más adecuado para redes de pequeñas oficinas o domésticas, la configuración es muy simple, la seguridad es aceptable y no necesita ningún componente adicional. (dns.bdat.net)

¹¹ TSN = Transition Security Network – Red de transición de seguridad

¹² TKIP = Temporal Key Integrity Protocol – Protocolo de Integridad de Llave Temporal

La principal debilidad de WPA-PSK es la clave compartida entre estaciones. Cuando un sistema basa su seguridad en un contraseña siempre es susceptible de sufrir un ataque de fuerza bruta, es decir ir comprobando contraseñas, aunque dada la longitud de la contraseña y si está bien elegida no debería plantear mayores problemas.

Debemos pensar que hay un momento de debilidad cuando la estación establece el diálogo de autenticación. Este diálogo va cifrado con las claves compartidas, cuando las claves se comprueban entonces se garantiza el acceso y se inicia el uso de claves dinámicas. La debilidad consiste en que conocemos el contenido del paquete de autenticación y conocemos su valor cifrado. Ahora lo que queda es, mediante un proceso de ataque de diccionario o de fuerza bruta, intentar determinar la contraseña.

1.5 La red como plataforma multiservicios

El uso de Internet como plataforma de comunicación, trae consigo una gran cantidad de ventajas y facilidades para brindar servicios a la población. El internet permite crear nuevas formas de comunicación, tales como:

Mensajería instantánea: Este tipo de comunicación se le conoce como de tiempo real, puede realizarse entre dos o más personas en forma de texto. El texto se envía a través de internet de una computadora a otra. En este caso se ven involucrados dirección de internet pública y privadas. Este sistema incorpora los servicios de transferencia de archivos, comunicación por voz y video. (CISCO, 2008)

Este tipo de comunicación es muy parecida al envío de e-mail, sin embargo a diferencia del e-mail que puede retrasar su llegada, en el msn (Ver Figura. 1-21) es necesario que el texto llegue de manera “instantánea” al otro extremo. Es por esto que se requiere de otros protocolos como RTP y RTCP, que constituyen dos grandes protocolos de tiempo real. Este tipo de protocolo se abordará con mayor detalle en unidades posteriores.



Figura. 1-21 Mensajería Instantánea

Otro tipo de comunicación son los **weblogs** y **wikis**. Los **weblog** (Ver Figura. 1-22) con páginas Web con gran facilidad para ser actualizadas y editadas por los creadores de esta (CISCO, 2008). Los usuarios autorizados pueden ver este tipo de páginas web y solo algunos de editarlas, es necesario tener cierto conocimiento en el área de programación para editar este tipo de páginas web.



Figura. 1-22 Ejemplo Weblog para obtener un trabajo

En el caso de los **Wikis**, son más conocidos por los usuario ya que uno de los sitios más conocidos es Wikipedia (Ver Figura. 1-23), siendo esta una enciclopedia en línea donde se comparte información sobre distintos temas de carácter científico. Los wikis como este, tiene la característica de ser modificados no solo por los encargados en administrar la página Web, cualquier usuario puede editar la información.



Figura. 1-23 Ejemplo de un Wiki

Esto genera cierto grado de inseguridad en la información que se lee, pues si bien la información puede ser tan correcta como incorrecta, es por eso que el administrador de la página debe realizar revisiones periódicas.

Otro método a mencionar es el **Podcasting**, teniendo este la finalidad inicial de funcionar como un MP3 player, pero que luego por desarrollo del internet se le ha dado la facilidad de compartir sus archivos de media, subiéndolos a un servidor o bien, a una

página web¹³. Permitiendo que los archivos de media sean compartidos (Ver Figura. 1-24 entre personas con cuentas de usuarios en ese servidor. (CISCO, 2008)

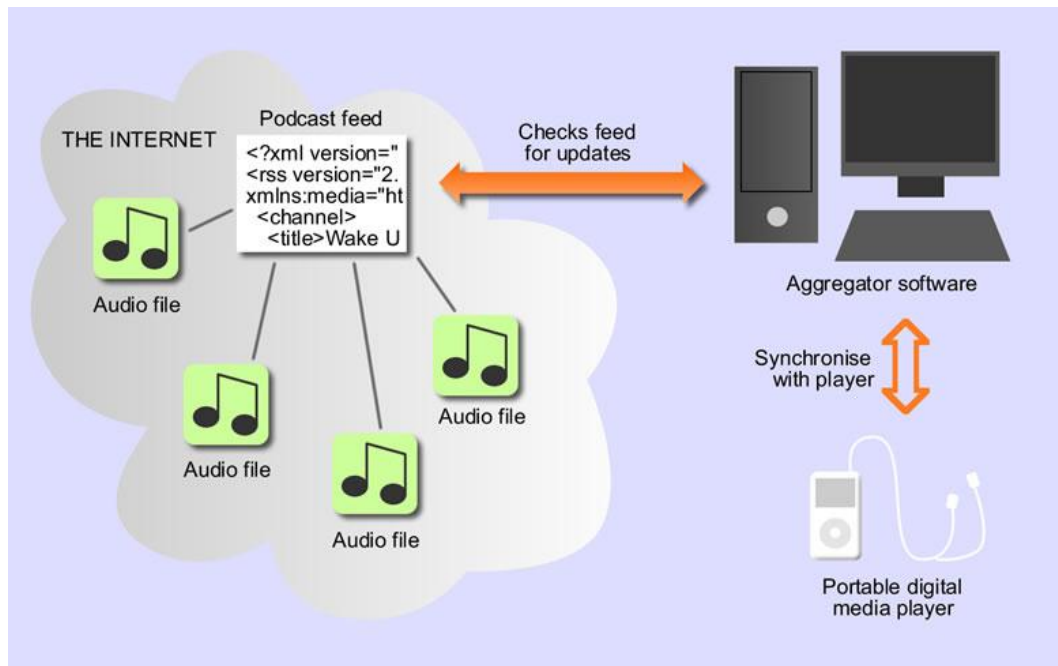


Figura. 1-24 Usuarios remotos acceden al servidor vía internet.

Los servicios antes mencionados ya están en uso y la tendencia a futuro es ocupar el internet como plataforma para más servicios, como lo es el sistema de telefonía convencional. La finalidad de este módulo es prepararle a estudiante para ser capaz de asociar algunos de los términos de redes de datos que se implementan en redes telefónicas y comprender su funcionamiento.

1.6 Tecnologías de procesamiento en la red.

Un aspecto importante de todas las redes es la forma en que estas procesan los datos. Este procesamiento está en función de las exigencias que tiene la empresa o el tipo de red que se desea desplegar. Se pueden diferenciar principalmente dos tipos de procesamiento:

Procesamiento Centralizado

Este tipo incluye el uso de mainframes y minicomputadoras. Los usuarios se conectan a la red mediante el uso de computadoras “tontas” que no tienen la capacidad de procesar datos y que requieren de un servidor central (Ver Figura. 1-25), el cual contiene todos los softwares de las máquinas. Este mainframe procesa los datos de todos los usuarios. (GS Comunicaciones, 1999)

¹³ Se hace referencia a página Web como servidor, pues la página Web debe estar almacenada en un ordenador - servidor.

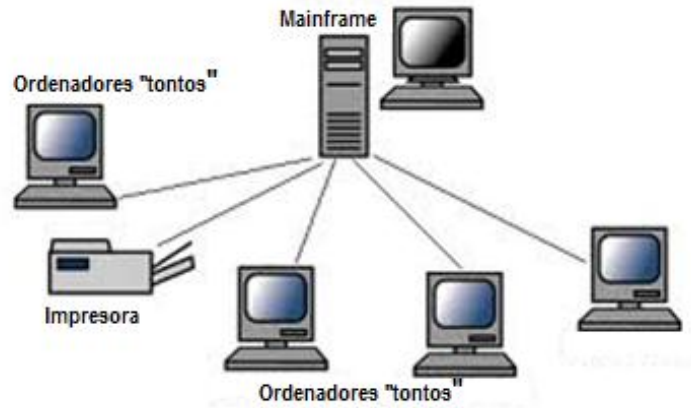


Figura. 1-25 Configuración de ordenadores para procesamiento centralizado en una red LAN

Uno de los principales problemas en las redes que implementan este tipo de procesamiento es la degradación del servicio de manera proporcional al número de terminales que se conectan al mainframe.

Procesamiento distribuido

Este sistema consta de estaciones de trabajo capaces de procesar datos a nivel local, es decir cada computador procesa los datos del usuario. Cada ordenador ejecuta una pequeña parte de una aplicación de la red general (Ver Figura. 1-26). Uno de estos ejemplos es el sistema cliente-servidor.

El objetivo principal de estos sistemas distribuidos es resolver problemas de gran tamaño como para ser resueltos por un solo mainframe, y a su vez trabajar en múltiples problemas pequeños. Al tener este un entorno multiusuario (varios ordenadores) son necesarias medidas de seguridad como técnicas de autorización.

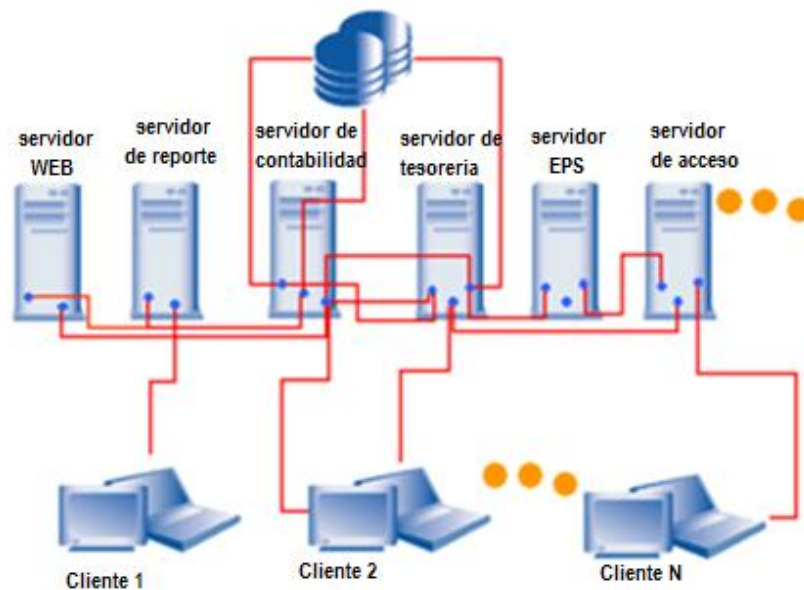


Figura. 1-26 Configuración de ordenadores para ejecutar un procesamiento distribuido

Los sistemas distribuidos utilizan los protocolos TCP/IP, en cuanto a los protocolos para aplicaciones de red se tiene: Telnet y FTP¹⁴_{ix}. Entre los sistemas operativos distribuidos podemos mencionar Amoeba y Beowolf. Es necesario mencionar la existencia e importancia de la herramienta **Globus** que es considerado un estándar de facto para la capa intermedia de la red.

Globus tiene los recursos necesarios para realizar (Wikipedia, 2009):

1. La gestión de recursos (Protocolo de Gestión de Recursos en malla o bien Grid Resource Management Protocol)
2. Servicios de Información (Servicio de Descubrimiento y Monitorización O minitoring and Discovery Service).
3. Gestión y Movimiento de Datos (Acceso Global al Almacenamiento Secundario, Global Access to secondary Storage y FTP en malla, GridFTP)

1.7 Breve reseña sobre elementos de una red de datos

Al igual que cualquier sistema de computadora una red de datos contiene elementos fundamentales para su funcionamiento. En esta sección nos enfocaremos en mencionar los elementos que pueden integrar la red y algunas características de estos, pues en las siguientes unidades se retoman cada uno de estos elementos con un mayor detalle en aspectos técnicos.

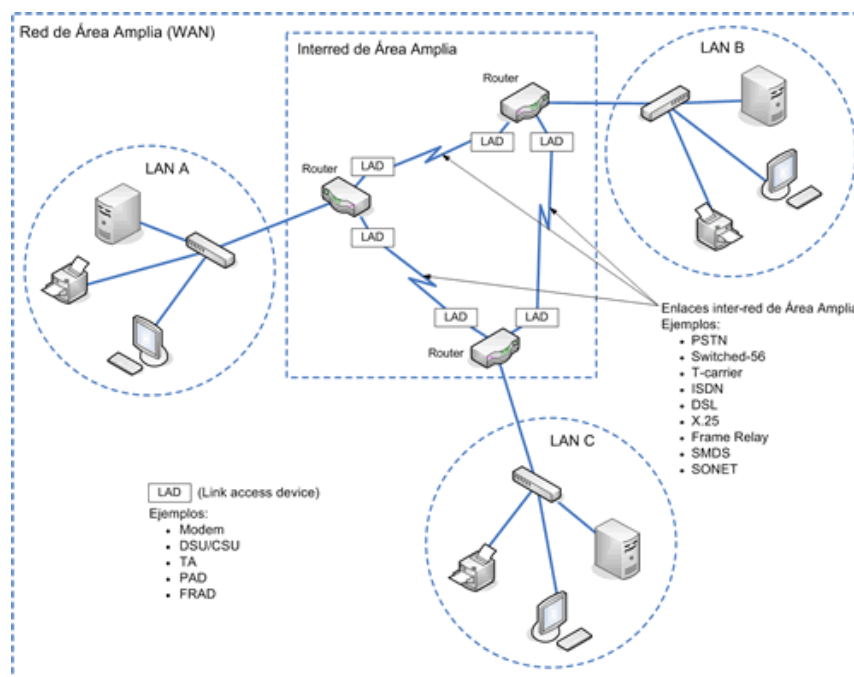


Figura. 1-27 Estructura general de interconexión de redes.

¹⁴ FTP = File Transfer Protocol – Protocolo de transferencia de archivo.

En la Figura. 1-27 se muestra un diagrama general de la estructura de Internet. Se pueden apreciar los siguientes elementos:

- Hosts (PC, PDA y teléfono móvil)
- Modem (modulador – demodulador)
- Enrutador (Router)
- Proxy (servidor de réplica)
- Conexiones LAN
- Conexiones WAN

Un **host** o anfitrión es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Un host debe tener una dirección de Internet (dirección IP) única y un nombre de dominio único o nombre de host. (Masadelante, 1999)

Un **modem** es un dispositivo de hardware que se conecta con al ordenador, una línea telefónica o una línea coaxial de televisión (cable modem). Haciendo una analogía para comprender de una mejor manera, se podría decir que un modem es para los ordenadores lo que para nosotros es un teléfono. (Masadelante, 1999)

Existen diferentes tipos de modem de acuerdo al medio seleccionado de transmisión:

1. De línea conmutada
2. De radio
3. Vía microondas
4. Satelitales
5. De fibra óptica
6. Laser

Los **enrutadores** o mejor conocidos por su nombre en inglés “Routers”, se emplean para traducir información de una red a otra. La información se intercambia mediante direcciones lógicas. (GS Comunicaciones, 1999)

El router conecta distintas redes, por lo cual se basa en funcionamiento de capa 3 o capa de red del modelo OSI. Entre las características físicas que estos tienen, son sus puertos LAN y por lo menos un puerto WAN para conectarse a Internet.

En algunos casos es necesario un **repetidor**, de todos los dispositivos de red este es el más rápido. Se usa para extender las longitudes físicas de las redes, pero no contiene inteligencia para funciones de enrutamiento. Un repetidor se utiliza cuando dos segmentos están acercando sus longitudes físicas máximas es decir alcanzan las distintas máximas entre ellos. Estas distintas se fijan por el medio de transmisión que se utiliza, pues en relación dependerá el grado de atenuación de la señal.

Otro de los elementos fundamentales es un **Servidor**, que no es más que un sistema de cómputo central que ejecuta un software especializado para proveer acceso compartido a los usuarios de la red. Esta unidad debe estar capacitada para procesar todas las peticiones

que generen las estaciones de trabajo. Como ejemplo de esto podemos usar el caso de Hotmail, el servidor central debe tener las características de hardware suficientes (procesador, memoria RAM, etc.) como para que los usuarios en hora pico puedan acceder a este sin ningún problema.

El termino *proxy* comúnmente se utiliza para hacer referencia a un servidor, la definición de proxy nos indica que este es un programa o dispositivo que realiza una tarea que involucre la conexión a internet. Es decir, es un punto intermedio entre un host conectado a internet y el servidor al que está accediendo. Las solicitudes que se envían al servidor son realmente peticiones que se realizan al proxy, siendo este el que controla el flujo de datos. (Alvarez, 1998)

Ejemplos claros de un proxy, puede ser un firewall que evita la recepción o envío de paquetes de datos que contengan cierto número de puerto¹⁵.

1.8 Aspectos importantes de una red de datos

1.8.1 Tolerancia a fallas

Una red de datos sirve como una plataforma para la comunicación entre miembros, dado el caso de una LAN de alguna empresa, se puede decir que la red interna de datos se puede utilizar para el intercambio de archivos, actualización de bases de datos, acceso de servidores privados, etc. Es debido a esta variedad de servicios brindados que las empresas logran mejorar su desempeño y agilidad al laborar.

Acorde a lo mencionado anteriormente, esta plataforma multi-servicios debe ser confiable o en otras palabras poseer una gran tolerancia a fallas. Imaginemos las pérdidas que se podrían dar en una empresa que depende de una red para vender productos en línea alrededor del mundo.

Por ello como medidas para el mantenimiento del acceso a los servidores de manera constante, se ha comenzado a implementar el uso de 2 routers (Ver Figura. 1-28) como punto de acceso al servidor de una empresa.

¹⁵ El número de puerto es el número que identifica una aplicación, de tal forma que la computadora al recibirle sabe a qué aplicación corresponde el paquete de datos.

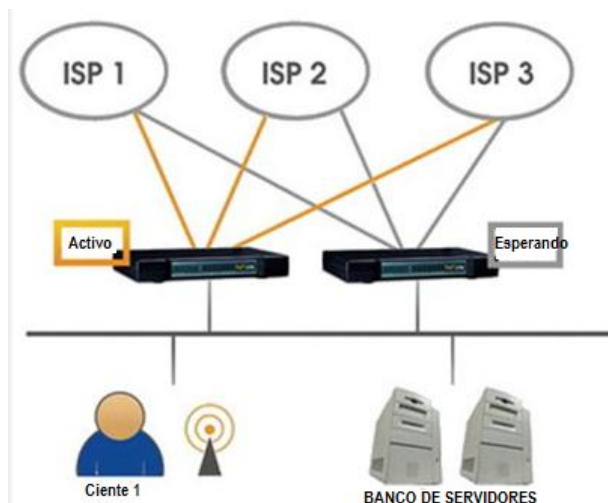


Figura. 1-28 El cliente 1 utiliza redundancias para acceder a los ISPs.

Algunas empresas para brindar una mayor fiabilidad en sus servicios deciden conectarse a más de un ISP¹⁶. Si bien sabemos que este incremento en el número de ISPs, aumentara los gastos mensuales que tiene la empresa.

Es por ello que es necesario hacer un balance¹⁷ entre el grado de tolerancia a fallas que se obtiene y el costo en la inversión por mejorar esta medida.

1.8.1.1 *Sistemas conmutados por circuitos vs Sistemas conmutados por paquetes.*

1.8.1.1.1 Sistemas conmutados por circuitos

Este tipo de sistema es característico de las redes telefónicas antiguas donde al realizar una llamada era necesario la conexión o establecimiento de una línea física y única entre el receptor y transmisor de voz. Dicha línea no podía ser interrumpida o compartida de manera simultánea por que de serlo la conversación iniciada se vería interrumpida o afectada por otra conversación.

En los casos en que múltiples llamadas se realizaran y estas igualaran al número de circuitos máximos posibles de conectarse, la central estaría saturada y las llamadas entrantes serian rebotadas. Esto en la experiencia del usuario resulta como una caída de la red si este intenta realizar una llamada.

En la actualidad, se realiza una multiplexación de canales en lugar de circuitos se utilizan canales lógicos sobre el mismo medio. Sin embargo, dicho canal permanece ocupado y existe un número máximo de canales por medio de transmisión. Por lo cual, la central telefónica podría saturarse si recibe en cantidad de llamadas, la cantidad de canales disponibles para la transmisión.

¹⁶ ISP = Internet Service Provider – Proveedor de servicios de Internet

¹⁷ A este balance entre partes se le menciona como trade-off.

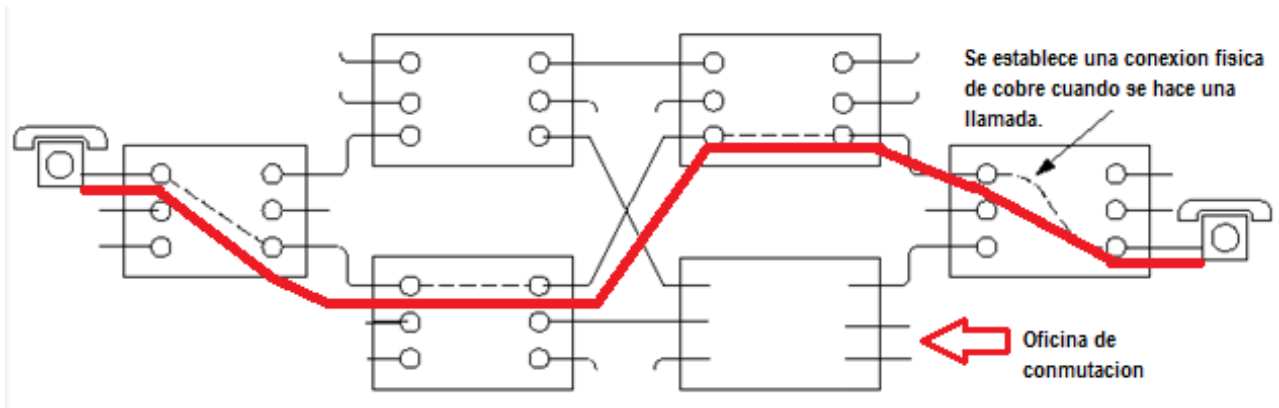


Figura. 1-29 Sistema telefónico conmutado por circuito.

En la Figura. 1-29 se observa que la oficina de conmutación tiene un enlace único para el teléfono en el extremo derecho y los puntos de conexión para este teléfono en la central no pueden variar, por lo que cualquier daño en estas terminales o central dejaría incomunicado al usuario.

1.8.1.1.2 Sistemas conmutados por paquetes

Cuando nos referimos a paquetes debemos imaginar un “regalo” que contiene parte de nuestro mensaje completo. El mensaje que se quiere enviar se divide en cada uno de estos paquetes en porciones iguales. Esto quiere decir que se puede enviar un paquete de manera individual a otro, no es necesario sostener una comunicación entre dos puntos de forma constante e ininterrumpida en el tiempo si se aplica este método.

Esto genera una gran ventaja en comparación con el sistema presentado anteriormente, pues otro usuario puede ocupar este canal o parte del circuito mientras la conversación entre dos terminales se esté realizando.

Para saber que paquete se dirige a qué punto se le deben atribuir dirección a cada uno, de esta manera los puntos en común no son así que “directores” o multiplexores de paquetes. No existen rutas fijas, lo que da una mejora en cuanto a la tolerancia de fallas, si un punto de cruce está dañado, el paquete puede tomar otra ruta pero igual llegará a su destino.

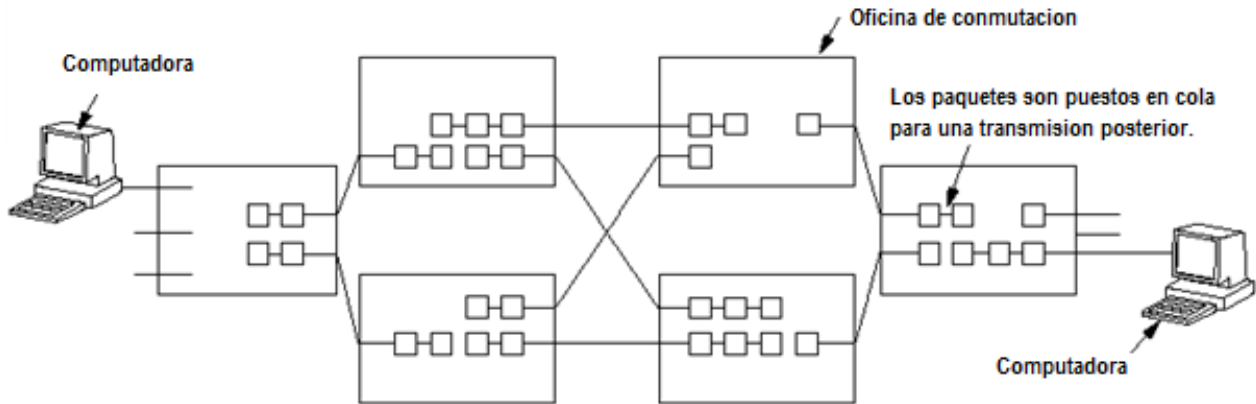


Figura. 1-30 Paquetes enviados a través de una ruta dinámica.

La Figura. 1-30 muestra que las central de conmutación poseen ahora no un punto de conexión sino varias redundancias para conexión, permitiendo así múltiples vías para transmitir el paquete hasta su destino.

Se debe mantener presente que el medio solo puede ser ocupado por un transmisor a la vez. Esta regla es indispensable en cualquier sistema, los paquetes de envió pueden mantenerse en cola mientras se reciben paquetes de otra terminal.

Ante cualquier daño posible en el camino existe una ruta alterna que permita habilitar al usuario a recibir la llamada o en este caso específico los datos en su computadora.

1.8.1.2 Jitter

El jitter en la variación en la transmisión digital de pulsos. Puede manifestarse a través de variaciones de amplitud, intensidad de la señal y otras formas como retrasos en la entrega. La generación de jitters usualmente se debe a tiempos de espera de conexión, congestión del tráfico de datos en la red y la interferencia de líneas.

En redes de datos el uso de paquetes facilita el envío y manipulación de información. Sin embargo cuando un jitter ocurre algunos paquetes de datos pueden perderse en el proceso de envío desde un extremo al otro. Esto puede generar un mal funcionamiento en el ordenador que recibe, la pérdida de un archivo que se descargaba si este paquete perdido formaba parte de la secuencia, interrupción de una llamada telefónica vía internet u otra operación. (TECH - FAQ, 2011)

El origen del jitter radica en la precisión en la entrega o recepción de un paquete que debe ser ensamblado en un orden específico en el receptor. La ocurrencia de un jitter significa que abra conflictos en el proceso de sincronización de recepción de paquetes. Los jitters pueden ocurrir al cruzar las distintas redes que pueden existir entre 2 computadoras o incluso al momento de recibirse el paquete.

El envío de información digital es obstaculizado por una variedad de fallas electrónicas y mecánicas las cuales pueden afectar la señal transmitida. En las comunicaciones a través de internet, por ejemplo, las tramas de datos enviados pueden ser adversamente afectadas por fuentes de poder, anchos de banda congestionados, pulsos electromagnéticos generados eventualmente en la naturaleza y otro tipos de eventos.

A fin de minimizar los impactos adversos de un los jitters en las descargas de archivos multimedias, se utilizan buffers (TECH - FAQ, 2011). Estos buffers permiten almacenar temporalmente, dando al sistema la oportunidad de reensamblar u ordenar los datos de tipo audio y video o cualquier otro archivo que requiera unirse en un orden específico para su reproducción o ejecución.

La corrección del jitter es usualmente se lleva a cargo por la tecnología, por lo general basada en el software o con mejoras en el hardware. Correcciones de software son por lo general el fin de modificar los contenidos digitales o revisión de la integridad de cada paquete.

1.8.1.3 Latencia

En el área de redes de datos se le denomina latencia a la suma de retardos temporales que pueden ocurrir en una red. El retardo es producido por una demora en la propagación y transmisión de paquetes dentro de la red. En una red puedes establecerse retardos de tránsito y de procesamiento, sin embargo estos retardos no pueden ser mayores a 150 ms dado que estos se consideran retardos importantes.

Mientras las tramas recorren las redes IP, estas pueden perderse como resultado de una congestión o corrupción en el camino. Además, para tráfico de tiempo real como la voz, la retransmisión de tramas perdidas en la capa de transporte no es práctica por ocasionar retardos adicionales. Por consiguiente, los terminales de voz tiene que retransmitir con muestras de voz perdidas, también llamadas “tramas borrables”. El efecto de las tramas perdidas en la calidad de voz depende de cómo las terminales gestionen las “tramas borrables”. (Wikipedia, 2011)

En el caso más simple si se pierde una muestra de voz el terminal dejara un intervalo en el flujo de voz. Si muchas tramas se pierden, sonara grietoso con silabas o palabras perdidas. Una posible estrategia de recuperación es reproducir las muestras de voz previas. Esto funciona bien si solo unas cuantas muestras son perdidas. Para combatir mejor las ráfagas de errores usualmente se emplean sistemas de interpolación. Basándose en muestras de voz previas, el decodificador predecirá las tramas perdidas.

1.8.2 Escalabilidad

Cuando una empresa inicia el número de empleados no es grande, los equipos y demandas de acceso de una red no son tan altos. Sin embargo, con el transcurrir y desarrollo de la empresa estos ámbitos aumentarán. Es decir, con el crecimiento de la empresa será necesario expandir y mejorar los servicios de la red.

Al diseñar una red es importante pensar en todas estas posibilidades, pues el reformar la red de cero requiere la inversión completa de una nueva red, siendo esta más costosa que reestructurarle solo parcialmente.

El uso inicial de un equipo que permita a las empresas funcionar previendo los posibles cambios a futuros años, le evitara gastos en equipos de red con mayor frecuencia. Entre estos hay que mencionar las velocidades de transmisión (Ver Figura. 1-31) y la capacidad de expansión de red que se refleja en el número de puertos que el router o switch. No obstante para incrementar el número de usuarios a los que se les puede dar acceso red es necesario un rediseño de la dirección de cada subred dentro de la LAN (Ver Figura. 1-32).

El término “colisiones” sobresale en esta parte, pues al aumentar el tamaño de una red existe una mayor probabilidad que estas ocurran. Una colisión es cuando dos o más equipos deciden ocupar el mismo medio para transmitir datos al mismo tiempo, esto genera una confusión en el sistema. Para solucionarles se utilizan ciertos métodos de los cuales se hablarán en la siguiente unidad.

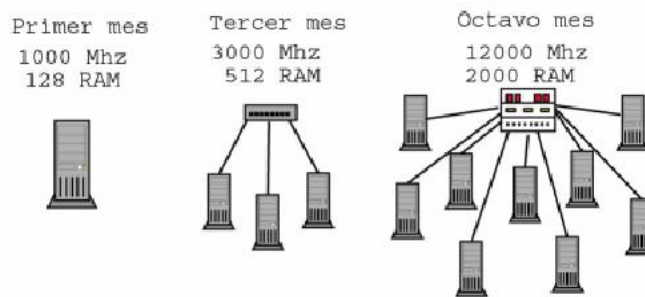


Figura. 1-31 Mejoramiento de la red en relación al tiempo.



Figura. 1-32 Ejemplo de incremento de recursos de red en relación a la cantidad de usuarios.

1.8.3 Calidad de servicios

Con los nuevos servicios implementados y servicios a implementar es necesario tener un control de calidad sobre estos. A medida que aumentan estos, se pueden ver afectados o deteriorados los primeros por que el ancho de banda para transferencia de datos se debe compartir entre más servicios.

Por otro lado, se valora la calidad de servicios basándose en aspectos como tolerancia a fallas y escalabilidad de la red en que se implementan. Según normas de CISCO, el factor de calidad es comparado con el nivel de experiencia que tiene un usuario como si estuviera frente a otro. Esto último solo es aplicable a servicios como llamadas vía on-line y video en tiempo real. (CISCO, 2008)

En el caso de las redes tradicionales, la transmisión de voz y video la calidad del servicio que brindan no se ve afectada pues la red está diseñada específicamente para ello, los medios son los más adecuados y la plataforma que ocupan es únicamente para esto. En el caso de una red de datos el factor de calidad se ve afectado directamente por el tipo de arquitectura que se decida utilizar para implementar la red (Ver Figura. 1-33).



Figura. 1-33 Aspectos a valorar para implementar un servicio.

En esta parte, también se ven involucrados el tipo de protocolo en el que se implementa el servicio. También existe un trade-off entre el ancho de banda que requiere aplicar un protocolo en un servicio¹⁸ y la calidad mínima para implementar el servicio. Es decir, se puede aplicar un protocolo que genere una mejor calidad de voz pero que consuma un mayor ancho de banda pero que traerá retrasos en la reproducción del mismo, o un protocolo que no generara retrasos a costa de pérdidas esporádicas de datos. Este caso se valorara en las unidades siguientes al tratar la capa de transporte y la unidad de protocolos TCP y UDP.

¹⁸ Un mayor ancho de banda significa un incremento en el costo para la transmisión de datos fuera de la LAN

1.8.3.1 QoS y Aplicaciones

Un flujo es un conjunto de paquetes que van de un origen a un destino. En una red orientada a la conexión, todos los paquetes que pertenezcan a un flujo siguen la misma ruta; en una red sin conexión, pueden seguir diferentes rutas. La necesidad de cada flujo se puede caracterizar por cuatro parámetros principales: confiabilidad, retardo, fluctuación y ancho de banda. Estos parámetros en conjunto determinan la QoS (calidad del servicio) que el flujo requiere. En la Tabla 1-1 se listan varias aplicaciones y el nivel de sus requerimientos.

Tabla 1-1

Aplicación	Confiabilidad	Retardo	Fluctuación	Ancho de banda
Correo electrónico	Alta	Bajo	Baja	Bajo
Transferencia de archivos	Alta	Bajo	Baja	Medio
Acceso a Web	Alta	Medio	Baja	Medio
Inicio de sesión remoto	Alta	Medio	Media	Bajo
Audio bajo demanda	Baja	Bajo	Alta	Medio
Vídeo bajo demanda	Baja	Bajo	Alta	Alto
Telefonía	Baja	Alto	Alta	Bajo
Videoconferencia	Baja	Alto	Alta	Alto

Las aplicaciones de correo electrónico, transferencia de archivos, acceso a Web e iniciación de sesión remota tienen requerimientos rigurosos en cuanto a confiabilidad (Ver Tabla 1-1). El cumplimiento de esta exigencia generalmente se logra haciendo una suma de los bits 1 que contiene el paquete y luego se almacena dicho valor en un campo específico, al llegar el paquete al receptor, este último se encarga de realizar nuevamente la suma y compara con el valor que adjunto el transmisor. En cambio, las 4 últimas aplicaciones de la Tabla 1-1, pueden tolerar errores, por lo que ni se realizan ni comprueban sumas de verificación.

Las aplicaciones de transferencia de archivos, incluyendo correo electrónico y video, no son sensibles al retardo. Si todos los paquetes se retrasan unos segundos de manera uniforme, no hay daño. Las aplicaciones interactivas, como la navegación en Web y el inicio de sesión remoto, son más sensibles al retraso. Las aplicaciones en tiempo real, como la telefonía y la videoconferencia, tienen requerimientos estrictos de retardo. Si cada una de las palabras de una llamada telefónica se retrasa exactamente por 2 segundos, los usuarios hallarán la conexión inaceptable.

Las primeras tres aplicaciones no son sensibles a los paquetes que llegan con intervalos de tiempo irregulares entre ellos. El vídeo y especialmente el audio son en extremo sensibles a la fluctuación. Si un usuario está observando vídeo a través de la red y todos los cuadros se retrasan exactamente 2 segundos, no hay daño. Pero si el tiempo de transmisión varía de manera aleatoria entre 1 y 2 segundos, el resultado sería terrible. En el audio, una fluctuación de incluso unos cuantos milisegundos es claramente audible.

1.8.3.2 Mantener el servicio activo acorde a su prioridad.

Algunos de los servicios que se brindan por internet tienen una mayor gravedad en cuanto a transmisión de datos. Por gravedad nos referimos a que no pueden esperar a ser recibidos, pues su nivel de calidad se disminuya considerablemente si se retrasa la entrega de los paquetes.

Este es el caso de una llamada de voz o video llamada, los paquetes de voz que llegan muy retrasados serán eliminados por el receptor o distorsionaran la conversación entre usuarios. Una de las técnicas implementadas para evitar los retrasos de paquetes es el garantizar un cierto porcentaje de ancho de banda de la red total (Ver Figura. 1-34). Se debe tener en cuenta que estas prioridades pueden variar acorde a las necesidades o servicios que se desean implementar en la red.

A continuación se muestra una lista de servicios y el orden según las posibles prioridades de una empresa (CISCO, 2008):

- Comunicaciones sensibles al tiempo: aumentan la prioridad por servicios como el teléfono o la distribución de vídeos.
- Comunicaciones no sensibles al tiempo: disminuyen la prioridad de recuperación de páginas Web o de correos electrónicos.
- Mucha importancia para la empresa: aumenta la prioridad de control de producción o de datos de transacciones comerciales.
- Comunicación indeseable: disminuye la prioridad o bloquea la actividad no deseada como la transferencia de archivos entre pares o el entretenimiento en vivo.



Figura. 1-34 Designación de ancho de banda en relación a la prioridad del tráfico.

1.8.3.3 Técnicas para alcanzar buena calidad de servicio.

Las técnicas que se presentan a continuación tienen como finalidad cumplir con los requerimientos de QoS planteados. Sin embargo, ninguna técnica proporciona un QoS eficiente y confiable de una forma ideal. En su lugar, se han desarrollado una variedad de técnicas, con soluciones prácticas que con frecuencia se combinan múltiples procedimientos.

1.8.3.3.1 Sobreaprovisionamiento

Una solución fácil es proporcionar la suficiente capacidad de enrutador, espacio en búfer y ancho de banda como para que los paquetes fluyan con facilidad. El problema con esta solución es que es costosa. Conforme pasa el tiempo y los diseñadores tienen una mejor idea de cuánto es suficiente, esta técnica puede ser práctica. En cierta medida, el sistema telefónico tiene un sobreaprovisionamiento. Es raro levantar un auricular telefónico y no obtener un tono de marcado instantáneo. Simplemente hay mucha capacidad disponible ahí que la demanda siempre se puede satisfacer.

1.8.3.3.2 Almacenamiento en búfer.

Los flujos pueden almacenarse en el búfer en el lado receptor antes de ser entregados. Almacenarlos en el búfer no afecta la confiabilidad o el ancho de banda, e incrementa el retardo, pero atenúa la fluctuación. Para el vídeo o audio bajo demanda, la fluctuación es el problema principal, por lo tanto, esta técnica es muy útil.

La Figura. 1-35 muestra un ejemplo de cómo funciona el almacenamiento de los datos en búfer.

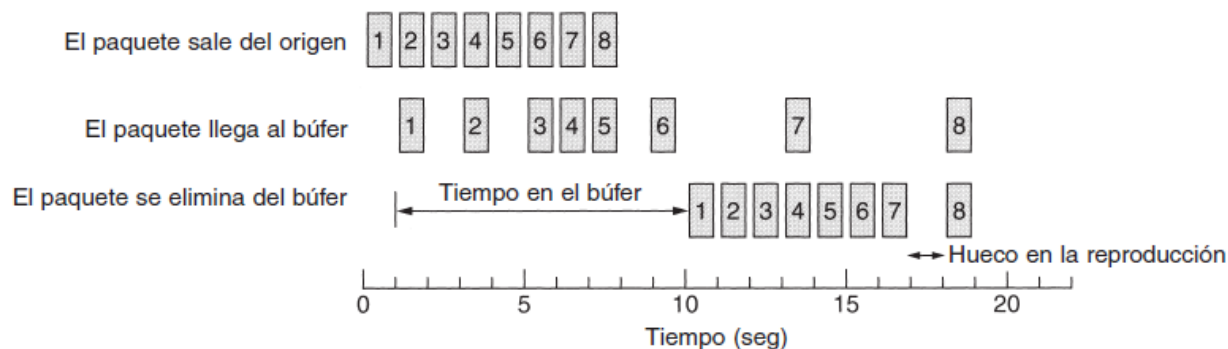


Figura. 1-35 Refinamiento del flujo de paquetes en el búfer

El paquete 1 se envía desde el servidor a $t=0$ y llega al cliente a $t=1$. El paquete 2 tiene un retardo mayor; tarda 2 segundos en llegar. Conforme llegan los paquetes, se almacenan en el búfer de la máquina cliente. En el segundo $t=10$, la reproducción continúa. En este momento, los paquetes 1 a 6 se han almacenado en el búfer de manera que pueden eliminarse de él en intervalos uniformes para una reproducción suave.

Observe que el paquete 8 se ha retrasado tanto que no está disponible cuando le toca el turno a su ranura de reproducción, por lo que esta debe esperar hasta que llegue dicho paquete, creando un molesto hueco en la música o película. Este problema se puede atenuar retrasando el tiempo de inicio aún más, aunque hacer eso también requiere un búfer más grande. Los sitios Web comerciales que contienen transmisión continua de vídeo o audio utilizan reproductores que almacenan en el búfer por aproximadamente 10 segundos antes de comenzar a reproducir.

1.8.3.3.3 Modelo de tráfico

En la Figura. 1-35, el origen envía los paquetes con un espaciado uniforme entre ellos, pero en otros casos, podrían emitirse de manera regular, lo cual puede causar congestión en la red. El envío no uniforme es común si el servidor está manejando muchos flujos al mismo tiempo, y también permite otras acciones, como avance rápido y rebobinado, autenticación de usuario y otras opciones.

El modelado de tráfico consiste en regular la tasa promedio de la transmisión de los datos. En contraste, los protocolos de ventana corrediza que estudiamos anteriormente limitan la cantidad de datos en tránsito de una vez, no la tasa a la que se envían. Cuando se establece una conexión, el usuario y la subred acuerdan cierto patrón de tráfico para ese circuito. Algunas veces esto se llama acuerdo de nivel de servicio. En tanto el cliente cumpla con su parte del contrato y sólo envíe los paquetes acordados, la empresa portadora promete entregarlos de manera oportuna. El modelado de tráfico reduce la congestión y,

por lo tanto, ayuda a la empresa portadora a cumplir con su promesa. Tales acuerdos no son tan importantes para las transferencias de archivos pero sí para los datos en tiempo real, como conexiones de vídeo y audio, lo cual tiene requerimientos rigurosos de calidad de servicio.

1.8.3.3.3.1 Algoritmo de cubeta con goteo

Con esta técnica cada host está conectado a la red mediante una interfaz que contiene una cubeta con goteo, es decir, una cola interna infinita. Si llega un paquete cuando la cola está llena, éste se descarta. En otras palabras, si uno o más procesos del host tratan de enviar paquetes cuando la cola ya tiene la cantidad máxima de paquetes, dicho paquete se descarta sin más. Este arreglo puede incorporarse en la interfaz del hardware, o simularse a través del sistema operativo del host. El esquema fue propuesto inicialmente por Turner (1986), y se llama algoritmo de cubeta con goteo. De hecho, no es otra cosa que un sistema de encolamiento de un solo servidor con un tiempo de servicio constante.

El algoritmo permite que un flujo desigual de paquetes de los procesos de usuario dentro del host en un flujo continuo de paquetes hacia la red, moderando las ráfagas y reduciendo en una buena medida las posibilidades de congestión.

Cuando todos los paquetes son del mismo tamaño (por ejemplo, celdas ATM), este algoritmo puede usarse como se describe. Sin embargo, cuando se utilizan paquetes de tamaño variable, con frecuencia es mejor permitir un número fijo de bytes por pulso, en lugar de un solo paquete. Por lo tanto, si la regla es de 1024 bytes por pulso, sólo pueden recibirse por pulso un paquete de 1024 bytes, dos paquetes de 512 bytes, cuatro paquetes de 256 bytes, etcétera.

1.8.3.3.4 Reservación de recursos

El hecho de tener la capacidad de regular la forma del tráfico ofrecido es un buen inicio para garantizar la calidad del servicio. Sin embargo, utilizar efectivamente esta información significa de manera implícita obligar a todos los paquetes de un flujo a que sigan la misma ruta. Su envío a través de enrutadores aleatorios dificulta garantizar algo. Como consecuencia, se debe configurar algo similar a un circuito virtual del origen al destino, y todos los paquetes que pertenecen al flujo deben seguir esta ruta.

Una vez que se tiene una ruta específica para un flujo, es posible reservar recursos a lo largo de esta ruta para asegurar que la capacidad necesaria esté disponible. Se pueden reservar tres tipos de recursos (Tanenbaum, 2003):

- ✓ Ancho de banda
- ✓ Espacio de búfer
- ✓ Ciclos de CPU

Si un flujo requiere 1 Mbps y la línea saliente tiene una capacidad de 2 Mbps, tratar de dirigir tres flujos a través de esa línea no va a funcionar. Por lo tanto, reservar ancho de banda significa no sobrecargar ninguna línea de salida.

El espacio de búfer resulta ser un recurso más escaso. Si no hay búfer disponible, el paquete se tiene que descartar debido a que no hay lugar para colocarlo. Para una calidad de servicio, es posible reservar algunos búferes para un flujo específico de manera que este no tenga que competir con otros flujos para obtener espacio en búfer. Los ciclos de CPU también son un recurso escaso. Para procesar un paquete se necesita tiempo de CPU del enrutador, por lo que un enrutador solo puede procesar cierta cantidad de paquetes por segundo. Para asegurar el procesamiento oportuno de cada paquete, es necesario verificar que la CPU no esté sobrecargada.

1.8.4 Seguridad

Con el crecimiento rápido del internet y más accesibilidad a esta, los administradores de red se vieron obligados a implementar nuevos métodos de seguridad para evitar que hackers o crackers invadieran los servidores que contenían sus páginas web y bases de datos.

El tema de seguridad es de gran importancia pues es necesario proteger los datos de las empresas. Imaginemos una red de Bancos que no posee sistema de autenticación para el acceso a sus bases de datos, cualquier usuario podría acceder para alterar su cuenta bancaria u otra.

Claro está que los sistemas bancarios utilizan redes privadas para la conexión entre sus sucursales. Sin embargo, en un caso más a nuestro alcance, ¿Que sería de los servidores Hotmail sin sistemas de seguridad? Cualquier usuario podría acceder a nuestra cuenta y revisar los e-mails privados que se tengan.

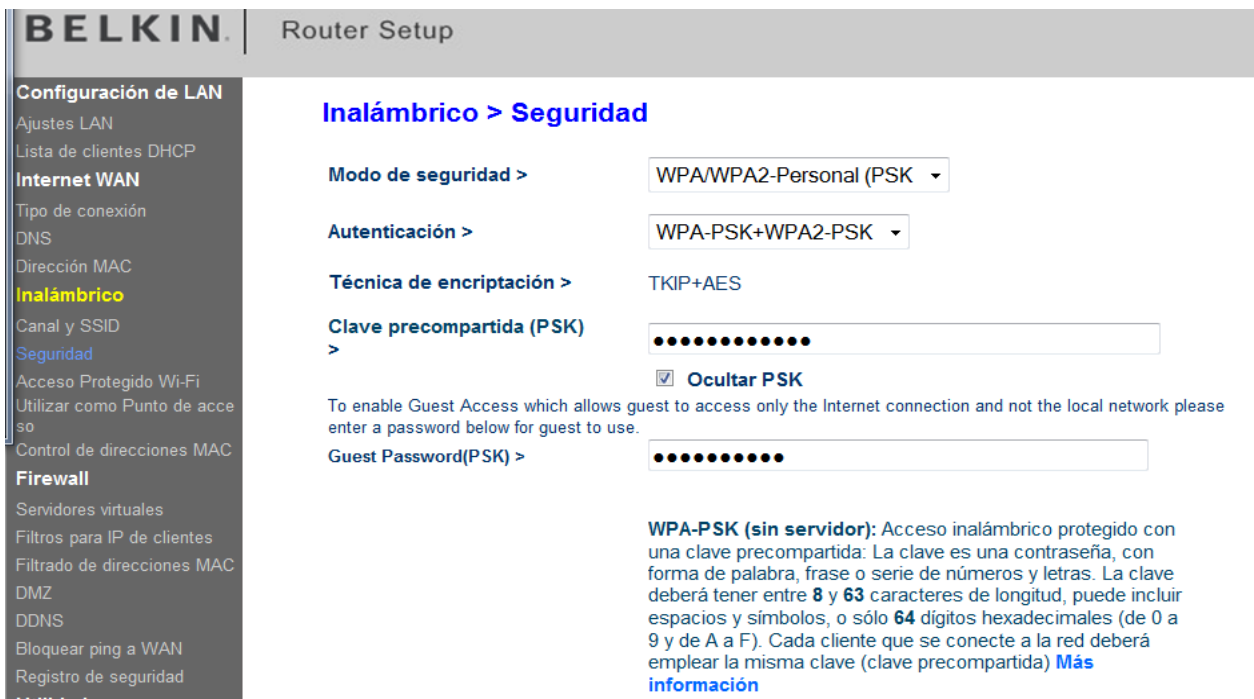


Figura. 1-36 Ejemplo de modo de seguridad implementado en un router.

Aunque el tema de seguridad no solo se limita al acceso prohibido a servidores. La seguridad se implementa incluso en sistemas LAN de los hogares (Ver Figura. 1-36). Una red doméstica por lo general posee un router que da la opción de clave de acceso a la red de la casa. Es necesario pues cualquier usuario puede acercarse al hogar con el único objetivo de acceder a nuestra red y de tal forma robar ancho de banda. Esta clave de seguridad es encriptada de forma que no sea fácil de obtener. El formato de encriptación de los datos estar dado por las características del router que se tenga.

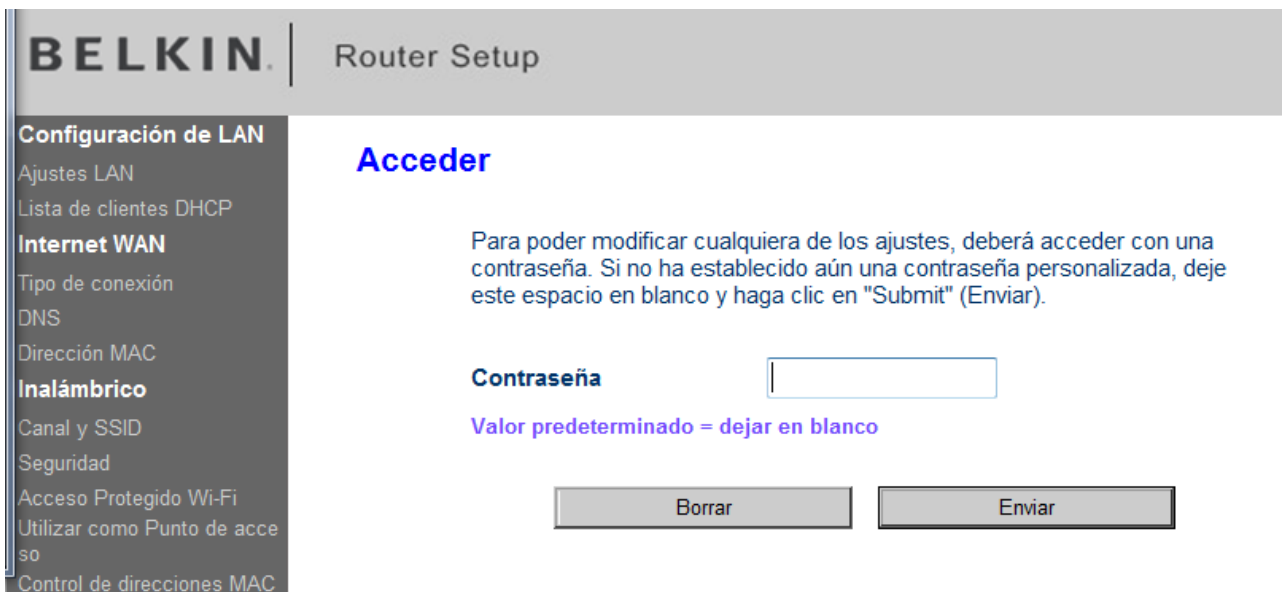


Figura. 1-37 Router solicitando clave de acceso para ingresar a configuraciones.

En algunos casos el agregar una clave de acceso (Ver Figura. 1-37) a nuestro router no es suficiente, también se puede realizar el proceso de filtrado por MAC (Ver Figura. 1-38). La dirección MAC de un dispositivo no es más que un código de 48 Bits agregado por la fábrica a cualquier dispositivo que se conecte a red. Este código MAC es único para cualquier tarjeta de red. Por lo tanto al agregarlo en la lista de filtro solo este y los otros equipos en la lista tendrán acceso.



Figura. 1-38 Configuración de filtrado MAC en un router.

1.8.4.1 Redes Virtuales Privadas

Algunas empresas tienen oficinas distribuidas en muchas ciudades o países. Inicialmente las empresas que deseaban llevar a cabo la interconexión entre sus distintas partes debían alquilar líneas a compañías telefónicas. Una red constituida por computadoras de compañías y líneas telefónicas se conoce como red privada. La Figura. 1-39 muestra una red privada virtual de ejemplo con 5 partes con ubicaciones posiblemente separadas geográficamente.

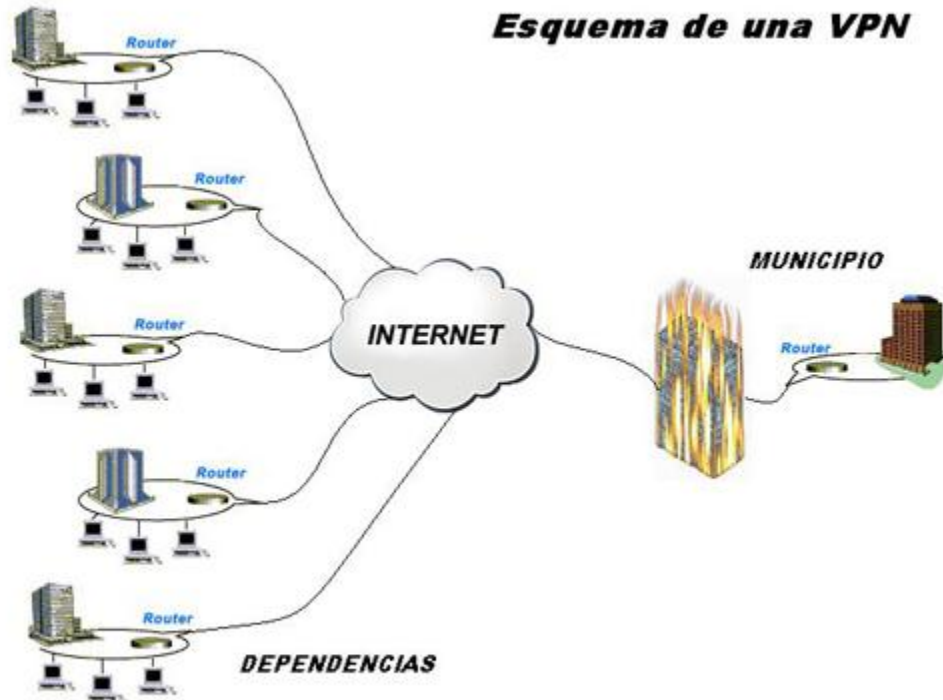


Figura. 1-39 Ejemplo VPN

Las redes privadas funcionan bien y son muy seguras, Si las únicas líneas disponibles son las alquiladas, el tráfico no puede fugarse de las ubicaciones de la compañía y los intrusos tienen que intervenir físicamente las líneas para infiltrarse, lo cual no es fácil de hacer. El problema con alquilar las líneas privadas es el costo que esto involucra. Con el aparecer de las redes de datos como Internet, muchas compañías quisieron trasladar su tráfico de datos a la red pública, aunque sin querer renunciar a la seguridad de la red privada.

Esto dio como origen la creación de Redes Privadas Virtuales¹⁹ que son redes superpuestas sobre redes públicas pero con muchas propiedades de las redes privadas. Se llaman virtuales porque son solo una ilusión, al igual que los circuitos virtuales no son circuitos reales ni la memoria virtual es memoria real.

Las VPNs pueden construirse directamente sobre internet. Un diseño común es equipar cada oficina con una firewall y crear túneles a través de Internet entre todos los pares de una oficina. Las partes involucradas en la VPN deben intercambiar los parámetros sobre autenticación y envío de datos. Una vez realizado este proceso el tráfico puede comenzar a fluir. Para un enrutador en Internet, un paquete que viaja a través de un túnel VPN es solo un paquete ordinario. Lo único extraño es la presencia de un encabezado

¹⁹ VPN = Private Virtual Network – Red Privada Virtual

especial luego del encabezado IP, pero debido a que estos encabezados adicionales no tienen efecto en el proceso de reenvío, los enrutadores no se preocupan por ellos (Tanenbaum, 2003).

La ventaja principal de organizar de esta forma una VPN es que es completamente transparente para todo el software de usuario. Los firewalls configuran y manejan los parámetros de sesión y comunicación. La única persona consciente de esta configuración es el administrador del sistema o red. (Tanenbaum, 2003)

1.8.4.2 Firewalls

Un firewall está constituido por un grupo de programas, ubicado como un servidor en la puerta de enlace a internet de una LAN. Este sistema protege los recursos y a los usuario de una red, del acceso ilícito a esta por parte de usuarios externos (Ver Figura. 1-40). Una red enterprise con una intranet en donde sus trabajadores necesitan el acceso de internet, debe utilizar un firewall para evitar a usuarios externos el acceso a los recursos de datos privados. (Whatls.com, 2009)

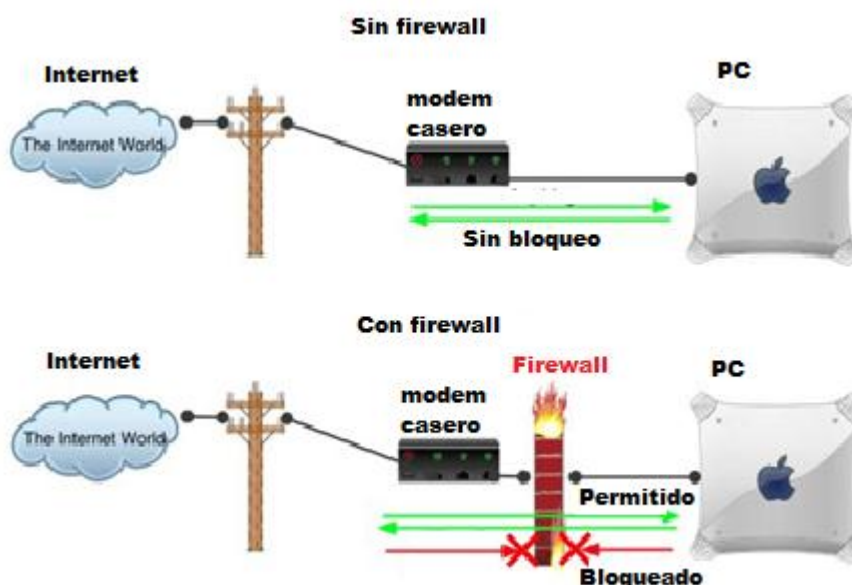


Figura. 1-40 Acceso de una PC con y sin el uso de de un Firewall.

Básicamente, un firewall opera con un programa²⁰ (Ver Figura. 1-41) muy similar al de un router. Pues el firewall debe examinar cada paquete de red para determinar si debe permitir la transmisión del paquete a su destino. Un firewall por lo general se instala en un ordenador separado del resto de la red para evitar que las peticiones de entrada proveniente de internet puedan acceder de forma directa a los recursos de la red privada.

²⁰ Algunos firewalls se venden como productos comerciales. Ejemplo de estos son: Firestarter, ZoneAlarm, Uncomplicated Firewall y Gutw.



Figura. 1-41 Ejemplo de programa firewall.

Existe una gran cantidad de métodos para implementar un firewall. Uno de los métodos más simples es configurarlo de tal forma que al recibirse una petición proveniente de un usuario externo desconocido el firewall envía un mensaje al administrador de red solicitando la autorización. En algunos casos se puede configurar un firewall para que reconozca un ordenador específico para permitir el acceso a los recursos incluso desde fuera de la intranet (Ver Figura. 1-42).

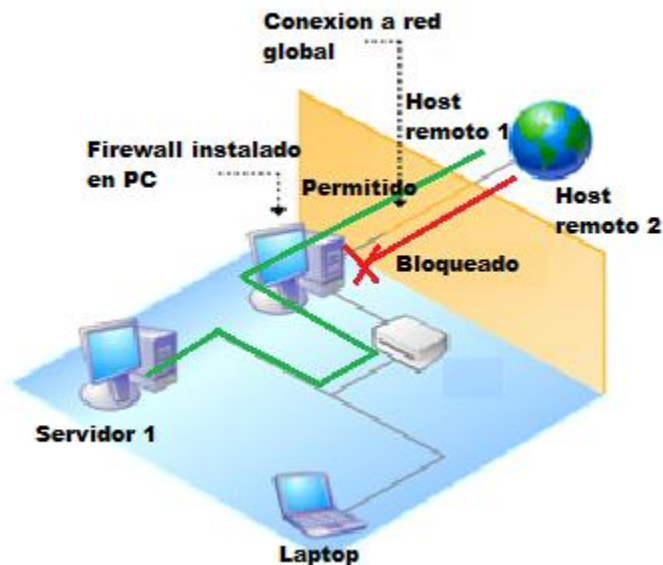


Figura. 1-42 Ejemplo de bloqueo a usuarios remotos no autorizados.

1.9 Importancia en Telefonía

Una de las importancias de usar Internet como plataforma para telefonía convencional, es la disminución de costos al realizar llamadas; para ello es necesario el uso de protocolos de transferencia de tiempo real (RTP²¹_{xii} y RTCP²²_{xiii}) utilizados en la mensajería instantánea, el protocolo IP²³_{xiv} como protocolo de red, y protocolos UDP²⁴_{xv} como protocolo de transporte. Estos protocolos permiten que la señal de voz pueda viajar a través de la red de forma segura y con cierto grado de confiabilidad.

Ya existen algunos sistemas que implementan los mencionados anteriormente como son sistemas que laboran bajo protocolos SIP²⁵_{xvi}. Este es el caso de las centrales telefónicas virtuales como Asterisk (Ver Figura. 1-43) o algún otro sistema de PBX²⁶_{xvii} (Ver. Figura. 1-44).

Este sistema de PBX se deja para el final del curso como ultimo modulo, debido a que primero, es necesario comprender tanto conceptos de redes de datos como de telefonía IP.

Figura. 1-44 Conexiones IP PBX a otras redes.

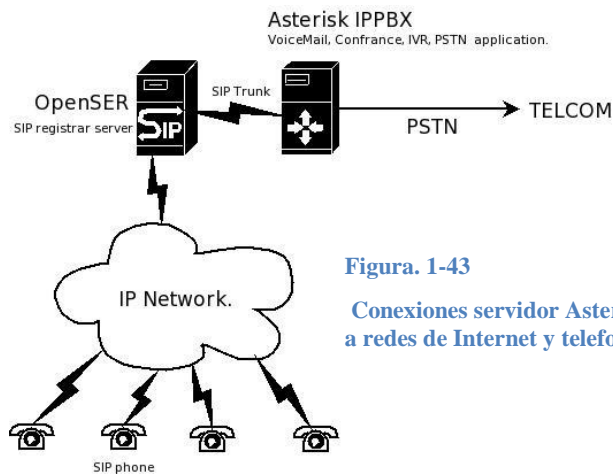
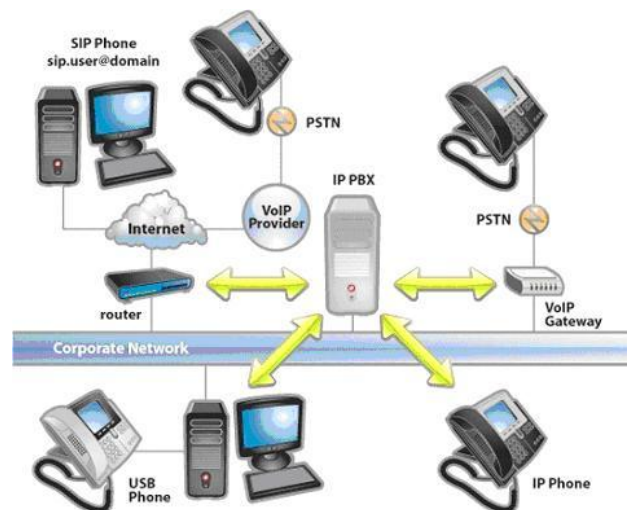


Figura. 1-43
Conexiones servidor Asterisk a redes de Internet y telefonía



²¹ RTP = Real Time Transfer Protocol = Protocolo de Transferencia en Tiempo real

²² RTCP = Real Time Control Protocol = Protocolo de Control de Transferencia en Tiempo real.

²³ IP = Internet Protocol – Protocolo de Internet

²⁴ UDP = User Datagram Protocol – Protocolo de Unidad de Datagrama

²⁵ SIP= Session Initiation Protocol – Protocolo de Inicio de Sesión.

²⁶ PBX = Private Branch Exchange - Central Privada de Conmutación.

1.10 Términos

A continuación se presentan algunos términos empleados en el estudio de redes computadoras.

Cable de conexión directa: cable de cobre trenzado no blindado (UTP) para conectar dispositivos de red diferentes.

Cable de conexión cruzada: cable de cobre UTP para conectar dispositivos de red diferentes.

Cable serial: cable de cobre típico de las conexiones de área ancha.

Ethernet: tecnología dominante de red de área local.

Dirección MAC: Capa 2 de Ethernet, dirección física.

Dirección IP: dirección lógica

Máscara de subred de Capa 3: necesario para interpretar la dirección IP.

Gateway por defecto: la dirección IP en la interfaz del router a la que una red envía el tráfico que sale de la red local.

NIC: tarjeta de interfaz de red; el puerto o interfaz que permite a un dispositivo final participar en una red.

Puerto (hardware): interfaz que le permite a un dispositivo red participar en la red y estar conectado a través del medio de networking.

Puerto (software): dirección de protocolo de Capa 4 en la suite TCP/IP.

Interfaz (hardware): un puerto.

Interfaz (software): punto de interacción lógica dentro del software.

PC: dispositivo final.

Estación de trabajo: dispositivo final.

Switch: dispositivo intermedio que toma decisiones sobre las tramas basándose en direcciones de Capa 2 (típicas direcciones MAC Ethernet).

Router: dispositivo de capa 3, 2 y 1 que toma decisiones sobre paquetes basados en direcciones de Capa 3 (generalmente direcciones IPv4.)

Bit: dígito binario, lógico 1 o cero, tiene varias representaciones físicas, como pulsos eléctricos, ópticos o microondas. PDU²⁷ de Capa 1.

Trama: PDU de Capa 2.

²⁷ PDU = Unidad de datos de protocolo.

1.11 Preguntas de control.

1. ¿Qué es una red de datos?
2. ¿Qué es un Host?
3. ¿Cuáles son los tipos de redes de datos según su cobertura en área geográfica?
4. ¿Qué es una Internetwork?
5. Defina Intranet
6. Defina Red Enterprise
7. Mencione algunos servicios de los servicios más comunes que operan en la red de datos global.
8. ¿Cuáles son los 2 tipos de topologías que existen? Explique brevemente cada una de ellas.
9. Enumere 4 tipos de topologías lógicas. Explique brevemente en que consiste cada una de ellas.
10. ¿Qué es una topología física? De algún ejemplo.
11. Explique brevemente en qué consiste el procesamiento centralizado.
12. Explique brevemente en qué consiste el procesamiento distribuido.
13. ¿Cuál es una desventaja de un sistema de procesamiento centralizado?
14. ¿Cuáles son las funciones que debe realizar el sistema operativo de un sistema distribuido?
15. Enumere algunos elementos de una red de datos.
16. ¿Qué es un servidor Proxy? De un ejemplo.
17. Enumere los aspectos importantes que se deben considerar al momento de diseñar o valorar una red de datos.
18. ¿Cuál es la ventaja de un sistema conmutado por paquetes sobre un sistema conmutado por circuitos?
19. ¿Cuál es la ventaja de un sistema conmutado por circuito sobre un sistema conmutado por paquetes?
20. Explique el concepto de Jitter
21. Explique el concepto de Latencia
22. ¿Qué significa que un dispositivo sea escalable?

23. ¿Cuáles son los 2 aspectos que afectan directamente la calidad al brindar servicios?
24. ¿Cuál es la importancia de los buffers en el mejoramiento de la calidad de servicio?
25. Mencione posibles parámetros para establecer la prioridad en la entrega de paquetes.
26. Mencione y explique dos técnicas para el mejoramiento de calidad de servicio.
27. ¿En qué consiste el algoritmo de cubeta por goteo?
28. ¿Para qué sirve la reservación de recursos de un sistema?
29. ¿En qué consiste el proceso de filtrado MAC en un router?
30. ¿Qué es una VPN?
31. Explique ¿cuál es la función y como opera un Firewall?
32. En base a lo estudiado, ¿Cuál es la importancia de las redes de datos en el servicio telefónico?

Unidad II

Arquitectura de Redes de datos.

Objetivos General:

- Brindar al estudiante los conceptos necesarios para comprender las estructuras y funcionamiento básico de las arquitecturas de las redes de datos en general.

Objetivos Específicos:

- Mencionar la estructura del modelo OSI.
 - Decir de forma breve las funciones y servicios de las capas del modelo.
 - Señalar las características y aspectos más sobresaliente del modelo TCP/IP
-

Unidad 2. Arquitectura de una red de datos

2.1 Introducción

En esta sección se pretende desarrollar los dos modelos más utilizados en el estudio y fabricación de equipos de red. Los modelos a desarrollar son OSI (Ver Figura. 2-1) y el modelo TCP/IP (Ver Figura. 2-2) los modelos son de referencia y de protocolos, respectivamente.

El modelo de Referencia OSI proporciona como su nombre lo menciona una referencia para el diseño de protocolos y servicios de red. El modelo no sirve para llevar a cabo una implementación directa, ni establece de forma detallada los servicios de la arquitectura de red. El objetivo principal es permitir la comprensión de las funciones y procesos involucrados en la comunicación.

Por otro lado, un modelo de protocolo declara de forma detallada la estructura de una suite de protocolos en particular. El conjunto de protocolos detalla en cada capa la funcionalidad que se requiere para interconectar a las personas o usuarios con la red de datos. El modelo TCP/IP se considera un modelo de protocolos pues detalla las funciones de cada capa dentro del esquema de TCP/IP.

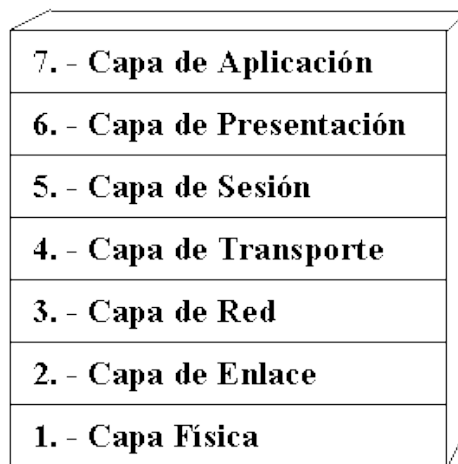


Figura. 2-1 Capas del modelo OSI

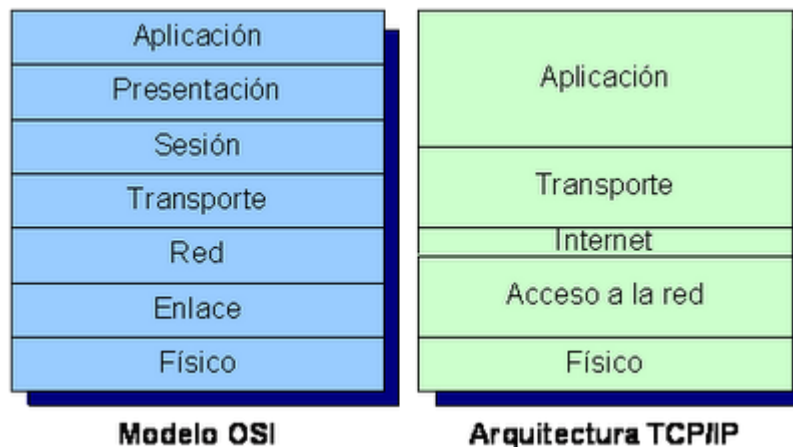


Figura. 2-2 Correspondencia de capas Modelos TCP/IP y OSI.

Los modelos mencionados son los principales al analizar las funcionalidades de red. No obstante, los diseñadores de protocolos de red, servicios o dispositivos pueden crear modelos propietarios o exclusivos para usar en sus productos. La organización internacional de estandarización exige a los diseñadores que asocien sus nuevos equipos y servicios a ambos modelos para que sean capaces de operar sin problemas.

2.2 Estructura del modelo de referencia OSI.

2.2.1 Introducción

El modelo de interconexión de sistema abierto o bien conocido como modelo OSI que fue aprobado en 1984 bajo la norma ISO 7498. Actualmente, es el esquema de referencia para internetworks más conocido. Permite el diseño de redes de datos junto con detalles generales para el funcionamiento y resolución de problemas.

Surgió como respuesta ante la necesidad de interconectar sistemas de distintos fabricantes que empleaban sus propios protocolos.

Este modelo fue creado como referencia, lo que implicaba en un comienzo que los fabricantes no necesariamente tienen que sujetarse a la estructura que plantea. Pero al convertirse este en un estándar todos los equipos que no son compatibles o que basan su funcionamiento en este modelo quedan desligados o relegados en el mercado. Esto se debía a que los usuarios no desean verse obligados a comprar productos de una sola marca.

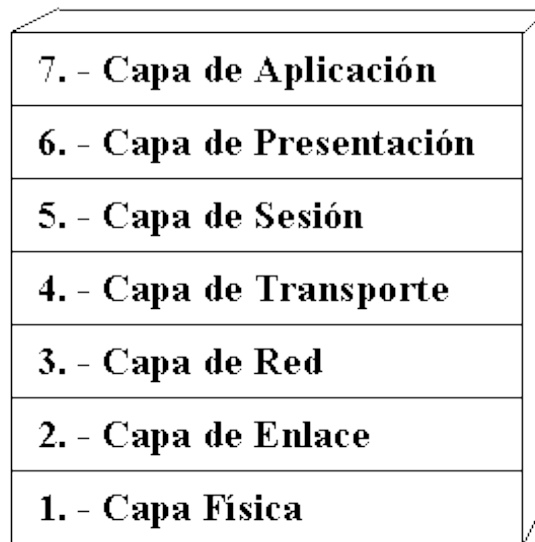


Figura. 2-3 Capas del modelo OSI

El modelo tiene una arquitectura de 7 capas (Ver Figura. 2-3) o niveles de los cuales se pueden desplegar o diseñar protocolos específicos que permitan a la variedad de usuarios comunicarse abiertamente. Para hacer la división de estas 7 capas la organización internacional de estandarización se debió basar en ciertos criterios.

A continuación se presentan los criterios para el desarrollo del modelo (Stallings, 2004):

- 1) No crear demasiadas capas de tal forma que la descripción e integración de las capas implique más dificultades de las necesarias.
- 2) Crear una separación entre capas en todo punto en el que la descripción del servicio sea reducida y el número de interacciones a través de dicha separación sea pequeña.
- 3) Crear capas separadas allá donde las funciones sean manifiestamente diferentes tanto en la tarea a realizar como en la tecnología involucrada.
- 4) Agrupar funciones similares en la misma capa.
- 5) Fijar separaciones en aquellos puntos en los que la experiencia acumulada haya demostrado su utilidad.
- 6) Crear capas que puedan ser rediseñadas en su totalidad y los protocolos cambiados de forma drástica para aprovechar eficazmente cualquier innovación que surja tanto en la arquitectura, el hardware o tecnologías de software, sin tener que modificar los servicios ofrecidos o usados por las capas adyacentes.
- 7) Crear una separación allá donde sea conveniente tener la correspondiente interfaz normalizada.
- 8) Crear una capa donde haya necesidad de un nivel distinto de abstracción (morfológico, sintáctico o semántico) a la hora de gestionar los datos.
- 9) Permitir que los cambios en las funciones o protocolos se puedan realizar sin afectar a otras capas.
- 10) Para cada capa establecer separaciones solo con sus capas inmediatamente superiores o inferiores.
- 11) Cada capa debe tener conocimiento de los niveles inmediatamente adyacentes y solo de estos.
- 12) Toda capa debe servirse de los servicios del nivel anterior y de igual forma prestar servicios a la capa superior.

En algunas capas de los modelos es necesario crear subcapas para implementar funciones. De igual forma existen criterios que permiten definir las propiedades de estas subcapas (Stallings, 2004):

- 1) Luego de crear las capas se pueden crear sub-agrupamientos y reestructurar las funciones formando subcapas dentro de una capa en aquellos casos en los que se necesiten diferentes servicios de comunicación.
- 2) Crear, donde sea necesario, dos o más subcapas con una funcionalidad común, y mínima, para permitir operar con las capas adyacentes.
- 3) Permitir la no utilización de una subcapa dada. Es decir, dejar a opción del diseñador de red el uso o no de las funciones proporcionadas por dicha subcapa.

2.2.2 Capas del modelo OSI.

2.2.2.1 Capa física

La capa física se encarga de la comunicación física que se da través de los medios entre los dispositivos. Es decir, esta capa define la forma en que son transmitidos los bits. El propósito principal de este nivel es definir las reglas para garantizar que cuando la computadora emisora transmita el bit 1, la computadora receptora verifique que un 1 fue recibido y no un 0.

Las principales características de este nivel son (Stallings, 2004):

Mecánicas: Relacionadas con las propiedades físicas de la interfaz con el medio de transmisión. Normalmente, dentro de estas características se incluye la especificación del conector que transmite las señales a través de conductores. A estos últimos se les denomina circuitos.

Eléctricas: Especifican como se representan los bits (por ejemplo, en términos de niveles de tensión), así como su velocidad de transmisión.

Funcionales: especifican las funciones que realiza cada uno de los circuitos de la interfaz física entre el sistema y el medio de transmisión.

De procedimiento: Especifican la secuencia de eventos que se llevan a cabo en el intercambio de flujo de bits a través del medio físico.

2.2.2.2 Capa de enlace de datos.

Mientras la capa física proporciona exclusivamente un servicio de transmisión de datos en los medios físico, la capa de de enlace de datos pretende hacer que el enlace físico sea fiable. De igual forma, proporciona los medios para activar, mantener y desactivar el enlace. El principal servicio proporcionado por la capa de enlace de datos a las capas superiores es el de detección y control de errores. Así, si se dispone de un protocolo en la capa de enlace de datos completamente operativo, la capa adyacente superior puede suponer que la transmisión está libre de errores. Sin embargo, si la comunicación se realiza entre dos sistemas que no estén directamente conectados, la conexión constara de varios enlaces de datos en serie, cada uno operando independientemente.

Por lo tanto, en este último caso, la capa superior no estará libre de la responsabilidad del control de errores.

La capa de enlace de datos es el nivel donde los bits toman significado en la red. Haciendo una analogía puede decirse que esta capa corresponde al área de recepción y envío de una empresa de empaquetado, la cual toma los paquetes provenientes de la capa superior y los prepara para la transmisión en los medios. A su vez, recibe los paquetes

provenientes de capas inferiores y elimina los datos de control y expone la PDU de capa 3 para que pueda ser interpretada correctamente.

Entre sus funciones esta el notificar al emisor si alguno de los paquetes que se ha recibido se encuentra en mal estado, o si dado el caso, alguna trama no fue recibida y se requiere de su reenvío. De igual forma, si alguna trama fue enviada y recibida sin problema alguno.

Algunos de los protocolos de comunicación que se implementan en esta capa son HDLC y LLC. El protocolo HDLC opera a nivel de línea y es un estándar universal, que muchos utilizan como modelo. Los datos en este protocolo se organizan por tramas, siendo estas un grupo de bits que incluyen por redundancia y control para corregir los errores de transmisión; además regula el flujo de las tramas para sincronizar su transmisión y recepción, también enmascara a las capas superiores de las imperfecciones de los medios de transmisión utilizados.

2.2.2.2.1 Subcapas de la capa de enlace de datos.

2.2.2.2.1.1 LLC - control lógico de enlace (*Logical Link Control sublayer*)

La subcapa más alta del nivel 2 en el modelo de referencia OSI es la capa de control lógico. Esta subcapa multiplexa los protocolos que operan en la capa de enlace, y opcionalmente provee el control de flujo, reconocimiento, y notificación de error. El LLC provee direccionamiento y control del enlace de datos. Específica cual mecanismo deberá ser usado para direccionar a las estaciones sobre el medio de transmisión y controlar el intercambio de datos entre el transmisor y receptor.

2.2.2.2.1.2 MAC – Control de acceso al medio (*Media Access Control sublayer*)

La subcapa inferior a LLC es la subcapa de control de acceso al medio (MAC). Algunas veces se refiere a esta como la subcapa que determina, quien está permitido a acceder al medio en cualquier momento. En otras ocasiones se le atribuye la función de ser el encargado de la estructura de la trama con direcciones MAC en su interior.

Existen generalmente 2 formas de control de acceso al medio: estas son distribuidos y centralizados. Ambas formas pueden ser comparadas a la comunicación entre personas. En una red hecha de personas teniendo una conversación, podemos observar que algunos estarán hablando o si alguno aparente estar a punto de hablar y eso nos limitara a esperar un turno. Si 2 personas hablan al mismo tiempo, ellos se detendrán y se disculparan cediendo el habla a la otra persona.

La capa de control de acceso al medio también determina cuando una trama de datos termina o cuando la próxima va a comenzar, a este proceso se le llama sincronización de

tramas. Existen cuatro términos en el proceso de sincronización de tramas: el tiempo base, conteo de caracteres, relleno de byte y relleno de bit.

El tiempo base se enfoca simplemente en colocar una cantidad específica de tiempo entre las tramas. La mayor desventaja de esto es que puede surgir un mayor aumento en el tiempo que existe entre tramas o que los tiempos originales pueden perderse debido a influencias externas.

El conteo de caracteres simplemente nota la cuenta de caracteres restante en la cabecera de la trama. Este método, sin embargo, es fácilmente alterable si el campo obtiene un error en algún sentido, haciendo así muy difícil el mantener la sincronización.

El relleno de byte precede a la trama con una secuencia especial de byte tal como DEL STX y le añade a esta con DEL ETX. Las apariciones de DLE (byte value 0x10) tienen que ser “escapadas” con otro DLE. Las marcas de comienzo y detención o finalización son detectadas en el receptor y removidas tanto como las inserciones de caracteres DLE. (Wikipedia - Enlace de datos, 2010)

Similarmente, el relleno de bit reemplaza estas marcas de comienzo y final con banderas consistiendo en un patrón de bit especial. Ocurrencias de este patrón de bits en los datos a ser transmitidos son eliminadas por la inserción de un bit. Para usar el ejemplo donde la bandera es 01111110, un 0 es insertado después de 5 unos consecutivos en la trama de datos. Las banderas y los 0s insertados son removidos al final del receptor. Esto aplica para tramas de longitudes arbitrarias y facilita la sincronización con el receptor. Debe mencionarse que este bit de relleno es añadido incluso si el siguiente carácter de dato es 0, lo cual no puede generar error para una secuencia sincronizada, de tal forma que el receptor puede sin ambigüedad distinguir los bits de relleno de los bits normales.

2.2.2.2.2 Servicios capa de enlace de datos

A continuación se presenta una lista de los servicios que puede brindar la capa de enlace de datos y de sus subcapas:

- Encapsulamiento de paquetes provenientes de la capa de red en tramas.
- Sincronización de tramas

2.2.2.2.2.1 Servicios de subcapa de control lógico:

2.2.2.2.2.1.1 Control de errores

Esta función permite el reenvío automático de solicitudes (ARQ), además del ARQ proveído por protocolos de capa de transporte, técnicas de corrección de posibles errores – Forward Error Correction (FEC) brindadas por la capa física, la detección de error y cancelación de paquetes que pueden realizar todas las otras capas. El control de errores de la capa de enlace de datos es utilizado en redes inalámbricas y redes de modem telefónicas como V.42, pero no es protocolos de redes LAN tal como Ethernet, desde que los errores

de bits se han vuelto poco comunes en líneas cortas. En este caso, solo la detección de errores y cancelación de paquetes erróneos o dañados son brindados. (CISCO, 2008)

Para asegurar una entrega confiable de paquetes de datos es necesaria la retroalimentación de información al emisor sobre la recepción de los paquetes. Como parte del protocolo, el receptor debe enviar tramas de control especiales confirmando la recepción positiva o negativa del paquete. Si al transmisor llega una trama con recepción negativa, deberá retransmitir la trama.

Estas fallas pueden darse en algunos casos debido a problemas en el hardware y que estos causen la desaparición de una trama completa. En estos casos el receptor no recibe la trama fallada simplemente un espacio de tiempo vacío. Por lo tanto, no abra una confirmación de recepción positiva o negativa. Surge en este punto la necesidad de la existencia de temporizadores en los extremos.

En el momento que el emisor envía la trama, este inicia un temporizador que establece un tiempo límite para la recepción de la trama de confirmación. Si el temporizador llega a su límite la trama vuelve a ser enviada.

Puede que en algunos casos la trama de confirmación se pierda y no llegue al emisor por lo tanto la trama será enviada nuevamente. A fin de evitar conflictos en el receptor, cada trama posee un número de secuencia para identificarle. Si al receptor llega una trama repetida este envía un mensaje especial al emisor notificado o solicitando la siguiente trama en la secuencia.

2.2.2.2.1.2 Control de flujo

En algunas ocasiones puede que el emisor envíe más datos de los que el receptor puede recibir debido a la velocidad que se tiene en la red. Por ejemplo, un emisor tiene una velocidad de transmisión superior a la velocidad de bajada que tiene un receptor. Esto quiere decir que abra un cuello de botella en la entrada a la red del receptor, lo que puede generar pérdidas de tramas.

Para evitar esta situación se utilizan dos métodos. El control de flujo que se basa en retroalimentación. En este método, el receptor regresa información al emisor autorizándolo para enviar más datos o indicándole el estado de recepción.

El segundo método es el control de flujo basado en tasa, en este caso el protocolo se encarga de limitar la tasa de transferencia a la que el emisor envía los datos, sin recurrir a retroalimentación por parte del receptor.

2.2.2.2.2 Servicios de subcapa de control de acceso al medio:

- Implementa protocolos de acceso múltiple para el control de acceso a canales, por ejemplo el protocolo CSMA/CD para detección de colisiones y retransmisión de

datos en red de bus de Ethernet y redes con concentradores, o el protocolo CSMA/CA para evitar colisiones in redes inalámbricas.

- Direccionamiento físico (direccionamiento MAC)
- Conmutación en la red LAN incluyendo el filtrado MAC.
- Calendarización de envío de paquetes de datos.
- Almacenamiento y envío por conmutadores o envío fragmento a través de conmutadores
- Control de calidad de servicios (QoS)
- Creación de Redes LAN virtuales (VLAN)

2.2.2.2.3 Métodos de control de acceso al medio

2.2.2.2.3.1 Acceso múltiple por detección de portadora.

Es un protocolo de control de acceso al medio probabilístico en el cual un nodo verifica la presencia de tráfico en la línea antes de transmitir en un medio compartido, tal como puede ser un bus eléctrico, o una banda de espectro electromagnético.

La detección de portadora describe el hecho que un transmisor utilice retroalimentación de un receptor que detecta una señal portadora antes de tratar de enviar los datos. Esto quiere decir, que el host trata de detectar la presencia de una señal codificada proveniente de otra estación. Si la portadora o señal de otro host es detectado, la estación deberá esperar para que la transmisión en progreso termine antes que iniciar su propia transmisión.

El termino acceso múltiple describe que muchas estaciones envían y reciben datos en un mismo medio. Las transmisiones por un nodo son generalmente recibidas por todas las otras estaciones de trabajo que comparten el medio.

2.2.2.3 Capa de red

La capa de red es la responsable del direccionamiento de mensajes y la “interpretación” de las direcciones lógicas a físicos. Es decir, este nivel se encarga de la transferencia de información entre sistemas finales a través de las redes de comunicación. Por lo tanto, los protocolos implementados en este nivel determinan la ruta que el paquete debe seguir desde la computadora emisora hasta la computadora receptora, en dependencia de las condiciones de la red.

Los computadoras hacen uso de los servicios de esta capa para establecer el dialogo con los dispositivos de red de forma que se puedan conocer las direcciones de posibles destinos para solicitar servicios. En el caso de una topología punto a punto, la capa de red se vuelve innecesaria en cuanto al direccionamiento de datos.

Esta capa es también la encargada de ensamblar los pequeños paquetes que se reciben y que forman parte de un gran mensaje, así como el envío de un gran mensaje en pequeñas partes o paquetes. A este proceso se le conoce como segmentación y reensamblaje. Es en esta parte cuando se le agrega a cada paquete un dato de ruteo en la red y control de errores.

Para diseñar las características de esta capa se deben tomar en cuenta algunos factores como (GS Comunicaciones, 1999):

- Los servicios deben ser independientes de la tecnología empleada en la red de datos.
- El nivel de transporte debe ser indiferente al número, tipo y topologías de las redes utilizadas.
- La numeración de la red debe ser uniforme a través de LANs y WANs.

2.2.2.4 Capa de transporte

A esta capa se le conoce comúnmente como nivel de host to host o el nivel de end to end, debido a que en él se establecen los protocolos que establecen, mantienen y terminan las conexiones virtuales o lógicas para la transferencia de información entre usuarios.

Este nivel se caracteriza por los beneficios de end to end, como las direcciones de red, el establecimiento de circuitos virtuales y los procedimientos de entrada y salida a la red. Este nivel es imperceptible desde el punto de vista de usuario y solamente desde la capa superior es cuando se vuelven visibles los beneficios.

Entre las funciones de la capa de transporte están (GS Comunicaciones, 1999):

- Especificar los mensajes de *broadcast*.
- El formato de los tipos de datagramas.
- El funcionamiento correcto de los servicios de correo electrónico.
- Las prioridades de los mensajes que transmiten en internet.
- La recolección de la información y su administración.
- Implementación de funciones de seguridad para la red.
- Definir los tiempos de respuesta de ACK.
- Implementación de estrategias de recuperación en casos de falla y segmentación de la información cuando el tamaño es mayor al máximo del paquete según el protocolo utilizado.

2.2.2.5 *Capa de sesión*

Esta capa es la encargada de manejar todo el dialogo entre computadores pues permite que varias aplicaciones puedan establecer, usar y terminar una conexión llamada “sesión”. Los protocolos implementados en esta capa son reglas para iniciar o terminar la comunicación entre dispositivos. A su vez, se encarga de brindar servicios de recuperación de errores si la comunicación falla. Parte de estos servicios es la retransmisión de información para completar el proceso de la comunicación.

Entre las funciones de esta capa está el reconocimiento de nombre para el caso de seguridad relacionado a aplicaciones que requieren comunicarse a través de la red. Otras de las funciones de la capa de red son (GS Comunicaciones, 1999):

- ▶ Establecimiento de la conexión a petición del usuario.
- ▶ Liberación de la conexión cuando la transferencia termina.
- ▶ Intercambio de datos en ambos sentidos.
- ▶ Sincronización y mantenimiento de la sesión para proporcionar un intercambio ordenado de los datos entre las entidades de presentación.

Como ejemplo de las funciones de esta capa es la administración de los token de red, que se implementa en una red tipo anillo. El nivel es encargado de decidir quien posee el token y la sincronización de la red.

Las conexiones consisten en los servicios de peticiones y servicios de respuestas que ocurren entre las distintas aplicaciones colocadas en los dispositivos de red. Estas respuestas y peticiones son coordinadas por protocolos implementados en la capa de sesión. Como ejemplo tenemos el protocolo de información de zona (ZIP), protocolo AppleTalk que coordina el proceso de vinculación de nombres; y el protocolo de control de sesión (SCP)

2.2.2.6 *Capa de presentación*

Los protocolos en este nivel definen el formato en que la información será intercambiada entre aplicaciones, así como la sintaxis empleada entre las mismas. Otras de las funciones son la traducción o conversión de la información recibida del formato empleado en la capa superior a otro intermedio que sea reconocido por la capa inferior o de sesión. Este proceso se revierte en la computadora receptora y la capa de presentación convierte la información para que la capa de aplicación pueda usarla.

Los servicios de encriptación y desencriptación de datos son brindados por esta capa, también las reglas de transferencia de información y la comprensión de datos para reducir el número de bits que necesitan ser transmitidos.

La capa maneja la presentación de la información de forma ordenada y significativa. La función principal de esta capa es la sintaxis y semántica de la transmisión de datos. Esta convierte la representación de los datos de las computadoras dentro de una red local a un formato estándar de red para transmisión sobre la red. En el lado del receptor, este formato de se cambia del formato estándar a el formato adecuado del para host, de tal forma que los datos pueden ser utilizados de forma independiente del host. Las conversiones, criptografía y procesos similares de estándares ASCII y EBCDIC son manejados en esta parte.

A su vez, provee de una variedad de funciones de codificación y conversión que son aplicados a la capa de aplicación. Estas funciones aseguran que la información enviada desde la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro sistema. Algunos ejemplos de los escenarios de conversión y codificación incluyen formatos de representación de datos comunes, conversiones de caracteres en formatos de representación u compresión de datos.

Los formatos de representación de datos, o el uso de imágenes estándar, sonido, y formatos de video, habilitan el intercambio de datos de aplicación entre los diferentes tipos de sistemas de computadoras. Usando diferentes representaciones de texto y datos, como EBCDIC y ASCII se logra el intercambio de información entre sistemas.

Las implementaciones de esta capa no son asociadas normalmente con una pila de protocolos particular. Algunos estándares bien conocidos para video son QuickTime y Motion Picture Experts Group (MPEG). Entre los formatos de imagen tenemos: Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), y Tagged File Format (TIFF). GIF es una estándar para compresión y codificación grafica de imágenes al igual que JPEG. TIFF permite la codificación de imágenes.

2.2.2.7 Capa de aplicación

Este es el nivel más alto del modelo OSI, sirve como medio para que los procesos del ordenador accedan al entorno OSI, es decir hagan uso de las otras capas del modelo. Proporciona los procedimientos que permiten a los usuarios ejecutar los comandos relativos a sus propias aplicaciones.

Existen 3 tipos de procesos fundamentales que se llevan a cabo en la capa de aplicación:

- 1) Procesos propios del sistema
- 2) Procesos de gestión
- 3) Procesos de aplicación del usuario.

La capa de aplicación del modelo OSI es la capa más cercana al usuario final, lo que significa que tanto el usuario y la capa interactúan directamente con el software utilizado. Esta capa interactúa con las aplicaciones de software que implementan el componente de comunicación. Tales programas no forman parte de modelo OSI. Las funciones de este nivel incluyen la identificación de parejas en la comunicación, determinar si los recursos están disponibles, y sincronizar la comunicación. Cuando se han identificado las parejas de comunicación, la capa de aplicación determina la identidad y disponibilidad en las partes involucradas de una aplicación para transmitir datos. Una vez que se ha determinado que el recurso está disponible, los servicios de la capa deben decidir si existe suficiente recurso de red para que exista la petición de comunicación. En la sincronización de comunicación, toda la comunicación entre aplicaciones requiere de cooperación que manejada por la capa de aplicación.

A continuación, se presenta una lista de protocolos que se implementan en esta capa:

1. SMTP- simple mail transfer protocol
2. GMTP- Group mail transfer protocol
3. FTP- File Transfer Protocol
4. TFTP- Trivial File Transfer Protocol

2.2.3 Funcionamiento del modelo OSI

El modelo OSI como se había mencionado anteriormente pasee 7 capas y cada una de ellas realizan funciones específicas. (Ver Figura. 2-4)

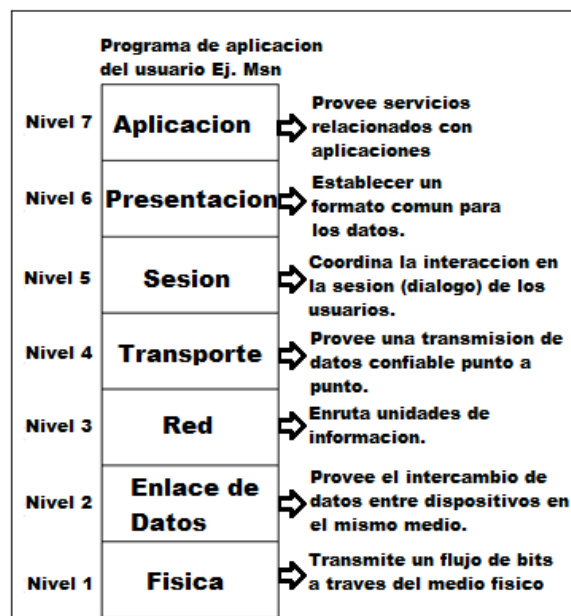


Figura. 2-4 Funciones de las capas OSI.

Cuando se realiza la transmisión o comunicación entre dos dispositivos el usuario necesita de una interfaz de acceso a la red, es aquí donde se inició el proceso de comunicación. El usuario utiliza un programa o aplicación. Supongamos que dos personas deciden utilizar Messenger, en cada ordenador se debe estar ejecutando dicho programa. A estas aplicaciones se les llamara msn1 y msn2 (Ver Figura. 2-5).

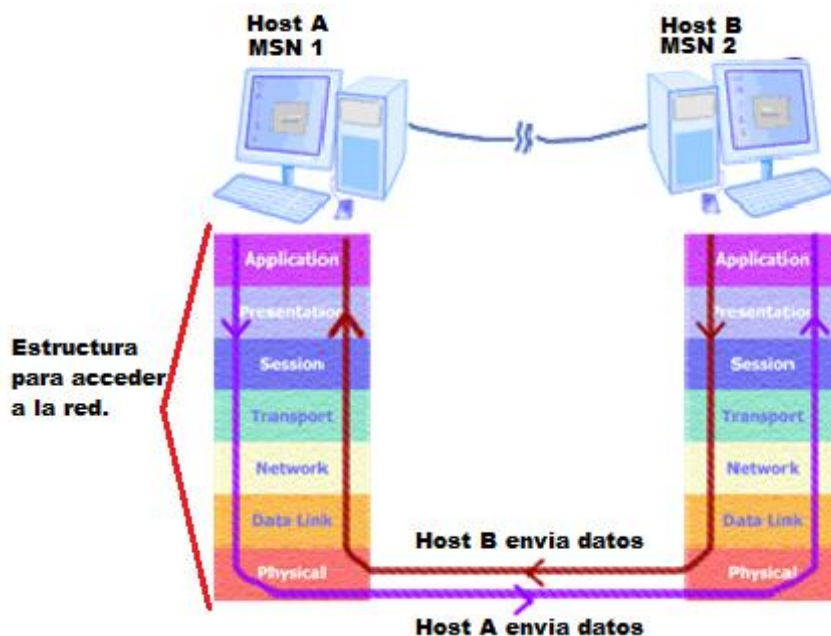


Figura. 2-5 Datos enviados y recibidos atraviesan las capas del modelo OSI.

Si el msn1 decide enviar un mensaje a msn2, el msn1 debe utilizar los servicios de la capa de aplicación (capa 7). Esta capa se encarga de establecer una relación paritaria con la capa 7 del ordenador que ejecuta msn2. Pero igual necesita de los servicios de capa de sesión (capa 6) y ambos ordenadores deben usar los mismos protocolos de esta capa. Cada ordenador debe usar los mismos protocolos en cada una de las 7 capas para que la comunicación sea exitosa.

A medida que la información desciende por cada una de las capas del modelo los datos se encapsulan para luego ser enviados por los medios (Ver Figura. 2-6). Cuando los datos se generan que crea una unidad de datos a la cual se le coloca un encabezado de capa de aplicación. Esta unión se convierte en la unidad de datos que recibe la siguiente capa inferior, que posteriormente agrega su encabezado de presentación. La nueva unidad de datos ahora contiene los encabezados de aplicación y presentación.

La siguiente capa es la capa de sesión que asume que los encabezados de aplicación y presentación forman parte de los datos del usuario, por lo tanto no genera ningún conflicto y agrega su encabezado de sesión (Ver Figura. 2-5). La capa de transporte recibe los datos y encabezados como un solo paquete al que debe encapsular y agregar su

encabezado para luego enviarlo a la capa de red, para que esta agregue su encabezado de red²⁸.

La capa de enlace de datos recibe los paquetes y coloca su encabezado y un tráiler. Finalmente los datos llegan a la capa 1 en donde son transmitidos en el medio de comunicación. Los paquetes y encapsulamientos se interpretan como tramas de bits sucesivos.

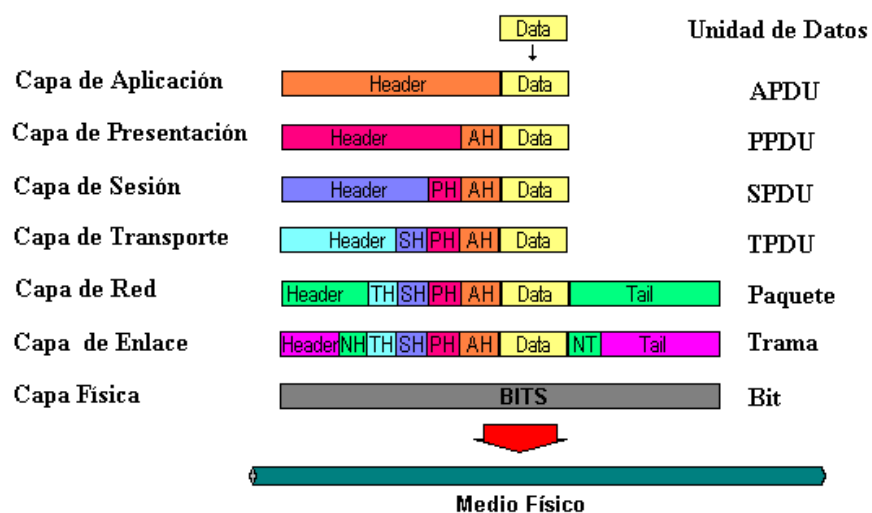


Figura. 2-6 Datos se encapsulan y encabezados se agregan al cruzar las capas OSI.

2.2.3.1 Des-encapsulamiento de datos.

Es el proceso inverso, cuando un dispositivo recibe el chorro de bits, la capa física del dispositivo remoto los pasa a la capa de enlace de datos para su manipulación.

Primero se revisa el trailer de la capa de enlace de datos (FCS) para ver si los datos están no contienen errores. Si los datos están errados, pueden ser descartados, y la capa de enlace de datos puede pedir la retransmisión.

Si no hay ningún error, la capa de enlace de datos lee e interpreta la información de control en el encabezado y remueve el encabezado y trailer y pasa lo que queda hacia la capa superior basada en la información de control del encabezado. Así mismo las capas superiores leen los encabezados correspondientes a sus capas y lo remueven para pasarlo a la capa superior inmediata.

²⁸ Algunos protocolos de capa de red adjuntan un tráiler luego de la unidad de datos proveniente de la capa de transporte.

2.2.4 Normalización en el modelo OSI

A continuación, desarrollaremos el aspecto de normalización en OSI refiriéndonos a esta como el establecimiento de normas para cada capa. El modelo define de forma clara las funciones correspondientes a los niveles, por lo que el proceso resulta mucho más sencillo.

Las funciones se dividen a lo largo de las capas, de tal forma que es fácil definir los protocolos de cada que cada una de estas contiene. Están lo suficientemente delimitadas como para elaborarlos de manera individual.

Por el mismo hecho de que las capas están muy bien delimitadas, los cambios que se realizan en los estándares de una capa no afectan el software de otras. Esto facilita la implementación de nuevos protocolos. Para realizar el proceso de normalización existen 3 elementos claves (Stallings, 2004):

Especificación de protocolos: dos entidades en la misma capa en sistemas diferentes cooperan e interactúan por medio del protocolo. El protocolo se debe especificar con precisión, ya que están implicados dos sistemas abiertos diferentes. Esto incluye el formato de la unidad de datos del protocolo, la semántica de todos los campos, así como la secuencia permitida de PDU.

Definición del servicio: Además del protocolo o protocolos que operan en una capa dada, se necesitan normalizaciones para los servicios que cada capa ofrece a la capa inmediatamente superior. Normalmente, la definición de los servicios es equivalente a una descripción funcional que definiera los servicios proporcionados, pero sin especificar cómo se están proporcionando.

Direccionamiento: Cada capa suministra servicios a las entidades de la capa inmediatamente superior. Estas entidades se identifican mediante un punto de acceso al servicio. Así, NSAP^{29xviii} identifica a una entidad de transporte usuaria del servicio de red (Ver Figura. 2-7).

²⁹ NSAP = Network Service Access Point – Punto de Acceso de Servicio de Red.

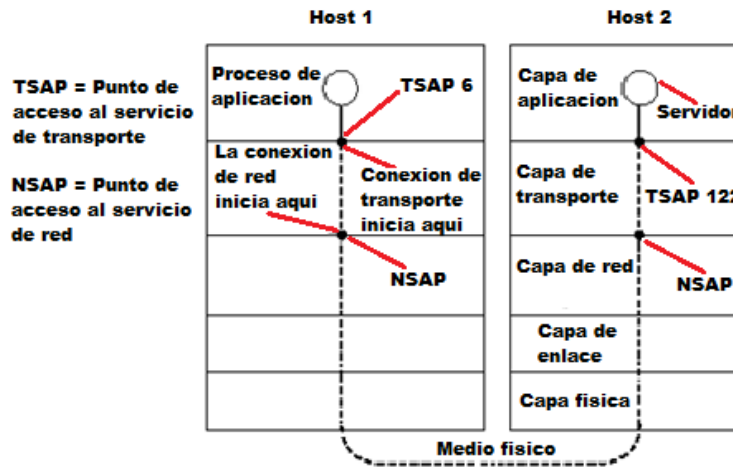


Figura. 2-7 Direccionamiento de datos entre capas del modelo OSI.

2.2.5 Parámetros y primitivas de servicio.

Los servicios que se implementan entre capas adyacentes en la arquitectura OSI se describen en términos de primitivas y mediante parámetros involucrados. Una primitiva define la función que se va a llevar a cabo y los parámetros necesarios para transmitir datos e información de control.

En el proceso de interacción entre las capas adyacentes la arquitectura utiliza 4 tipos de primitivas que son: solicitud, indicación, respuesta y confirmación (Ver Figura. 2-8).

A continuación presentamos las definiciones respectivas a cada primitiva obtenidas de (Stallings, 2004).

Solicitud: Primitiva emitida por el usuario del servicio para invocar algún servicio y pasar los parámetros necesarios para especificar completamente el servicio solicitado.

Indicación: Primitiva emitida por el proveedor del servicio para:

1. Indicar que ha sido invocado un procedimiento por el usuario de servicio par en la conexión y para suministrar los parámetros asociados.
2. Notificar al usuario del servicio una acción iniciada por el suministrador.

Respuesta: Primitiva emitida por el usuario del servicio para confirmar o completar algún procedimiento invocado previamente mediante una indicación a ese usuario.

Confirmación: Primitiva emitida por el proveedor del servicio para confirmar o completar algún procedimiento invocado previamente mediante una solicitud por parte del usuario del servicio.

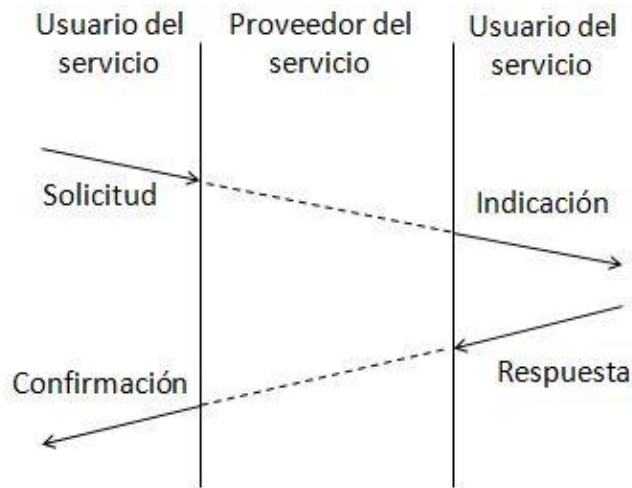


Figura. 2-8 Proceso de ejecución de primitivas.

2.3 Modelo TCP/IP

2.3.1 ¿Qué es TCP/IP?

El modelo TCP/IP (Ver Figura. 2-9 un modelo de aplicación para el diseño de protocolos de red de computadoras y para llevar a cabo la comunicación sobre el internet. Este modelo abstracto tiene una arquitectura de red basada en un sistema compuesto por capas tal como el modelo OSI.

En la primera capa del modelo es denominada capa de aplicación donde operan algunos protocolos como SMTP, FTP, SSH y HTTP.

En el nivel 2 de orden descendente se encuentra la capa de transporte donde se realiza conexión por protocolos tal como TCP. De igual forma, otros protocolos como UDP, DCCP, GTP y SCTP son implementados. Esta capa permite iniciar y mantener conexiones. Entre las funciones de esta capa está el asegurar que los mensajes de cada paquete son recibidos apropiadamente.

Luego está la capa de internet o capa 3, la cual define el sistema de direccionamiento IP y los escenarios de enrutamiento para que los paquetes puedan “navegar” de una dirección IP a otra. Algunos ejemplos de protocolos implementados en la capa de internet son IPv4, IPv6, ICMP e IGMP.



Figura. 2-9 Modelo TCP/IP

La capa de acceso a la red es la cuarta capa de este modelo, en ella se contienen los protocolos de bajo nivel usados para señalización y comunicación de datos. Ejemplos de estos protocolos son PPP, FDI, Frame Relay, ATM y GRPS.

Finalmente en el nivel más bajo se encuentra la capa física, la cual está constituida del equipo físico necesario para la comunicación, tal como el par de cobre trenzado, equipo y sistemas para la señalización en la línea como Ethernet, SONET/SDH, ISDN y Modems

2.3.2 TCP/IP en el mundo

TCP/IP consiste en una serie de protocolos diferentes, pero solamente algunos de ellos definen verdaderamente la operación principal de toda la suite. De todos los protocolos claves o fundamentales solamente 2 son considerados cruciales o indispensables en todos los sentidos. Estos son el protocolo de internet (IP), siendo este un protocolo que opera en la capa 3 del modelo OSI permitiendo el direccionamiento, ruteo de datagramas y otras funciones en la red. El protocolo de control de transmisión (TCP) es el protocolo de principal funcionamiento en cuanto a transporte, y es el responsable del establecimiento de la conexión, administración y verdadero transporte de datos entre los procesos de dispositivos (CISCO, 2008).

Debido a la importancia de estos 2 protocolos, sus abreviaciones representan una suite completa: TCP/IP. IP y TCP son importantes porque muchas de las funciones más críticas son implementadas en las capas 3 y 4. Sin embargo, hay mucho más que TCP/IP que solo TCP e IP. La suite de protocolos tiene un grupo de requerimientos para el funcionamiento de una variedad de protocolos y tecnologías para hacer que una red funcional brinde sus servicios a los usuarios y las aplicaciones que estos necesiten.

2.3.3 Factores importantes de TCP/IP

TCP/IP fue un tiempo solamente uno de muchos suite de protocolos que pudieron ser utilizados para proveer funcionalidades de una capa de red y capa de transporte. En la actualidad, todavía existen otras opciones de suite de protocolos para el funcionamiento de red, pero TCP/IP es el estándar en de la red mundial aceptado. Su gran popularidad ha sido debido a un número de factores importante. Algunos de estos son (CISCO, 2008):

Sistema de direccionamiento integrado: TCP/IP incluye un sistema para la identificación y direccionamiento a dispositivo tanto para redes pequeñas como grandes. El sistema de direccionamiento está diseñado para permitir a los dispositivos que se les asigne una dirección independientemente de bajo nivel de detalle de cómo cada red es construida. Con el tiempo, estos mecanismos de direccionamiento en TCP/IP han sido mejorados, para satisfacer las necesidades de las crecientes redes como Internet. El sistema de direccionamiento también incluye la capacidad de administración centralizada para el Internet, de tal forma se puede asegurar que cada dispositivo tiene una dirección única.

Diseñado para el enrutamiento: A diferencia de algunos protocolos de capa de red, TCP/IP está especialmente diseñado para facilitar el enrutamiento de información sobre una red de complejidad arbitraria. De hecho, TCP/IP se enfoca más en conexiones de red, que en conexiones físicas de dispositivos. Los routers de este modelo permiten a los datos el ser entregados a dispositivos de diferentes redes, pasando los datos uno a la vez a la siguiente red en el camino hasta la red final. Un número de protocolos de soporte esta también incluidos en TCP/IP para permitir a los routers el intercambio de información crítica y administración del flujo de información de forma eficiente de una red a otra.

Escalabilidad: Una de las características más sorprendentes de TCP/IP es la escalabilidad que sus protocolos han demostrado tener. Como prueba de esto es él como el Internet ha avanzado desde implementado unas pocas maquinas hasta millones alrededor del mundo. Mientras que algunos cambios han sido necesarios periódicamente para apoyar este crecimiento, estos cambios han tenido lugar en el marco del TCP/IP proceso de desarrollo, y el núcleo de TCP/IP es básicamente el mismo que era hace 25 años.

Estándar y proceso de desarrollo abierto: Los estándares de TCP/IP no son propietarios, pero son estándares abiertos y de fácil acceso al público. Además, el proceso usado para el desarrollo de TCP/IP es completamente abierto. Los protocolos de TCP/IP son desarrollados y modificados usando el único proceso democrático RFC. Esto asegura que cualquier persona con un interés en los protocolos TCP/IP tenga la oportunidad de aportar en su desarrollo, y también asegura la aceptación mundial de la suite de protocolos.

2.4 Preguntas de control.

1. ¿Qué es el modelo OSI? ¿Cuáles son sus capas?
2. ¿Cuáles son las ventajas de un modelo de referencia en capas?
3. Explique cómo se realiza el proceso de envío de datos entre dos host a través de OSI?
4. ¿Cuáles son los parámetros y primitivas de servicio? ¿Cómo interactúan?
5. ¿Cuáles son las subcapas de la capa de enlace? Explique brevemente la función de cada una.
6. ¿Cuáles son los servicios de la capa de enlace de datos?
7. ¿Cómo se realiza el control de errores en la capa 2?
8. ¿Qué es CSMA?
9. ¿Cuál es la función de la capa de red?
10. ¿Cuál es la función de la capa de transporte?
11. ¿Qué es la capa de sesión? ¿Cuáles son sus funciones?
12. ¿Qué función realiza la capa de presentación?
13. ¿Para qué sirve la capa de aplicación?
14. ¿Cuáles son los elementos clave de la normalización? Explique cada uno de ellos.
15. ¿Qué es el modelo TCP/IP?
16. Explique brevemente los factores que le han permitido al modelo TCP/IP ser el modelo de mayor aceptación mundial.
17. ¿Cuáles son las capas del modelo TCP/IP?

Unidad III

Protocolos del modelo TCP/IP

Objetivos General:

- Desarrollar contenido referente a tecnologías contenidas en las capas del modelo TCP/IP.

Objetivos Específicos:

- Señalar los estándares V.24 y Ethernet.
 - Mencionar las tecnologías más usadas de la capa de enlace
 - Identificar los protocolos y algoritmos de enrutamiento de capa de red.
 - Determinar el uso de los protocolo TCP, UDP y RTP.
 - Decir las funciones y servicios implementados en la capa de aplicación.
-

Unidad 3. Protocolos del modelo TCP/IP

3.1 Capas del modelo TCP/IP

El modelo de aplicación de TCP/IP basa su estructura de funcionamiento en 5 capas, siendo estas (GS Comunicaciones, 1999):

- Capa de aplicación
- Capa de transporte
- Capa Internet
- Capa de acceso a la red
- Capa física

La Figura. 3-1 muestra la pila de capas TCP/IP y algunos ejemplos de protocolos asociados a cada uno de sus niveles.



Figura. 3-1 Capas de TCP/ IP y protocolos asociados.

3.1.1 Capa Física

3.1.1.1 NIC

Todo dispositivo de red ya sea un ordenador o servidor necesita de una tarjeta de interfaz de red o bien conocida por sus siglas NIC³⁰. Esta tarjeta o adaptador puede utilizarse en cualquier topología a la que se desea incorporar el host.

El adaptador debe cumplir con los protocolos adecuados para evitar conflictos con el resto de nodos o con otros dispositivos conectados a la computadora como un monitor, mouse, etc.

³⁰ NIC = Network Interface Card



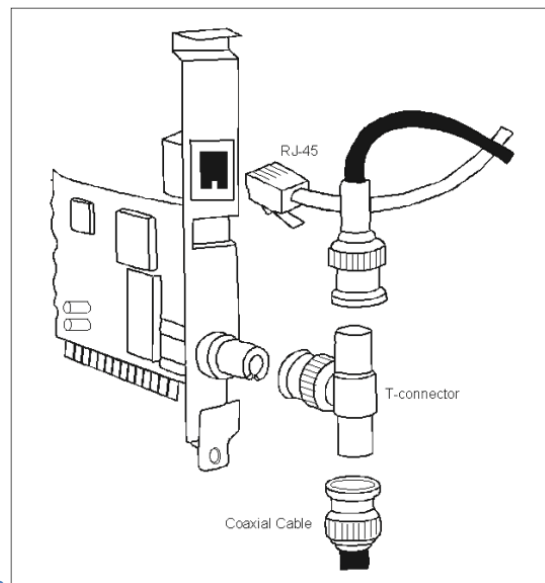
Figura. 3-2 Tarjeta de red para conexiones inalámbricas.

La Figura. 3-2 muestra una tarjeta de interfaz para una red inalámbrica. Se observa en la parte inferior de la tarjeta la conexión de ranura(slot) para puerto PCI.

Esta tarjeta debe cumplir con las requerimientos para el estándar 802.11 que se desea implementar

En otros casos (Ver Figura. 3-3), se tiene una NIC para conectarse a la red a través de un medio alambrado (cable UTP). El tipo de conector que se requiere es un RJ 45.

La imagen también nos muestra que algunas tarjetas permiten la conexión de cables coaxiales utilizando un conector tipo T.



y Coa

xial.

En la Figura. 3-4 se muestran otros conectores que se pueden ocupar junto con los *host* a los que se les puede asociar.

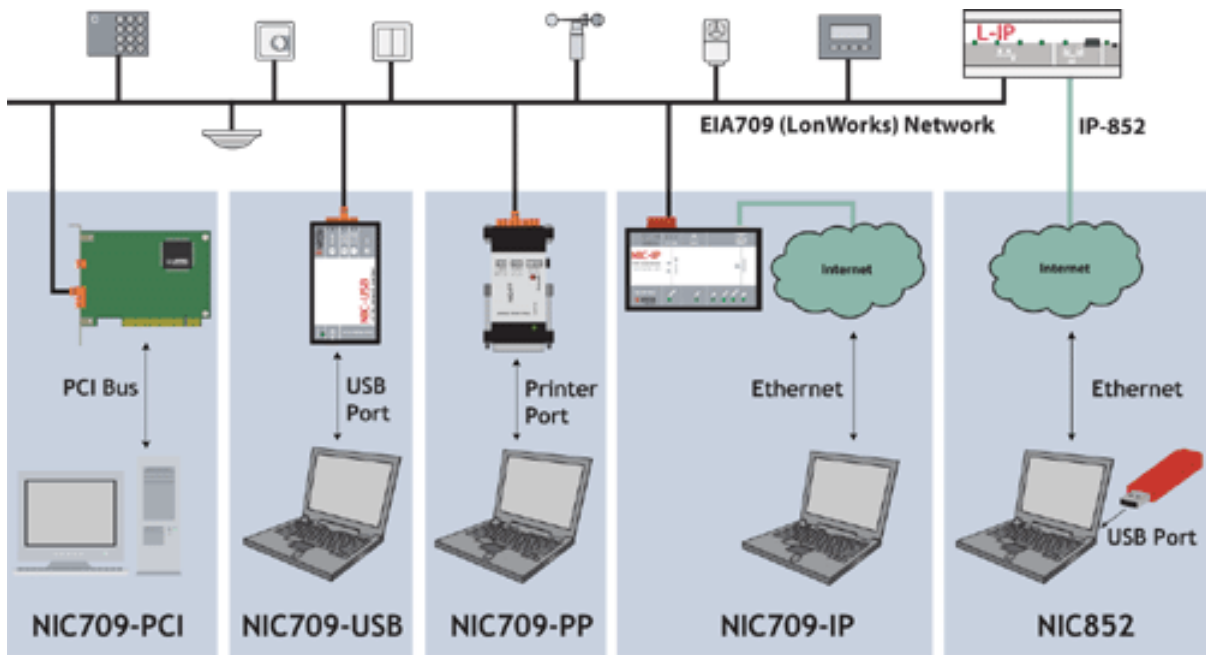


Figura. 3-4 Tipos de conectores para acceder a la red.

<p>Los requisitos mínimos que debe cumplir una NIC para su funcionamiento son (GS Comunicaciones, 1999):</p> <ol style="list-style-type: none"> 1. Debe utilizar los protocolos adecuados según el tipo de red que se desea implementar. 2. Tener el conector adecuado para adaptarse a la ranura de expansión o puerto disponible en el equipo.
--

3.1.1.2 Estándar V.24

En este segmento nos enfocaremos en uno de los estándares de capa física más comunes como es el V.24 o también conocido como RS232.

El estándar V.24 es una especificación para comunicación de terminales únicas. Es decir conexiones únicas entre dispositivos, que incluye la definición del conector y la ubicación de los pines. Este estándar puede emplearse junto con el V.28 para definir una especificación serial asincrónico o comunicaciones sincrónicas.

Por otro lado el V.28 es un estándar que al igual que el V.24 se utiliza en comunicación de terminales únicas y a su vez define las características de las señales

eléctricas que utiliza. El estándar RS232C es esencialmente equivalente a combinar el V.24 y V.28. Debe mencionarse que los estándares de EIA han reemplazado de manera efectiva los estándares RS.

3.1.1.2.1.1 Característica de la Interfaz

Típicamente la interfaz está limitada a una velocidad máxima de transmisión de 115Kbps. La distancia máxima a la que se puede implementar una comunicación con este estándar es de 6m, el rendimiento actual depende mayoritariamente en las especificaciones del cable. Algunos ejemplos de esta interfaz tienen un mayor rendimiento. Los avances tecnológicos le permiten a la interfaz el integrar circuitos para el soporte de tasa de transferencias de bits que exceden los 230Kbps (FarSite Communications, 2010). En modo síncrono, tanto el reloj del transmisor como del receptor son usados para transmitir datos.

3.1.1.2.1.2 Aplicaciones de la Interfaz.

Una de las aplicaciones más comunes para el interfaz V.24 es para ubicación de puertos COM y conexión en puertos seriales de una gran variedad de dispositivos periféricos. Estas implementaciones usan el modo de comunicación asincrónico³¹.

V.24 es también usado para la operación de interfaces en modo síncrono, por ejemplo para conectar un modem síncrono de una línea arrendada a un adaptador de comunicaciones síncronas instalado en un sistema de computadora. Usualmente los protocolos usados en interfaces sincrónicas V.24 son HDLC, X.25, SNA y PPP. (FarSite Communications, 2010)

3.1.1.2.1.3 Pines y tipos de conectores de la interfaz

El conector DB25 es usado para los tipos de conexión síncronos y asíncronos. Muchas de las señales son definidas en el estándar. A continuación se presenta una imagen con las especificaciones de este.

³¹ ASYNC= Asynchronous mode of communications – Modo de comunicación Asíncrono.

DB25 Connector Pinouts		
Signal Name	DB25 Contact No	Supported on FarSync Cards
Shield	1	Yes
TD	2	Yes
RD	3	Yes
RTS	4	Yes
CTS	5	Yes
DSR	6	
Signal Ground	7	Yes
DCD	8	Yes
+ VOLTAGE	9	
- VOLTAGE	10	
Unassigned	11	
Secondary DCD	12	
Secondary CTS	13	
Secondary TD	14	
Transmitter Signal Element Timing (clock line)	15	Yes
Secondary RD	16	
Receiver Signal Element Timing (clock line)	17	Yes
Local Loopback	18	
Secondary RTS	19	
DTR	20	Yes
Remote Loopback	21	
RI	22	
Data Signal Rate Selector	23	
Transmit Signal Element Timing	24	
Test Mode	25	

Figura. 3-5 Configuración de pines en un conector DB25

El conector DB9 es usado únicamente para conexiones asincrónicas, tales como las utilizadas en puertos COM de las PCs. La configuración de los pines para este tipo de conector se muestra en la Figura. 3-6

DB9 Connector Pinouts		
Signal Name	DB9 Contact	Supported on FarSync cards
DCD	1	Yes
RD	2	Yes
TD	3	Yes
DTR	4	Yes
Signal Ground	5	Yes
DSR	6	
RTS	7	Yes
CTS	8	Yes
RI	9	

Figura. 3-6 Configuración de pines en un conector DB9

3.1.1.3 Estándar Ethernet

La capa física Ethernet incluye una serie de interfaces físicas y una gran variedad de velocidades de transmisión. Los rangos de velocidades de 1Mbit/s a 100Gbit/s son característicos junto con los medios físicos que pueden operar en estos rangos como cables coaxiales, par trenzados de cobre o fibra óptica. En general, la pila de protocolos de red y los softwares podrán trabajar de forma normal en todas estas variantes.






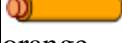


Ethernet posee una gran variedad de implementaciones. Cada una de estas implementaciones puede ser denominada en relación a la velocidad de transmisión con que operan. El estándar 10 Gigabit Ethernet se ha vuelto más popular en las redes Enterprise. Velocidades superiores a 40 y 100 Gbit/s han sido menos desarrolladas. Algunas empresas creen que las aplicaciones comerciales de estándares Ethernet que operen en términos de terabits posiblemente aparecerán cerca del 2015 (GS Comunicaciones, 1999).

Muchos de los adaptadores de Ethernet y puertos de switch soportan múltiples velocidades, usando auto negociación para establecer la velocidad y tipo de comunicación dúplex más adecuada para los dispositivos conectados. Si la auto negociación falla, un dispositivo que opere a múltiples velocidades escanea la velocidad usada por su contraparte o receptor en el otro extremo; pero este dispositivo asumirá una comunicación half- dúplex. Un puerto Ethernet 10/100 soporta 10BASE –T y 100BASE – TX. Un puerto Ethernet 10/100/1000 soporta velocidades de 10BASE – T, 100BASE – TX y 1000BASE – T. (Wikipedia - Ethernet, 2010)

3.1.1.3.1.1 Ethernet implementado en un cable de par trenzado.

Muchas variantes de Ethernet son específicamente diseñadas para funcionar sobre 4 pares de cobre. Este tipo de cable estructurado puede ser instalado sobre cualquier locación. ANSI recomienda usar cable UTP de una categoría de 6 para nuevas instalaciones. La Tabla 3-1 muestra la configuración o uso de cada una de las líneas contenidas dentro del cable UTP para distintos estándares de Ethernet.

Tabla 3-1

RJ-45 Wiring (TIA/EIA-568-B T568A)								
Pin	Pair	Color	telephone	10BASE-T	100BASE-TX	1000BASE-T	PoE mode A	PoE mode B
1	3	 white/green	-	TX+	z	bidirectional	48V out	-
2	3	 green	-	TX-	z	bidirectional	48V out	-
3	2	 white/orange	-	RX+	z	bidirectional	48V return	-
4	1	 blue	ring	-	-	bidirectional	-	48V out
5	1	 white/blue	tip	-	-	bidirectional	-	48V out
6	2	 orange	-	RX-	z	bidirectional	48V return	-
7	4	 white/brown	-	-	-	bidirectional	-	48V return
8	4	 brown	-	-	-	bidirectional	-	48V return

Combinando las versiones 10Base-T (o 100 BASE – TX) con “IEEE 802.3af en el modo A” se le puede permitir a un hub el transmitir la energía y dato a través de solamente 2 pares. Este sistema fue diseñado para las otros 2 pares libre para señales de telefonía analógica.

Los pines usados en la versión IEEE 802.3af en modo B proveen energía por medio de los pares “spare” no usados en las versiones 10BASE – T y 100BASE- TX (GS Comunicaciones, 1999).

A manera de avance sobre ambas tecnologías 10BASE-T y 100BASE-TX, el estándar 1000BASE-T utiliza los 4 pares de cables para transmisión simultánea en ambas dirección con el uso de eco cancelación. Es decir se permite la comunicación full – dúplex. Dial-up módems también usan eco cancelación para transmitir de forma simultánea datos en ambas direcciones sobre un par simple de cobre.

3.1.1.3.1.2 Ethernet longitudes mínimas de cables.

Todos los segmentos Ethernet de cobre que funcionan bajo la detección de colisiones que es una parte de CSMA/CD tienen una longitud mínima de cable para funcionar de manera apropiada debido a las reflexiones. Esto es aplicable solo a las versiones 10BASE-T y 100BASE-TX.

Las conexiones de fibra también tienen un mínimo en cuanto a la longitud del medio o cable debido a los requerimientos en los niveles de las señales recibidas. Los puertos de conexiones a medios de fibra diseñados para largas longitudes de ondas requieren un atenuador de señal si son usados dentro del mismo edificio.

La aplicación de Ethernet industrial utiliza topologías de estrellas sin colisiones por lo que la longitud mínima del cable no es requerida. El estándar 1000BASE-TX soporta una comunicación half-duplex haciendo las colisiones posibles. Consecuentemente, este estándar requiere una longitud mínima del cable para que la detección de colisiones funcione de forma apropiada. Para evitar este problema en el estándar Gigabit, pequeñas tramas son enviadas dentro de la transmisión en el modo half – dúplex.

3.1.1.4 Estándares relacionados

Algunos estándares de networking no son parte del IEEE 802.3 Ethernet sin embargo es necesario que esto puedan operar con Ethernet. Cuando nos referimos a operar significa que deben ser capaces de interpretar las tramas recibidas con un formato Ethernet y enviarle tramas a estos transmisores.

Algunos de estos estándares son (Wikipedia - Ethernet, 2010):

100Base-VG: Este es un contendiente temprano para el 100Mbit/s de Ethernet. Este puede operar en cable de categoría 3, utilizando 4 pares de cable. Pero este sistema se volvió un fracaso comercial.

TIA 100BASE-SX: Este estándar fue impulsado por Asociación de la industria de telecomunicaciones. 100BASE-SX es una implementación alternativa de 100Mbit/s sobre un medio de fibra. Esta versión es incompatible con el estándar oficial 100BASE-FX. La

principal característica de este sistema es la interoperabilidad con el estándar 10BASE-FL, con la funcionalidad de auto negociación entre operaciones 10Mbit/s y 100Mbit/s.

TIA 1000BASE-TX: Fue impulsado por la misma asociación que el estándar 100BASE-SX, es considerado un fracaso comercial, y no existen productos en el mercado. 1000BASE-TX utiliza protocolos simples al igual que el estándar oficial 1000BASE-T de tal forma que los dispositivos electrónicos son más baratos, pero requieren de un cableado de categoría 6.

G.hn: Este estándar fue desarrollado por la ITU-T y promocionado por el foro de HomeGrid para transmisión de alta velocidad (más de 1 Gbit/s) para redes de área local sobre infraestructuras cableadas ya existentes en los hogares como cables coaxiales, líneas de energía y líneas telefónicas. G.hn define una capa de protocolo de convergencia para aplicación que acepta tramas Ethernet y encapsula para un formato G.hn MSDU.

Estándares de networking que no usan tramas en el formato Ethernet pero que pueden todavía ser conectadas a Ethernet utilizando MAC basado en puentes son:

802.11: Este estándar para implementar redes de área local inalámbricas, usualmente son conectadas con un “backbone” de interfaz Ethernet.

802.16: Es un estándar que se utiliza en la creación de redes inalámbricas de área metropolitana, incluyendo Wimax.

10BaseS: Es el estándar de Ethernet pero funcionando sobre VDSL

3.1.2 Capa de acceso a la red

3.1.2.1 Direccionamiento de tramas.

Es muy importante conocer cómo funciona el direccionamiento de tramas, es por ello que en esta parte estudiaremos las partes de una unidad de datos de protocolo o bien PDU. Existen una gran variedad de protocolos en la capa de enlace de datos que es la capa 2 del modelo OSI. Esta capa es encargada de encapsular las PDU que se envía de las capas superiores y los elementos que sea agregan permiten el reconocimiento y direccionamiento de los datos a nivel de LAN.

Esta sección nos permitirá entender el funcionamiento y necesidad de cada uno de los elementos que se agregan en la capa de enlace de datos. Se valoran 3 secciones de forma general pues son las partes en común que poseen los protocolos de distintas marcas.

Esta capa del modelo tiene el objetivo de preparar el paquete de datos para los distintos medios. En la trama que se envía se agrega un segmento de control para evitar errores, pero este varía dependiendo del tipo de control de acceso al medio que se implementa y la topología lógica (CISCO, 2008). A continuación, desarrollaremos estas 2 partes: el encabezado y el tráiler de la PDU.

3.1.2.1.1 El encabezado.

Es el encargado de transportar la información de control de la trama que permite la transmisión correcta de esta a través de un medio. En esta parte de toda la trama la información enviada es única para el protocolo de capa 2 que se implementa y el medio en que se transmite la trama (CISCO, 2008).

La Tabla 3-2 muestra algunos de los parámetros que contiene la información de control del encabezado y la función en el entramado.

Tabla 3-2

<i>Campo</i>	<i>Función</i>
Inicio de trama	Indica el comienzo de la trama
Dirección de origen y destino	Indica los nodos de origen y destino en los medios
Prioridad/Calidad del Campo de servicio	Indica un tipo particular de servicio de comunicación para el procesamiento.
Tipo	Indica el servicio de la capa superior contenida en la trama
Control de conexión lógica	Utilizada para establecer la conexión lógica entre los nodos
Control de enlace físico	Utilizado para establecer el enlace a los medios
Control de flujo	Utilizado para establecer el enlace a los medios
Control de congestión	Indica la congestión en los medios

Obtenido de: (CISCO, 2008)

Los elementos de la trama que se muestran en la Figura. 3-7 son idénticos para todas las topologías de red. Este provee una interfaz general entre los diferentes protocolos IPX, TCP/IP y otros. Y a su vez, entre los diferentes tipos de red como Ethernet, Token Ring, etc. (ckp, 2006)

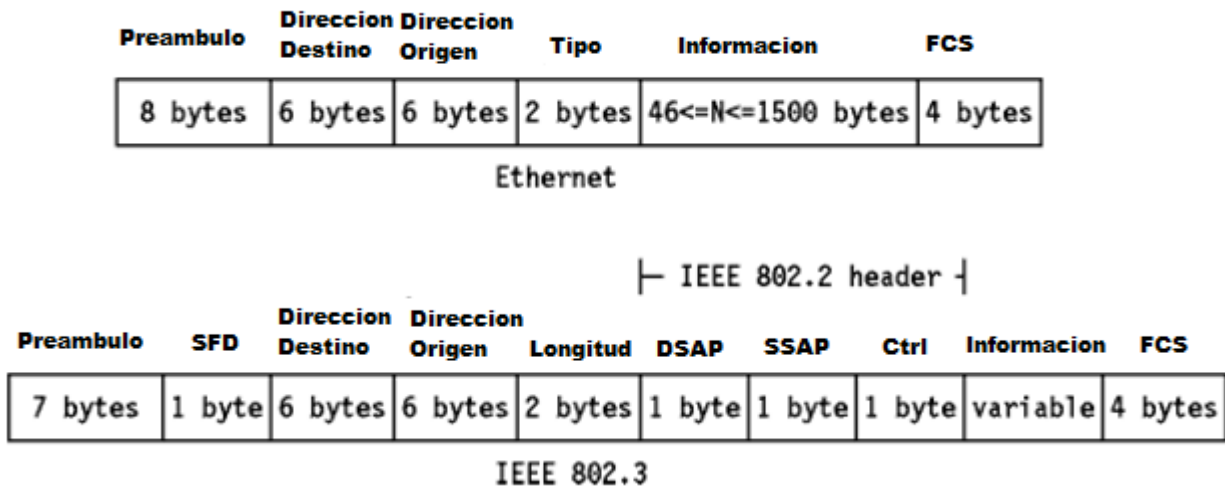


Figura. 3-7 Campos de trama del Estándar 802.2

Más información sobre esta capa se desarrolla en la siguiente unidad al tratar las subcapas LLC y MAC de la capa de enlace de datos.

3.1.2.1.2 El tráiler

Como parte del protocolo de capa de enlace se agrega a cada trama una última secuencia de datos denominada “tráiler” (Ver Figura. 3-8). La función principal es la detección de errores a través de un resumen lógico de los bits que comprenden la trama en el tráiler. La casilla de FCS³² o “Secuencia de verificación de trama” se compara con checksum³³ y adjuntado por el transmisor antes de enviar la trama. (CISCO, 2008)

El CRC o comprobación de redundancia cíclica es el valor lógico calculado por el transmisor y se coloca en el FCS, luego el receptor calcula su propio FCS y si estos coinciden entonces la trama se acepta. Sin embargo, puede que una trama que se acepta por no corrupta en realidad lo esté si se generan errores que compensen la sumatoria.

El proceso de la sumatoria se desarrollara más adelante al abarcar los otros protocolos de capa de enlace de datos.



Figura. 3-8 Campo trailer colocado al final de la trama.

Como ultima mención en esta parte sobre el tráiler, existe una parte de la trama que se denomina “Stop frame”. Esta parte permite avisar o informar al receptor cuando finaliza

³² FCS = Frame Check Sequence – Secuencia de verificación de trama.

³³ Checksum es un valor calculado para verificación.

el marco de trama enviado. Esto le permite al receptor informar a su receptor que la trama se recibió de forma completa.

Acorde al protocolo que se implementa en receptor y transmisor esta parte de la trama puede hacer que el receptor envíe un mensaje al transmisor indicando que la trama no se recibió completa.

3.1.2.2 Dispositivos de capa de enlace

3.1.2.2.1 Hub

Es un dispositivo pequeño, simple y económico que permite la unión de varias computadoras. Muchos de los hub(concentradores) de redes están disponibles para soportar conexión bajo el estándar Ethernet. Otro tipos soportan la conexión a través de puertos USB (Ver Figura. 3-9), pero el estándar Ethernet es el más ocupado en las redes domesticas.



Figura. 3-9 Concentrador de red tipo USB

3.1.2.2.1.1 Características de hubs tipo Ethernet

Los concentradores tipos Ethernet varían su velocidad de transmisión (Ver Figura. 3-10). Las velocidades de transmisión en los hubs alcanzaban un máximo de 10 Mbps. Sin embargo los modelos de hubs actuales pueden operar con una velocidad de transmisión de 100Mbps e incluso tienen la opción de configurarse a funcionar a 10Mbps. (Mitchell, About.com, 2010)

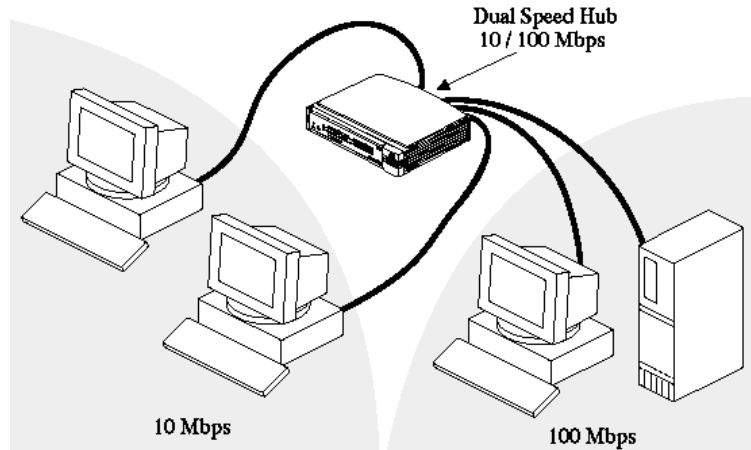


Figura. 3-10 Concentrador de red opera utilizando 2 velocidades de transmisión.

El número de puertos en un hub Ethernet puede variar de tal forma que pueda adaptarse a los márgenes de necesidad y costo de los clientes. Los concentradores más comunes son los que tienen 4 o 5 puertos Ethernet (Ver Figura. 3-11), puesto que estos se pueden encontrar en algunos hogares. En el caso de pequeñas empresas pueden requerirse entre 8 o 16 puertos (Ver Figura. 3-12).



Figura. 3-11 Concentrador de 4 puertos



Figura. 3-12 Concentrador de 16 puertos

Los hubs antiguos eran relativamente grandes y generaban ruidos producto de ventiladores o unidades de enfriamiento. Los nuevos dispositivos son mucho más pequeños, móviles y no ruidosos.

3.1.2.2.1.2 ¿Cuándo utilizar un hub?

Los hubs tipo Ethernet operan a nivel de capa 2 del modelo OSI, al igual que un switch. Los concentradores ofrecen funcionalidades comparables a los conmutadores, sin

embargo en relación a las otras ventajas ofrecidas por los switch se prefieren reemplazar los hubs. No obstante, al ser más económico un hub puede ser utilizado para reemplazar de forma momentánea un switch de red dañado.

3.1.2.2.2 Switch

Un switch es un dispositivo que al igual que un hub permite la conexión de varias computadoras dentro de una red de área local. Técnicamente un switch opera en relación a los protocolos de capa 2 del modelo OSI.

Un switch (conmutador) físicamente es muy parecido a un hub, pero el switch es “más inteligente” y por ende más caro que un hub. A diferencia de los concentradores, los conmutadores son capaces de inspeccionar los paquetes de datos que recibe por cada uno de sus puertos, determinando así el dispositivo transmisor y el receptor de la trama para luego enviarle únicamente por el puerto del host receptor. Esto permite conservar el ancho de banda al disminuir el tráfico en las otras líneas (Ver Figura. 3-13).

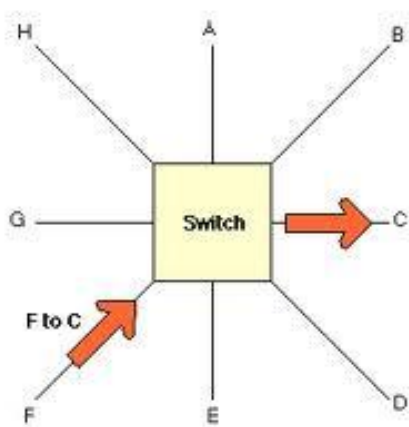


Figura. 3-13 Funcionamiento lógico de un Switch.

Al igual que con hubs, la implementación de switch basados en el estándar Ethernet son las más comunes. Las redes Ethernet que se construyen con conmutadores son capaces de soportar velocidades de entre 10 y 100 Mbps, que corresponden al estándar Fast Ethernet. De igual forma el estándar Gigabit Ethernet acepta velocidades de 10, 100 y 1000 Mbps. (Mitchell, About.com, 2010)

La Figura. 3-14 muestra el uso selectivo de los puertos Ethernet de una switch y las velocidades que se emplean acorde al dispositivo al que se conecta.

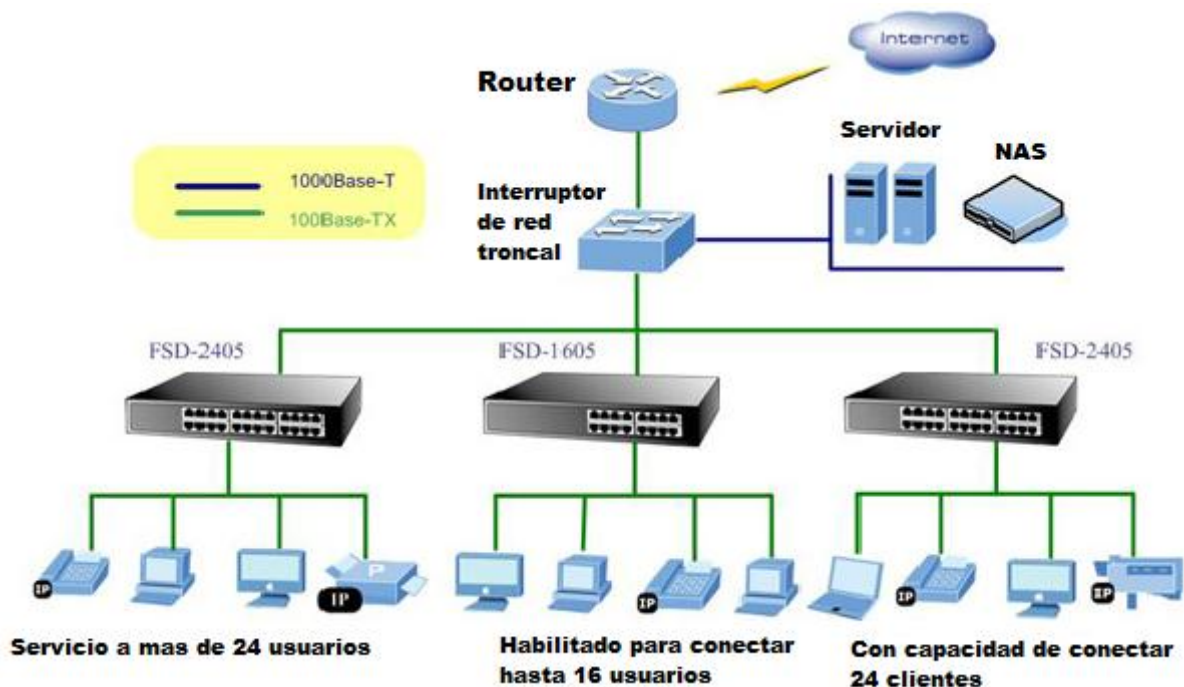


Figura. 3-14 Infraestructura de red con un switch como punto de conmutación entre secciones LAN.

El número de dispositivos que se conecta a un switch varía según el modelo que se utiliza. La mayoría de usuarios compran conmutadores que traen entre 4 o 5 puertos de conexión tipo Ethernet.

Los switches pueden ser conectados entre ellos, lo que permite aumentar la capacidad de conectar dispositivos. A este procedimiento se le conoce como *daisy chaining* o “conexión en serie”. (Mitchell, About.com, 2010)

3.1.2.2.1 Redes de Área Local Virtuales

El hecho de tener usuarios de una empresa conectados a la misma red local, genera un problema para brindar confidencialidad entre los usuarios de esta.

Por otro lado, el hecho de conectar una gran cantidad de usuarios en una red LAN indica que todos ellos forman parte de un dominio de colisión, por lo cual el ancho de banda disponible en la red no se aprovechaba de forma eficiente.

La solución a este problema se resuelve dividiendo la red LAN (Ver Figura. 3-15) en pequeñas secciones o dominios de colisiones más pequeños en lugar de un solo gran dominio de colisiones.

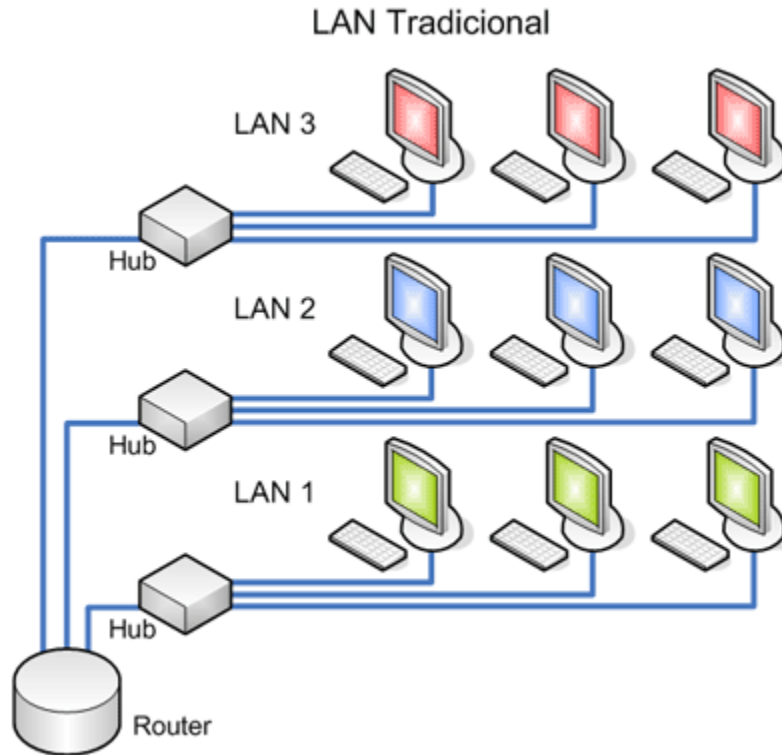


Figura. 3-15 División de red LAN en varios dominios.

Este proceso involucra la compra de nuevos equipos para llevar a cabo la división de la red LAN. Lo que en algunos casos no resulta como una opción debido al cargo económico por recurso. Es por ello que surge la necesidad de crear un método virtual de división de red LAN.

Una VLAN se encuentra conformada por un conjunto de dispositivos de red interconectados de forma “virtual”, se define como una subred definida por software y es considerada como un dominio de broadcast que puede estar en el mismo medio físico o bien los integrantes pueden estar ubicados en distintos sectores de la corporación.

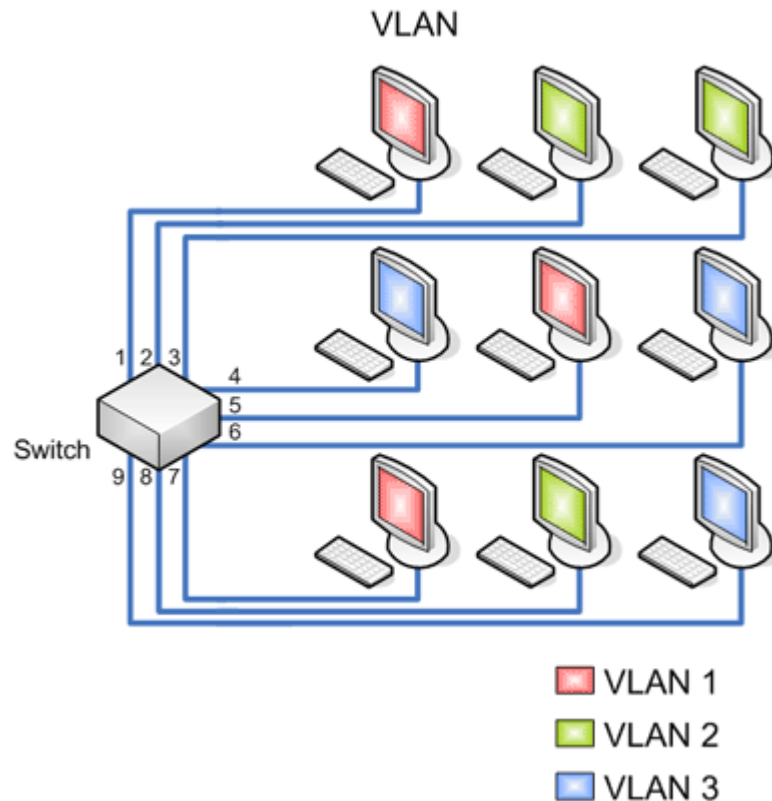


Figura. 3-16 División de una red LAN en 3 LANs virtuales.

Las redes VLANs se implementan en switches, en lugar de hubs o concentradores. Esto permite un control más inteligente del tráfico de la red, ya que los switches trabajan a nivel de la capa 2 del modelo OSI y son capaces de aislar el tráfico de un segmento del resto de la red. Esto permite aumentar considerablemente la eficiencia de la red. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios.

3.1.2.2.2.2 Tipos de VLAN

Existen distintos tipos de Redes LAN Virtuales. Entre ellas están:

3.1.2.2.2.2.1 VLAN de puerto central

En este tipo de de VLAN todos los nodos se conectan al mismo puerto del switch

3.1.2.2.2.2.2 VLAN Estaticas

Los puertos del switch están pre asignados a las estaciones de trabajo.

3.1.2.2.2.3 VLAN por asignación de puertos

En este caso se configura una cantidad “n” de puertos en el cual se puede indicar que puerto pertenece a cada VLAN. Este tipo tiene como ventaja la facilidad de movimientos y cambios en la asignación de puertos. La asignación realizada de puertos es independiente de los protocolos utilizados, no existen limitaciones en cuanto a los protocolos utilizados.

Sin embargo tiene la desventaja de que cualquier cambio en la estación de trabajo hace necesaria la reconfiguración del puerto del switch al que está conectado el usuario.

3.1.2.2.2.4 VLAN por dirección MAC

Las direcciones MAC de las computadoras que utilizan los usuarios que pertenecen a la VLAN están agregados en una tabla. Cada dirección MAC se asocia a una VLAN específica. Es una ventaja sobre las VLAN por asignación de puertos pues el usuario puede cambiarse de puerto en el switch sin ningún inconveniente.

El problema de este sistema es la configuración manual de las direcciones MAC de cada usuario en la tabla de registro.

3.1.2.3 Protocolos de enlace

Acceso múltiple por detección de portadora con detección de colisiones - Carrier Sense Multiple Access With Collision Detection (CSMA/CD), es una modificación de CSMA.

CSMA/CD es usado para mejorar el rendimiento de CSMA por la terminación de transmisiones tan pronto como la colisión es detectada, y reduciendo la probabilidad de una segunda colisión en el reenvío (CISCO, 2008).

Acceso múltiple por detección de portadora con prevención de colisión - Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA): es al igual que el caso anterior una modificación de CSMA.

La prevención de colisiones es usada para mejorar el rendimiento utilizando en una menor medida el canal. Si el canal está siendo usado antes de la transmisión entonces es retenida por un intervalo de tiempo aleatorio. Esto reduce la probabilidad de colisiones en el canal.

3.1.2.3.1 CSMA/CD

Este es un método de acceso en redes de datos en el cual (Stallings, 2004):

- Un escenario de detección de portadora es implementado
- Una estación transmisora de datos que detecta otra señal mientras está transmitiendo, detiene el envío de esa trama, envía una señal de colisión y luego espera por un intervalo de tiempo aleatorio antes de volver a enviar la trama de datos de nuevo.

Como ya se había mencionado anteriormente CSMA/CD es una modificación de CSMA.

Este es usado para mejorar el rendimiento mediante la terminación tan pronto como le es posible una vez que una colisión es detectada, y reduciendo la probabilidad de una segunda colisión en el proceso de reenvío.

3.1.2.3.1.1 Procedimiento o algoritmo de ejecución.

1. La trama debe estar lista para la transmisión
2. El host debe verificar si el medio está libre. Si el medio no lo está, debe esperar.
3. Si el medio esta libre, la transmisión comienza.
4. Luego el transmisor debe verificar si durante la transmisión a ocurrido una colisión. Si es así, se inicia el proceso de colisión detectada.
5. Finalmente se reinician los contadores de retransmisión y finaliza el envío de esa trama.
(CISCO, 2008)

3.1.2.3.1.2 Procedimiento de colisión detectada.

1. Se continúa la transmisión hasta alcanzar el tiempo mínimo que debe durar un paquete de datos para que todas las unidades puedan percibir que ha ocurrido una colisión.
2. Se incrementa el contador de retransmisión.
3. Luego el transmisor verifica si la última retransmisión ha excedido o no el número máximo de retransmisiones aceptables. Si así, se deja de intentar de enviar el paquete.
4. Si no se ha excedido, se calcula el tiempo aleatorio que debe esperar el transmisor antes de un nuevo intento basado en el número de colisiones que han ocurrido.

Esto puede explicarse a través de una analogía a una cena, donde todos los invitados hablan a través de un medio común, que sería el aire. Antes de hablar cada invitado de forma educada espera a que la persona que está hablando termine. Si dos invitados empiezan a hablar al mismo tiempo, ambos se detendrán y esperaran por poco tiempo pero

que igual será un periodo aleatorio para cada uno. En el estándar Ethernet, este tiempo está dado en términos de microsegundos. Se espera que cada uno escoja un periodo aleatorio y diferente para que no ocurra nuevamente una colisión.

Los métodos para detección de colisiones son aplicables dependiendo del medio, pero en un bus eléctrico tal como 10BASE-5 o 10BASE-2, las colisiones pueden ser detectadas mediante la comparación entre los datos transmitidos y datos recibidos o bien a través del reconocimiento de niveles no normales en la amplitud de las señales en el bus.

3.1.2.3.1.3 Aplicaciones

CSMA/CD ha sido utilizado en la topología de bus para distintas variantes de Ethernet y en versiones más tempranas de Ethernet aplicado en par trenzado de cobre. Las redes Ethernet modernas construidas con switches y conexiones full-duplex ya no utilizan CSMA/CD. Por otro lado, el estándar de la IEEE 802.3, el cual define las variantes de Ethernet, por razones históricas mantiene el título de “Carrier sense multiple Access with collision detección”.

3.1.2.3.2 CSMA/CA

En el ambiente de computadoras este sistema es implementado en redes inalámbricas como método de acceso para medios compartidos, en el cual (GS Comunicaciones, 1999):

- Se implementa la detección de portadoras en el medio
- Cuando un nodo tiene intenciones de transmitir datos primero tiene que escuchar en el canal durante un lapso de tiempo previo para determinar si otro nodo está transmitiendo dentro del rango de acceso inalámbrico. Si el canal se encuentra libre, entonces se le permite al nodo el comenzar el proceso de transmisión. Si el canal está ocupado, el nodo retiene la transmisión por un tiempo aleatorio. Una vez que el proceso de transmisión comienza, es todavía posible que la transmisión realizada desde la capa de aplicación nunca ocurra.

La prevención de colisión es usada para mejorar el rendimiento o desempeño del CSMA no permitiendo a estaciones inalámbricas el transmitir si otra unidad está transmitiendo dentro del rango de la red inalámbrica. De tal forma que se reducen las probabilidades de colisiones debido al uso del tiempo de retardo aleatorio exponencial truncado binariamente³⁴.

Esta última opción casi siempre es implementada, un intercambio de señales RTS/CTS puede ser requerido para mejorar el manejo de los escenarios tal como un problema generado por un nodo oculto en una red inalámbrica.

³⁴ En ingles: random truncated binary exponential backoff time

El uso de la prevención de colisiones mejora aún más el rendimiento de CSMA a través de la división de los canales inalámbricos en una cantidad igual o mayor al número de nodos transmisores sin incluir el rango de dominio de colisiones. CSMA/CA difiere de CSMA/CD en debido al medio en que es implementado y el radio del espectro de frecuencia. Las colisiones no pueden ser detectadas mientras estas ocurran en el nodo transmisor. CSMA/CA es usado en el estándar 802.11 utilizado en redes LAN inalámbricos y otros sistemas de comunicación alambrados e inalámbricos. Uno de los problemas de las comunicaciones de datos inalámbricos es que no les es posible escuchar al medio mientras estos están transmitiendo, por lo que la detección de las colisiones no son posibles. Otra razón es el problema de una terminal oculta, supongamos que un nodo A esta en el rango de un receptor R, pero que no está en el rango del transmisor S, y por lo tanto el nodo A no sabe qué R está transmitiendo.

3.1.2.3.2.1.1 RTS/CTS

En esta sección se desarrollan los conceptos de RTS/CTS y su aplicación en el estándar 802.11.

CSMA/CA puede de manera opcional ser sustituido por el proceso de intercambio de paquetes de Peticione de envío – Request to send (RTS) enviados desde el transmisor, y paquetes de Despeje para enviar – Clear to send (CTS) enviados por receptor correcto, en el caso anterior R se encargaría de enviar estos CTS a las otras unidades. Esto permite alertar a todos los nodos que no se encuentren en el rango del transmisor, receptor o ambos para que no transmitan datos mientras se esté enviando la trama. La cantidad de tiempo que el nodo debe esperar antes de intentar transmitir en el medio es incluida tanto en las trama de RTS y CTS.

Esto es conocido como el estándar de IEEE 802.11 RTS/CTS. La implementación de este estándar ayuda a resolver el problema de terminales ocultas que generalmente sucede en las redes inalámbricas.

3.1.2.4 Tecnologías de capa de enlace de datos

3.1.2.5 HLDC

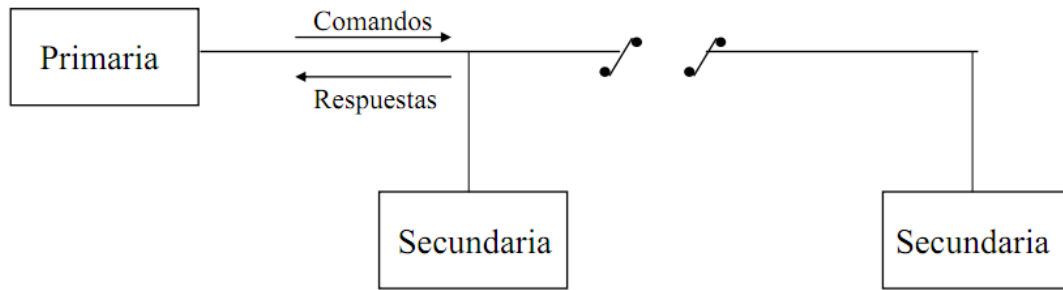
HDLC³⁵ es un “estándar” ISO y deriva del SDLC (Synchronous Data Link Control) desarrollado por IBM en 1972 para su arquitectura SNA.

Surge como evolución de SDLC, considera el protocolo que ha incluido los aspectos recogidos por SDLC y otras funcionalidades. Tanto SDLC como HDLC son protocolos de ventana deslizante muy completos.

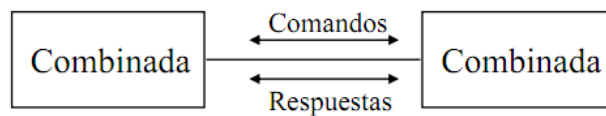
³⁵ HDLC = High level Data Link Control – control de enlace de datos de alto nivel

SDLC/HDLC es un protocolo inicialmente pensado para conexiones remotas a un supercomputador en modo bien punto a punto o bien multipunto. En las conexiones punto a punto, son llamadas “balanceadas”, una comunicación de igual a igual.

En las conexiones multipunto, son llamadas “no balanceadas”, los elementos que participan en SDLC/HDLC son un nodo llamado primario y varios secundarios. (Ver Figura. 3-17) El nodo primario controla a los secundarios por “polling” o monitorización. Los secundarios, sólo responden a los primarios bajo petición.



a) Modo no balanceado



b) Modo balanceado

Figura. 3-17 Elementos HDLC

Los protocolos del nivel de enlace definen, típicamente, reglas para: iniciar y terminar un enlace (sobre un circuito físico previamente establecido), controlar la correcta transferencia de información y recuperarse de anomalías.

El HDLC consiste en tramas de bits que están delimitadas por unas banderas de 8 bits de longitud que contienen el valor 01111110 binario. Cuando el receptor encuentra este valor en el canal, comienza la lectura de una trama, lectura que termina cuando vuelve a encontrar este mismo valor. Nótese que una bandera puede indicar, simultáneamente, el final de una trama, y el comienzo de la siguiente. Puesto que dentro de una trama, en el campo de datos de usuario puede aparecer este valor, el transmisor insertará automáticamente un bit a 0 detrás de cada bloque de cinco bits a 1; el receptor, a su vez, eliminará cada bit a 0 que siga a un bloque de cinco bits a 1; con este esquema se garantiza que nunca aparecerá el valor de la bandera dentro de los bits de datos, es decir, el usuario puede colocar cualquier información dentro del paquete, la transmisión es totalmente transparente.

Las tramas incorporan una dirección, un código de control y unos números de secuencia. Los números de secuencia de recepción indican el número de secuencia de la siguiente trama que se espera recibir; así, si una trama es recibida correctamente, este valor se incrementará, haciendo que el emisor mande la siguiente trama; si la trama se pierde el valor permanecerá igual, con lo que el emisor la volverá a enviar.

Las tramas de control gestionan fundamentalmente el control de flujo y la notificación de errores.

3.1.2.5.1.1 Características

Tipos De Estaciones.

Definimos tres tipos de estaciones que dan lugar a dos configuraciones de enlace y tres modos de transferencia de datos.

- **Estación primaria:** Controla las operaciones del enlace. Actúa como maestra y sus tramas son órdenes para las estaciones secundarias. Recibe respuestas de éstas últimas.
- **Estación secundaria:** Opera bajo el control de una estación primaria. Actúa como esclava de la primaria y sus tramas son respuestas. Mantiene solamente una sesión con la estación principal y no tiene responsabilidad en el control del enlace. Las estaciones secundarias no pueden comunicarse directamente entre sí, lo hacen a través de la estación primaria.
- **Estación combinada:** Es capaz de transmitir y recibir tanto órdenes como respuestas procedentes de otra estación combinada.

Configuraciones Del Enlace.

- **Configuración no balanceada (o no equilibrada):** para una estación primaria y una o varias estaciones secundarias. Pueden ser punto a punto o multipunto, dúplex o semidúplex. Se la llama "no balanceada" porque la estación primaria es responsable de controlar cada una de las estaciones secundarias y de establecer y mantener el enlace.
- **Configuración balanceada (o equilibrada):** consiste en dos estaciones combinadas en un enlace punto a punto ya sea dúplex o semidúplex. Cada estación tiene la misma responsabilidad en el control del enlace.

Nota: Los términos balanceado y no balanceado empleados no tienen nada que ver con las características eléctricas del circuito. De hecho el control del enlace de datos no debe ser consciente de los atributos físicos del circuito. Los dos términos son usados en un contexto totalmente distinto en el nivel físico y en el nivel de enlace.

3.1.2.6 PPP

El PPP³⁶ es un protocolo que permite la conexión entre dos puntos de una red. El protocolo punto a punto fue desarrollado por el grupo de trabajo IETF³⁷ (ALEGSA, 2010).

Permite conectar computadoras utilizando distintos medios físicos como: cable serial, línea telefónica, teléfono celular, enlace de fibra óptica y otros. Generalmente es empleado para establecer la conexión a internet desde un usuario al proveedor de internet a través de un módem telefónico. En algunos casos es usado para conexiones de banda ancha tipo DSL.

Además del simple transporte de datos, PPP facilita dos funciones importantes:

- Autenticación. Generalmente mediante una clave de acceso.
- Asignación dinámica de IP. Los proveedores de acceso cuentan con un número limitado de direcciones IP y cuentan con más clientes que direcciones.

Naturalmente, no todos los clientes se conectan al mismo tiempo. Así, es posible asignar una dirección IP a cada cliente en el momento en que se conectan al proveedor. La dirección IP se conserva hasta que termina la conexión por PPP. Posteriormente, puede ser asignada a otro cliente.

PPP también tiene otros usos, por ejemplo, se utiliza para establecer la comunicación entre un módem ADSL y la pasarela ATM del operador de telecomunicaciones. También se ha venido utilizando para conectar a trabajadores desplazados (p. ej. ordenador portátil) con sus oficinas a través de un centro de acceso remoto de su empresa. Aunque esta aplicación se está abandonando en favor de las redes privadas virtuales, más seguras.

³⁶ PPP= Point to Point Protocol - Protocolo Punto a Punto

³⁷ IETF= Internet Engineering Task Force

3.1.2.6.1 Detalles técnicos del protocolo Punto a Punto

PPP provee un protocolo de encapsulación tanto sobre enlaces sincrónicos orientados a bits, como sobre enlaces asincrónicos con 8 bits de datos sin paridad.

PPP puede operar a través de cualquier interfaz DTE/DCE. Estos enlaces deben ser Full-Duplex pero pueden ser dedicados o de circuitos conmutados.

La Tabla 3-3 muestra los componentes del protocolo punto a punto.

Tabla 3-3

Componentes de PPP.
A. Una forma de encapsulamiento no ambiguo que identifica claramente el comienzo de un datagrama y el final del anterior.
B. Un protocolo de control de enlace para activar y probar líneas, negociar opciones y desactivar el enlace ordenadamente cuando éste ya no sea necesario.
C. Una familia de NCP ³⁸ , que permiten negociar los parámetros de la capa de red con independencia del protocolo de red utilizado.

Uno de los usos de este protocolo en el ámbito de la telefonía es cuando se implementa el servicio “devolución de llamada”, si la red está configurada para la conexión de acceso telefónico, se finaliza la conexión física y el servidor de acceso remoto devuelve la llamada al cliente de acceso remoto.

3.1.2.6.1.1 Funcionamiento

PPP consta de las siguientes fases:

1. Estable de conexión. Durante esta fase, una computadora contacta con la otra y negocian los parámetros relativos al enlace usando el protocolo LCP. Este protocolo es una parte fundamental de PPP y por ello está definido en el mismo RFC. Usando LCP se negocia el método de autenticación que se va a utilizar, el tamaño de los datagramas, números mágicos para usar durante la autenticación,...

³⁸ NCP = Network Control Protocols – Protocolos de control de red.

2. Autenticación. No es obligatorio. Existen dos protocolos de autenticación. El más básico e inseguro es PAP, aunque no se recomienda dado que manda el nombre de usuario y la contraseña en claro. Un método más avanzado y preferido por muchos ISPs es CHAP, en el cual la contraseña se manda cifrada.
3. Configuración de red. En esta fase se negocian parámetros dependientes del protocolo de red que se esté usando. PPP puede llevar muchos protocolos de red al mismo tiempo y es necesario configurar individualmente cada uno de estos protocolos. Para configurar un protocolo de red se usa el protocolo NCP correspondiente. Por ejemplo, si la red es IP, se usa el protocolo IPCP para asignar la dirección IP del cliente y sus servidores DNS.
4. Transmisión. Durante esta fase se manda y recibe la información de red. LCP se encarga de comprobar que la línea está activa durante periodos de inactividad. Obsérvese que PPP no proporciona cifrado de datos.
5. Terminación. La conexión puede ser finalizada en cualquier momento y por cualquier motivo.

3.1.2.7 Frame Relay

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama “Frame Relay”. También incorporan los nodos que conmutan (Ver Figura. 3-18) las tramas “Frame Relay” en función del identificador de conexión, a través de la ruta establecida para la conexión en la red.

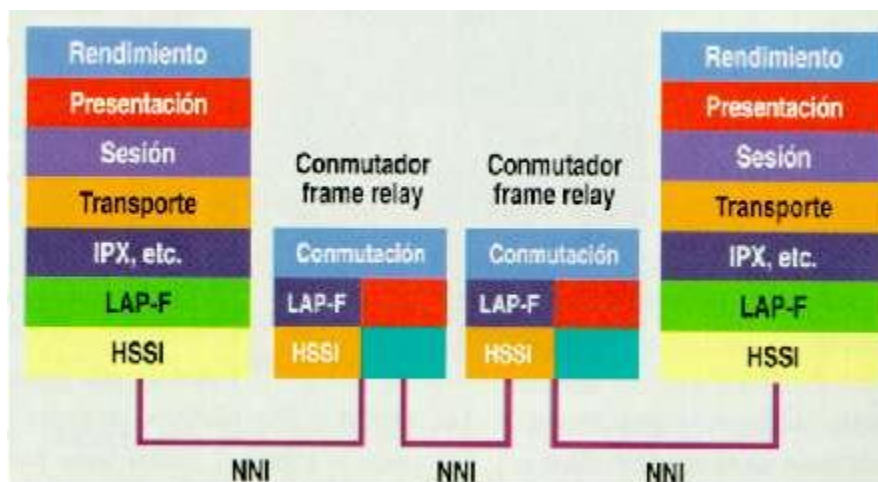


Figura. 3-18 Estructura OSI de la red Frame Relay

Las tramas y cabeceras de Frame Relay pueden tener diferentes longitudes (Ver Figura. 3-19), ya que hay una gran variedad de opciones disponibles en la implementación,

conocidos como anexos a las definiciones del estándar básico.

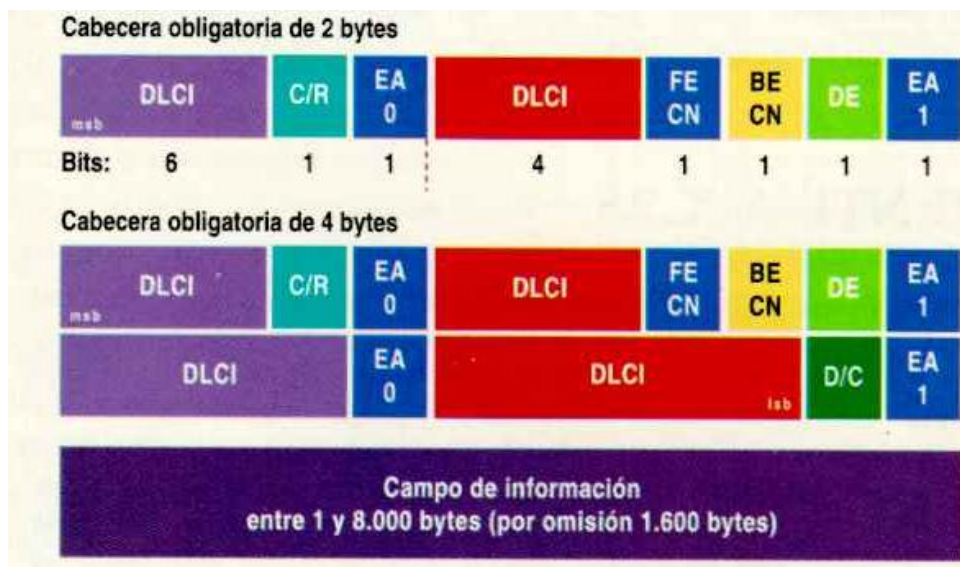


Figura. 3-19 Formatos de cabecera Frame Relay

La información transmitida en una trama Frame Relay puede oscilar entre 1 y 8.250 bytes, aunque por defecto es de 1.600 bytes. (Palet, 1997)

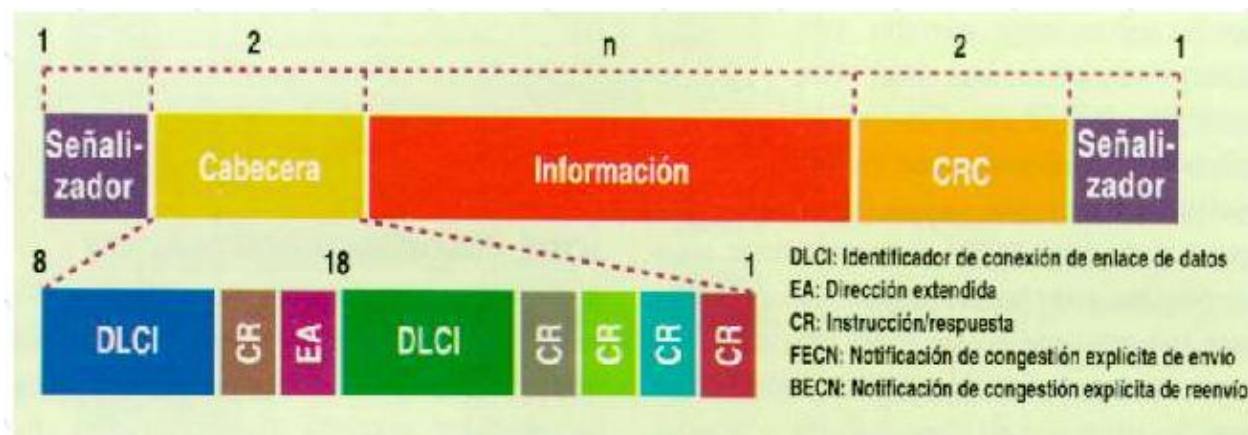


Figura. 3-20 Ubicación de señalizadores Frame Relay en la trama de datos.

Frame Relay puede funcionar utilizando un gran número de formas y tamaños de tramas. Por otro lado, este protocolo ha demostrado poseer un alto grado de interoperabilidad entre diferentes fabricantes de equipos y redes. Esto se debe a que siempre existe la posibilidad de "convertir" los formatos de Frame Relay a uno común, intercambiando así las tramas en dicho formato.

En Frame Relay, los dispositivos del usuario se interrelacionan con la red de comunicaciones, siendo estos los responsables del control de flujo y de errores (Ver Figura.

3-20). La red sólo se encarga de la transmisión, conmutación de los datos e indicar cuál es el estado de los recursos de esta. En el caso de errores o de saturación de los nodos de la red, los equipos del usuario solicitarán el reenvío (al otro extremo) de las tramas incorrectas y si es preciso reducirán la velocidad de transmisión, para evitar la congestión.

Las redes Frame Relay son orientadas a conexión. El identificador de conexión es la concatenación de dos campos HDLC³⁹, en cuyas especificaciones originales de unidad de datos (protocolo de la capa 2), se basa Frame Relay. Entre los dos campos HDLC que forman el "identificador de conexión de enlace de datos" o DLCI⁴⁰ se insertan algunos bits de control (CR y EA). (Palet, 1997)

3.1.2.7.1 Ejemplo practico

Observe la Figura. 3-21. Si el usuario "A" desea una comunicación con el usuario "B", establecerá un VC⁴¹, que primero los una. La información a ser enviada se segmenta en tramas a las que se añade el DLCI.

Una vez que las tramas son entregadas a la red, son conmutadas según unas tablas de enrutamiento que se encargan de asociar cada DLCI de entrada a un puerto de salida y un nuevo DLCI.

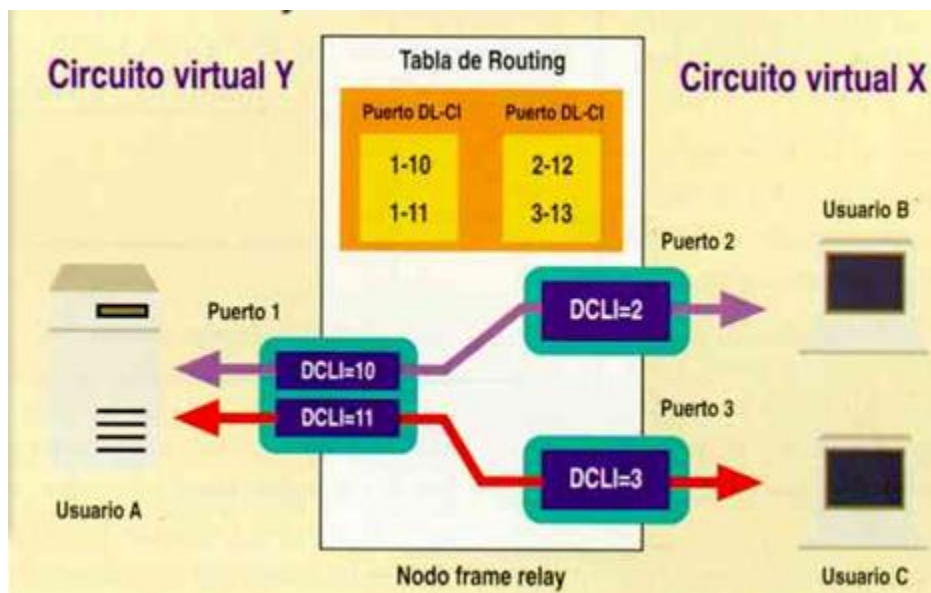


Figura. 3-21 Ejemplo Red Frame Relay

En el destino, las tramas son reensambladas.

³⁹ HDLC = High-level Data Link Control – Control de enlace de alto nivel para datos.

⁴⁰ DLCI = Data Link Connection Identifier – Identificador de conexión de enlace de datos.

⁴¹ VC = Circuito virtual

En la actualidad las redes públicas sólo ofrecen PVC⁴² (Ver Figura. 3-22). En el futuro podremos disponer de SVC⁴³ o), según los cuales el usuario establecerá la conexión mediante protocolos de nivel 3, y el DLCI será asignado dinámicamente

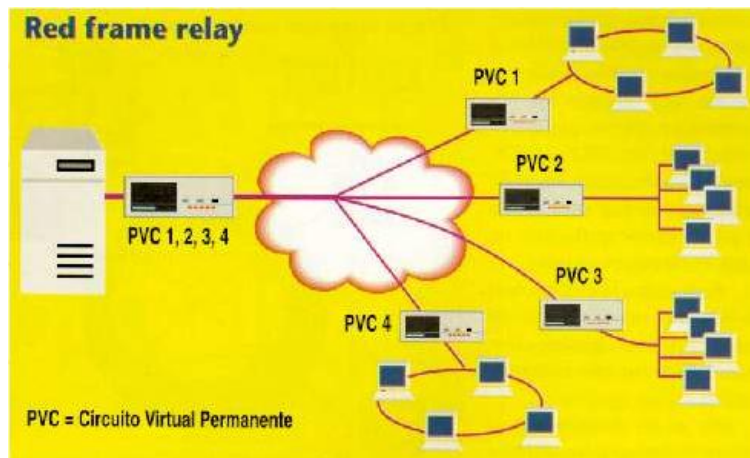


Figura. 3-22 Ejemplo conexión de PVCs en red Frame Relay

3.1.2.8 ATM

Con esta tecnología, a fin de aprovechar al máximo la capacidad de los sistemas de transmisión, sean estos de cable o radioeléctricos, la información no es transmitida y conmutada a través de canales asignados en permanencia, sino en forma de cortos paquetes (celdas ATM) de longitud constante y que pueden ser enrutados individualmente mediante el uso de los denominados canales virtuales y trayectos virtuales.

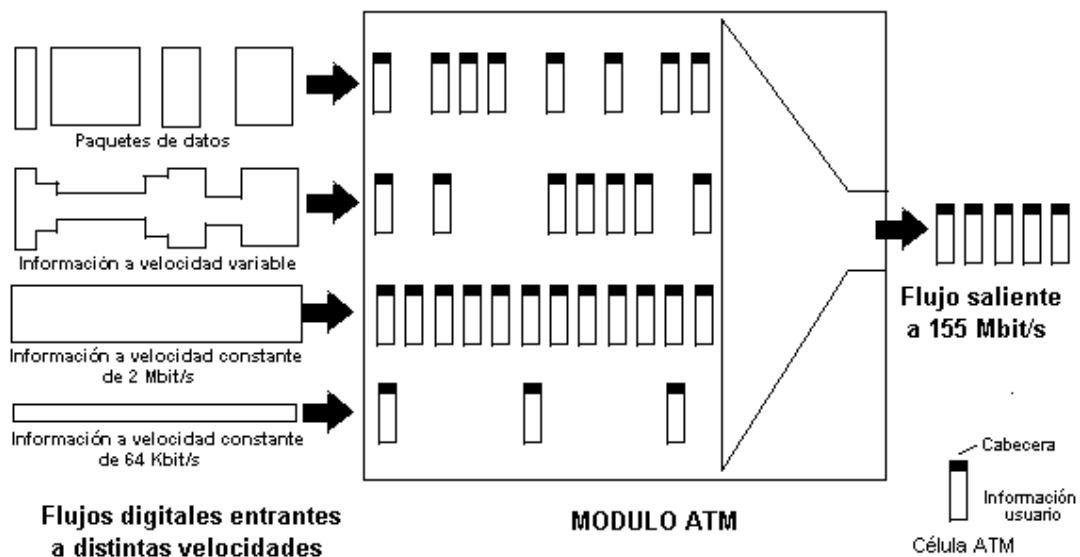


Figura. 3-23 Proceso de conmutación de ATM

⁴² PVC = Permanent Virtual Circuit - Circuitos Virtuales Permanentes

⁴³ SVC = Switched Virtual Circuit - Circuitos Virtuales Conmutados -

En la Figura. 3-23 se ilustra la forma en que diferentes flujos de información, de características distintas en cuanto a velocidad y formato, son agrupados en el denominado Módulo ATM para ser transportados mediante grandes enlaces de transmisión a velocidades (bit rate) de 155 o 622 Mbit/s facilitados generalmente por sistemas SDH (Wikipedia, 2011).

En el terminal transmisor, la información es escrita byte a byte en el campo de información de usuario de la celda y a continuación se le añade la cabecera.

En el extremo distante, el receptor extrae la información, también byte a byte, de las celdas entrantes y de acuerdo con la información de cabecera, la envía donde ésta le indique, pudiendo ser un equipo terminal u otro módulo ATM para ser encaminada a otro destino. En caso de haber más de un camino entre los puntos de origen y destino, no todas las celdas enviadas durante el tiempo de conexión de un usuario serán necesariamente encaminadas por la misma ruta, ya que en ATM todas las conexiones funcionan sobre una base virtual.

3.1.3 Capa de Internet

3.1.3.1 Router

Son dispositivos físicos que permiten la unión o conexión de varias redes. Técnicamente, un enrutador o router opera bajo los protocolos de capa 3 del modelo OSI. El router funciona como una puerta de enlace o acceso para una LAN.

Los diseñadores de redes domésticas implementan el protocolo de internet (IP) en la operación de los routers. El protocolo IP es el protocolo de red más comúnmente utilizado. Un router IP permite a una red LAN hogareña acceder a internet, tal como lo haría un router DSL⁴⁴ o cable modem.

El router mantiene la información de su configuración en una memoria llamada “Tabla de enrutamiento” o “*Routing table*”. Además, los routers alámbricos o inalámbricos tiene la capacidad de filtrar tráfico tanto de entrada o de salida a la red LAN basándose en las direcciones lógicas de capa 3 que tienen los receptores y transmisores

La construcción de una red de computadoras utilizando un router puede facilitar a los usuarios a:

- Compartir archivos entre computadoras
- Compartir una conexión a internet entre computadoras
- Compartir una impresora
- Conectar una consola de juego u otro equipo de entretenimiento casero a internet.

⁴⁴ DSL = Digital Subscriber Line – Línea Digital de subscritor.

3.1.3.1.1 ¿Cómo escoger un router?

En el Mercado existe una gran variedad y tipos de router para uso doméstico (Ver Figura. 3-24). Los 2 tipos más conocidos son los que se incorporan los estándares 802.11b y 802.11g. Estos modelos son de tipo inalámbricos. El modelo 802.11n es el más reciente, pero la primera versión (802.11b) opera bajo un precio mucho menor.

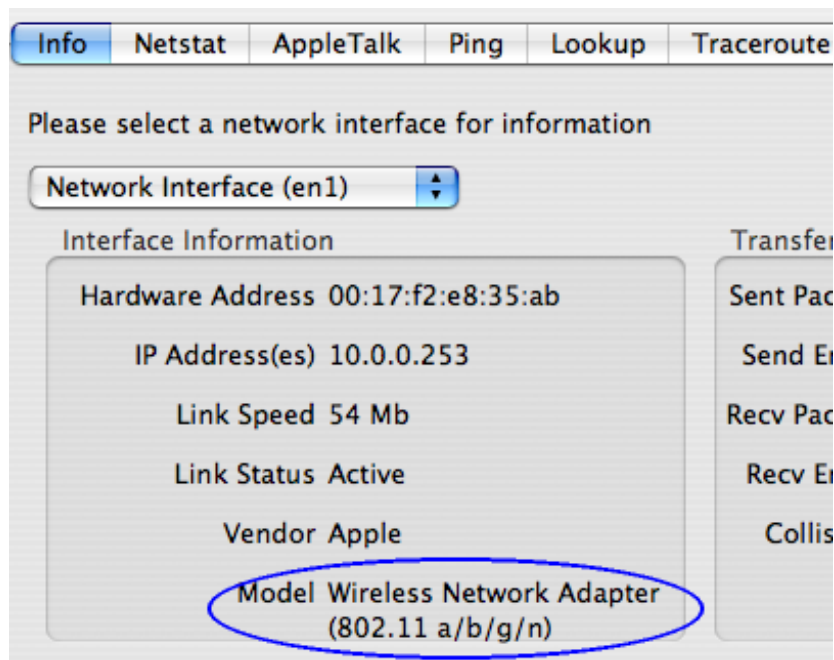


Figura. 3-24 Los dispositivos terminales de red poseen la capacidad de operar con distintos estándares.

Un factor importante al escoger un router es la tasa de transmisión máxima que este puede tener. Las velocidades de los routers como se ha mostrado anteriormente se establecen en Mbps. Los modelos más antiguos ofrecen velocidades de 11 Mbps, mientras que los modelos 802.11g permiten hasta 54 Mbps y la última generación 802.11n un valor superior a 300 Mbps.

La Figura. 3-25 muestra la interacción o posible configuración que se puede realizar utilizando 2 estándares 802.11 para dar servicio a distintos equipos.

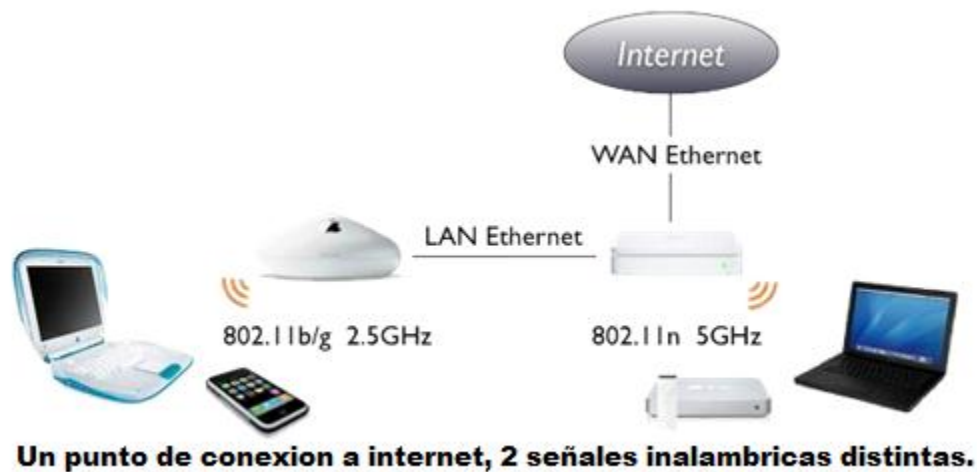


Figura. 3-25 Interconexión entre redes LAN que utilizan distintos estándares 802.11

La opción de un router con la mayor velocidad es probablemente la mejor opción a simple vista, sin embargo se debe tomar en cuenta el rendimiento actual de la red que se desea implementar. A mayor velocidad de transmisión en el router, el costo del mismo aumenta. Es por ello que no tendría ningún sentido ocupan un router con una tasa de transferencia de hasta 300 Mbps si las necesidades de los usuarios no demandan más de 54 Mbps.

Existe otra categoría de escogencia de router que radica en los aspectos domiciliario y empresarial. Un router para uso doméstico no exige capacidades extremas o demanda una confiabilidad tan alta como lo haría un router que se propone para funcionar en una empresa.

En el caso de los router empresariales se piden equipos de carácter escalable y más administrable. Por ejemplo, un router de tipo domiciliario (Ver Figura. 3-26) tiene por lo general 5 puertos Ethernet y permite crear una red inalámbrica. Brinda a su vez cierto grado de seguridad y en el mejor de los casos puede llegar a proveer opciones de filtrado de paquetes.



Figura. 3-26 Ejemplo de router domiciliario

Sin embargo estas opciones no son suficientes cuando se trata de un router de uso empresarial. La empresa puede aumentar su tamaño considerablemente y por ello se necesita que tenga una gran escalabilidad. Por ejemplo, el router Cisco CRS3 (Ver Figura. 3-27) tiene una escalabilidad de hasta 322 tbps. El equipo no solamente puede encaminar los paquetes a las rutas necesarias sino que además de esto puede hacer uso de las nuevas tecnologías multi-direccionales logrando determinar el camino más corto a un contenido determinado mejorando el impacto sobre la red y la experiencia del usuario.



Figura. 3-27 Router Cisco CRS3

Por otro lado, escoger un router para una empresa requiere justificar el porqué de la compra. Es decir, el router cisco podría ser la solución para muchas opciones pero si se

emplea en una empresa donde el tráfico de red muy inferior a la capacidad del router puede que estemos haciendo un gasto por demás.

El router cisco cuesta alrededor de 90,000 dólares (Wetcom Group, 2011), es posible que existan otros equipos que resulten más económicos y de igual forma puedan manejar el tráfico que cruza por la red. La escalabilidad de este nuevo router puede no igual a la escalabilidad del router cisco CRS3, pero bien puede ser suficiente para el crecimiento de la empresa por los próximos 3 o 4 años.

Otro factor importante en la escogencia de un router de uso empresarial, es su capacidad de administración de la red. Esto quiere decir que el equipo a escoger debe tener más opciones que las que tiene un router convencional. Debemos recordar que ambas capacidades escalabilidad y capacidad de administración dependen directamente de las exigencias de la empresa. Cada inversión en estos equipos requiere recursos monetarios, por lo cual tomar la decisión de escoger un router no debe ser a la ligera, es importante hacer un balance entre capacidades que se necesita y costo por el equipo, previo a su compra.

3.1.3.1.2 Switch vs Hub vs Routers

En esta parte nos enfocaremos en remarcar las diferencias y sobresalir algunas características de los 3 elementos intermediarios. Primero un router tiene la capacidad de leer en el encabezado de capa 3 de un paquete de datos que llega a él.

Los routers permiten la conexión de una red con otras, por lo cual puede pertenecer no solo a una red. En cambio un switch o hub puede únicamente funcionar siendo parte de una red o solo direccionara paquetes dentro de esa red.

Otras de las cualidades de los router es que estos pueden funcionar como un servidor DHCP⁴⁵ o servidor Proxy. Ambos temas se abordan en la siguiente sección. En la actualidad, a los routers se les han agregado algunas funciones propias de switch como la capacidad de leer el encabezado de capa 2. (CISCO, 2008)

En los hogares donde se implementan redes inalámbricas no existe ni switches, ni hubs estos equipos solamente pueden ser usados en redes alambradas. Un router inalámbrico incorpora gran parte de las funciones de una red alambrada.

⁴⁵ DHCP = Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Hosts.

3.1.3.2 Protocolo de red IPv4

3.1.3.2.1 Estructura de trama IPv4

El protocolo de red IP sólo tiene cabecera, ya que no realiza ninguna comprobación sobre el contenido del paquete. Sus campos se representan siempre alineados en múltiplos de 32 bits.

Los campos de este protocolo se muestran en la Figura. 3-28, seguida por las definiciones de cada uno de sus campos.

0-3	4-7	8-15	16-18	19-31
Versión	Tamaño Cabecera	Tipo de Servicio	Longitud Total	
Identificador			Indicadores	Posición de Fragmento
Checksum Cabecera				
Dirección IP de Origen				
Dirección IP de Destino				
Opciones				Relleno

Figura. 3-28 Formato de la cabecera IPv4

Versión	Actualmente se utiliza la versión 4, aunque ya está en funcionamiento la versión 6. Este campo permite a los routers discriminar si pueden tratar o no el paquete.
Longitud de cabecera (IHL)	Indica el número de palabras de 32 bits que ocupa la cabecera. Esto es necesario porque la cabecera puede tener una longitud variable.
Tipo de servicio	Determina el tipo de servicio al cual pertenece el paquete, sin embargo los routers no hacen mucho caso de esto y en la práctica no se utiliza. Los tipos de servicio disponibles serían: Delay, Throughput y Reliability.
Longitud del paquete	Este valor incluye la cabecera de encapsulamiento, el paquete más largo que puede enviarse es de 65535, pero la carga útil será menor porque se debe descontar la carga de cabecera.
Identificación	Esta casilla contiene el número de serie del paquete. Esto entra en vigencia cuando un paquete se parte en pedazos más pequeños por el camino (se fragmenta) cada uno de los fragmentos llevara el mismo número de identificación.
Control de fragmentación	Estos bits se dividen en: 1 bit de sobra, 1 bit para evitar la fragmentación, 1 bit para indicar que el paquete forma parte de un

paquete más grande que se fragmento. Y un último bit de “desplazamiento de fragmento”.

<i>Tiempo de vida</i>	Determina el número máximo de routers por los cuales puede cruzar antes de ser descartado. Este valor tiene un máximo de 255 saltos.
<i>Protocolo</i>	El campo modifica el protocolo de nivel de transporte al que va destinado este paquete.
<i>Cheksum de la cabecera</i>	Aunque no se comprueben los datos, la integridad de la cabecera es importante.
<i>Direcciones de origen y destino</i>	32 bits cada una. Son las direcciones IP del origen y destino.
<i>Opciones</i>	Esta parte puede presentarse o no, de estarlo su longitud máxima es de 40 bytes.

3.1.3.3 Protocolo IPv6

Hasta hace pocos años la Internet era utilizada en gran medida por universidades, industrias de alta tecnología y el gobierno. Con la explosión del interés por el Internet que comenzó a mediados de la década de los 90, los diseñadores de redes se percataron que era necesario realizar un cambio en el protocolo de internet para satisfacer las nuevas necesidades y exigencias del futuro. La versión o estándar conocido como IPv4 debía evolucionar y volverse más flexible.

La IETF comenzó a trabajar en 1990 en una versión nueva del IP, una que nunca se quedaría sin direcciones, resolviera otros problemas o debilidades de IPv4, sería más flexible y eficiente. Las metas principales eran:

- 1) Manejar miles de millones de *hosts*, aún con asignación de espacio de direcciones ineficiente.
- 2) Reducir el tamaño de las tablas de enrutamiento.
- 3) Simplificar el protocolo, para permitir a los enrutadores el procesamiento más rápido de los paquetes.
- 4) Proporcionar mayor seguridad (verificación de autenticidad y confidencialidad) que el IP actual.
- 5) Prestar mayor atención al tipo de servicio, especialmente con datos en tiempo real.
- 6) Ayudar a la multidifusión permitiendo la especificación de alcances.
- 7) Posibilitar que un *host* sea móvil sin cambiar su dirección.
- 8) Permitir que el protocolo evolucione.
- 9) Permitir que el protocolo viejo y el nuevo coexistan por años.

Para encontrar un protocolo que cumpliera con todos estos requisitos, la IETF hizo una convocatoria solicitando propuestas. Se recibieron 21 respuestas, no todas propuestas completas. Tres de las mejores propuestas se publicaron en *IEEE Network* las cuales correspondían a Deering, Francis, Katz y Ford. Estos dos últimos trabajaron conjuntos en una propuesta. Se seleccionó una versión modificada de la combinación de las propuestas de Deering y Francis, llamada ahora **SIPP (Protocolo Simple de Internet Mejorado)**, y se le dio la designación **Ipv6**.

El IPv6 cumple los objetivos bastante bien: mantiene las buenas características del IP, descarta y reduce las malas, y agrega nuevas donde se necesitan. En general, IPv6 no es compatible con IPv4, pero es compatible con todos los demás protocolos Internet, incluidos TCP, UDP, ICMP, IGMP, OSPF, BGP y DNS.

3.1.3.3.1 Mejoras de IPv6 sobre IPv4

La mejora más sobresaliente es que IPv6 tiene direcciones más grandes que el IPv4. Estas direcciones son de 16 bytes de longitud, lo que resuelve el problema de escases de direcciones IP; pues proporcionar una cantidad prácticamente ilimitada de direcciones Internet.

La segunda mejora principal del IPv6 es la simplificación del encabezado, que contiene sólo 7 campos (contra 13 en el IPv4). Este cambio permite a los enrutadores procesar con mayor rapidez los paquetes y mejorar, por tanto, la velocidad real de transporte.

La tercera mejora importante fue el mejor apoyo de las opciones. Este cambio fue esencial con el nuevo encabezado, pues campos que antes eran obligatorios ahora son opcionales.

Una cuarta área en la que el IPv6 representa un avance importante es la seguridad. La autenticación y la privacidad son características clave del IP nuevo.

3.1.3.3.2 Encabezado IPv6

La Figura 3-1 muestra el encabezado IPv6. El campo versión siempre es 6 para el IPv6. Durante el periodo de transición del IPv4 a IPv6, los enrutadores podrán examinar este campo para saber el tipo de paquete que tienen.

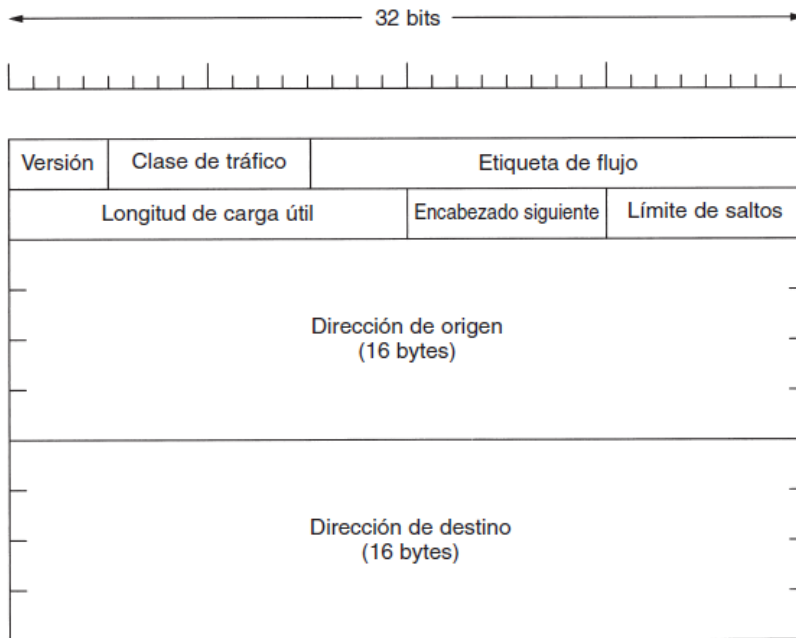


Figura 3-1 Encabezado IPv6

El campo clase de tráfico se usa para distinguir entre los paquetes con requisitos diferentes de entrega en tiempo real. Un campo diseñado para este propósito ha estado en el IP desde el principio pero los enrutadores lo han implementado solo esporádicamente.

El campo etiqueta de flujo aun es experimental, pero se usara para permitir a un origen y a un destino establecer una pseudoconexión con propiedades y requisitos particulares.

El campo longitud de carga útil indica cuantos bytes siguen al encabezado de 40 byte. El nombre de campo se cambió de longitud total en el IPv4 por que el significado cambio ligeramente, debido a que los 40 bytes del encabezado ya no se cuentan como parte de la longitud.

El encabezado siguiente revela el secreto. La razón por la que pudo simplificarse el encabezado es que puede haber encabezados adicionales pero opcionales de extensión. Este cambio indica cuál de los seis encabezados de extensión que se tengan en ese momento, es el siguiente. Si este encabezado es el último encabezado de IP, el campo de Encabezado siguiente indica el manejador de protocolo de transporte al que se entregara el paquete.

El campo límite de saltos se usara para evitar que los paquetes vivan eternamente. Tiene la misma función que el campo TTL.

Los campos de direcciones de origen y destino utilizan 16 bytes para evitar el agotamiento futuro de direcciones IP. Este tipo de direcciones tiene una notación diferente debido a la gran cantidad de argumentos contenidos. Las direcciones se asocian en 8 grupos de 4 dígitos hexadecimales, separados los grupos por dos puntos. Por ejemplo: 001:0db8:85a3:08d3:1319:8a2e:0370:7334

Por último el campo de Suma de verificación desaparece, porque su cálculo reduce en gran medida el desempeño. Las capas de enlace de datos y de transporte tienen su propia suma de verificación, por lo cual un cálculo más de suma de verificación no tienen sentido.

3.1.3.3.3 Funciones del protocolo IP

1. Describir el costo de la mejor ruta en diversas formas de acuerdo a la métrica de enrutamiento.
2. Permitir múltiples rutas activas entre dos redes
3. Propagar información de enrutamiento exacta y eliminar rutas incorrectas.
4. Minimizar el tráfico de red debido a enrutamiento del protocolo
5. Minimizar el tráfico de las máquinas que no realizan enrutamiento
6. Minimizar picos súbitos en tráfico de la red después de cambiar una ruta
7. Escalar adecuadamente en grandes redes
8. Permitir la convergencia rápida en una topología de red después de un cambio de enrutamiento
9. Eliminar la propagación de rutas con falla en enlaces de gran distancia
10. Evitar actualización de tablas de enrutamiento en falso, mediante mecanismos de seguridad.

3.1.3.4 *Direccionamiento*

Durante el proceso de comunicación entre ordenadores el protocolo IP se encarga de direccionar la información entre los nodos de la red. Este proporciona los mecanismos para enviar los datos, pero no garantiza que lleguen de una manera correcta, es decir el protocolo IP es un protocolo no orientado a la conexión. La tarea de verificar la entrega del paquete encarga al protocolo TCP. IP forma paquetes de datos que se envían a través de internet uno de estos paquetes puede llegar a tener hasta 65,535 bytes.

Para enviar un mensaje a una computadora determinada es necesario asignar una dirección IP particular a cada ordenador que se conecta a la red. La dirección IP es un conjunto de 4 números separados por punto. Esto es así porque cada uno de los 4 números que forman la dirección es un byte. La dirección total contiene un total de 32 bits.

Al igual que una dirección tiene un formato de dos partes estándar (el nombre de la calle y el número del domicilio), cada dirección IP está dividida internamente en dos partes: un Id. de red y un Id. de host:

- El Id. de red, también conocido como dirección de red, identifica un único segmento de red dentro de un conjunto de redes (una red de redes) TCP/IP más grande. Todos los sistemas que están conectados y comparten el acceso a la misma red tienen un

Id. de red común en su dirección IP completa. Este Id. también se utiliza para identificar de forma exclusiva cada red en un conjunto de redes más grande.

- El Id. de host, también conocido como dirección de host, identifica un nodo TCP/IP (estación de trabajo, servidor, enrutador u otro dispositivo TCP/IP) dentro de cada red. El Id. de host de cada dispositivo identifica de forma exclusiva un único sistema en su propia red.

En la Figura. 3-29 muestra la dirección IP (131.107.16.200) dividida en las secciones de Id. de red y host. La parte de Id. de red (131.107) está indicada por los dos primeros números de la dirección IP. La parte de Id. de host (16.200) está indicada por los dos últimos números de la dirección IP.

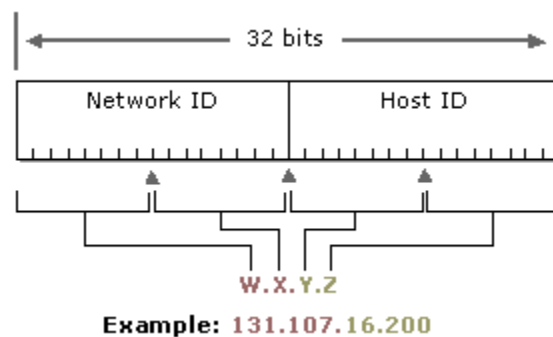


Figura. 3-29 Ejemplo de dirección IP

3.1.3.4.1 Clasificación de direcciones de red.

La comunidad de Internet ha definido cinco clases de direcciones. Las direcciones de las clases A, B y C se utilizan para la asignación a nodos TCP/IP.

La clase de dirección define los bits que se utilizan para las partes de Id. de red e Id. de host de cada dirección. La clase de dirección también define el número de redes y hosts que se pueden admitir por cada red.

La Tabla 3-4 sirve para mostrar:

- Cómo el valor del primer octeto de una dirección IP dada indica la clase de dirección.
- Cómo están divididos los octetos de una dirección en el Id. de red y el Id. de host.
- El número de redes y hosts posibles por cada red que hay disponibles para cada clase.

Tabla 3-4

Clase de direcciones. IP	Valor del primero octeto	Mascara de red	Numero de redes	Numero de host por red.
A	1 – 126	255.0.0.0	126	16,777,214
B	128 – 191	255.255.0.0	16,384	65,534
C	192 – 223	255.255.255.0	2,097,152	254
D	224 – 239	No disponible	No disponible	No disponible
E	240 – 254	No disponible	No disponible	No disponible

A su vez las direcciones IP pueden clasificarse en públicas y privadas. Las direcciones privadas se utilizan a nivel interno en las redes LAN. Las direcciones IP públicas, son únicas y no deben repetirse. Representan un enlace directo a Internet.

La IANA ha reservado tres bloques del espacio de direcciones IP uso de redes privadas. Estos bloques son (Microsoft, 2011):

- Bloque de direcciones privadas clase A, 10.0.0.0 a 10.255.255.255
- Bloque de direcciones privadas clase B, 172.16.0.0 a 172.31.255.255
- Bloque de direcciones privadas clase C, 192.168.0.0 a 192.168.255.255

Otras direcciones IP son especiales, pues se asignan o reservar para propósitos específicos. Entre estas tenemos:

- ✓ Dirección de local host: 127.0.0.0/8⁴⁶
- ✓ Direcciones de red: x.0.0.0/8
- ✓ Direcciones de broadcast: 224.0.0.0/3

3.1.3.4.2 Mascaras de red.

Los Id. de red y de host en una dirección IP se distinguen mediante una máscara de subred. Cada máscara de subred es un número de 32 bits que utiliza grupos de bits consecutivos de todo unos (1) para identificar la parte de Id. de red y todo ceros (0) para identificar la parte de Id. de host en una dirección IP.

La Tabla 3-5 se muestra la clasificación de las máscaras de red (Microsoft, 2011).

Tabla 3-5

Clase de dirección	Bits para la máscara de subred	Mascara de subred
Clase A	11111111.00000000.00000000.00000000	255.0.0.0

⁴⁶ La escritura 127.0.0.0/8 indica que se tiene una dirección IP 127.0.0.0 con una máscara de red de 8 bits.

Clase B	11111111.11111111.00000000.00000000	255.255.0.0
Clase C	11111111.11111111.11111111.00000000	255.255.255.0

Normalmente, los valores predeterminados de máscara de subred son aceptables para la mayor parte de las redes sin requisitos especiales en las que cada segmento de red IP corresponde a una única red física.

En algunos casos, puede utilizar máscaras de subred personalizadas para implementar la creación de subredes IP. Con la creación de subredes IP, se puede subdividir la parte de Id. de host predeterminada en una dirección IP para especificar subredes, que son subdivisiones del Id. de red basado en la clase original.

3.1.3.4.3 VSLM

VSLM es una técnica que permite dividir una red grande en subredes más pequeñas. Está sujeto a la regla que la dirección que se desea subdividir no sea utilizada en el momento de división por un host de la red.

VSLM permite crear las subredes de forma que estas puedan ajustarse a las necesidades reales de la red. A diferencia de la división de redes, en este método se puede adaptar el número de host de una subred de forma precisa.

Para implementar este tipo de división se requiere de routers que utilicen protocolos de enrutamiento sin clase como RIPv2 y OSPF. Estos protocolos operan con esquemas de direccionamiento de diferentes tamaños de máscaras.

3.1.3.4.3.1 Funcionamiento de VSLM

Supongamos que tenemos una red con dirección IP 10.0.0.0/8, lo cual no indica que según el sistema asignación de máscaras por clase es de tipo A. El objetivo puede ser desplegar una red en una empresa. A su vez, queremos que limitar el número máximo de usuarios que puedan conectarse a esta red y dividir la red en subredes con el propósito de utilizar una subred distinta para cada sector laboral.

A manera de ejemplo, vamos a dividir esta subred en 3 subredes de distintos tamaños. Puede darse el caso en que no se desee hacer uso de todas las direcciones IP disponibles, con el objetivo de utilizarlas posteriormente en subredes que se crearán más adelante.

La red LAN 1 tendrá un total de 20 usuario, la red LAN 2 un máximo de 35 usuarios y la red LAN 3 solamente 6 usuarios.

Comenzaremos creando la red LAN 1, esta podrá brindar servicio a un total de 20 usuarios. El número de usuario representa el número de direcciones de host que se tendrán, al cual debemos adicionarle 2 direcciones más que son las de red y broadcast. En total

tenemos 22 direcciones de red. Para este número serán necesarios 8 bits en la sección de host de la dirección IP. Si bien 2^5 es 32 es el número más cercano al número de usuarios a los que se debe brindar servicio. El exponente representa el número de bits que deben mantenerse en la sección de dirección de host.

Como podemos observar en la Figura. 3-30, la máscara de red inicial es de 8 bits de izquierda a derecha⁴⁷, lo que da un valor de máscara de 255.0.0.0. Es en esta parte donde se realiza los cambios para variar el tamaño de la máscara original. Tomaremos prestados 4 bits de la parte de dirección de host y los añadiremos a la sección de dirección de red, convirtiendo en 1 todos los 0s de la parte de dirección de host que no utilizaremos con el nuevo número de usuarios.

Dirección de red	10.0.0.0 – 00001010.00000000.00000000.00000000
Máscara de red	255.0.0.0 – 11111111. <u>00000000.00000000.00000000</u>

Estos bits serán convertidos a 1
con el objetivo de variar el tamaño
de la máscara para LAN1

Dirección de red LAN 1

10.0.0.0 – 00001010.00000000.00000000.00000000

Máscara de red LAN1

255.255.255.240 – 11111111.11111111.11111111.11100000

Los bits sobre la línea roja forma la nueva máscara de red y los bits en rojo son los bits necesarios para brindar acceso a los 20 usuarios.

Figura. 3-30 Ejemplo de VSLM

Se realiza el mismo proceso para crear la red LAN2. La Figura. 3-31 muestra que la red LAN2 inicia en 32 pues las direcciones inferiores forman parte de la red LAN1.

⁴⁷ Recuerde que las direcciones IP se integran por 4 octetos de bits, que por lo general se expresan en términos decimales, pero en este caso usaremos su notación binaria.

Dirección de red LAN 2

10.0.0.32 – 00100000.00000000.00000000.00000000

La sección marcada corresponde a la dirección de red LAN2

Máscara de red LAN2 para 35 usuarios.

255.255.255.240 – 11111111.11111111.11111111.11000000

Los bits sobre la línea roja forma la nueva máscara de red y los bits en rojo son los bits necesarios para brindar acceso a los 35 usuarios.

Figura. 3-31 División VSLM para red de 35 usuarios.

3.1.3.4.4 Mecanismo de traducción de direcciones de red.

El proceso de la **traducción de direcciones de red** (NAT, por sus siglas en inglés) se desarrolló en respuesta a la falta de direcciones de IP con el protocolo IPv4.

En efecto: en la asignación de direcciones IPv4, no hay suficientes direcciones IP enrutables (es decir, únicas en el mundo) para permitir que todas las máquinas que necesiten conectarse a internet puedan hacerlo.

El concepto de NAT consiste en utilizar una dirección IP enrutable (o un número limitado de direcciones IP) para conectar todas las máquinas a través de la traducción, en la pasarela de internet, entre la dirección interna (no enrutable) de la máquina que se desea conectar y la dirección IP de la pasarela (Ver Figura. 3-32).

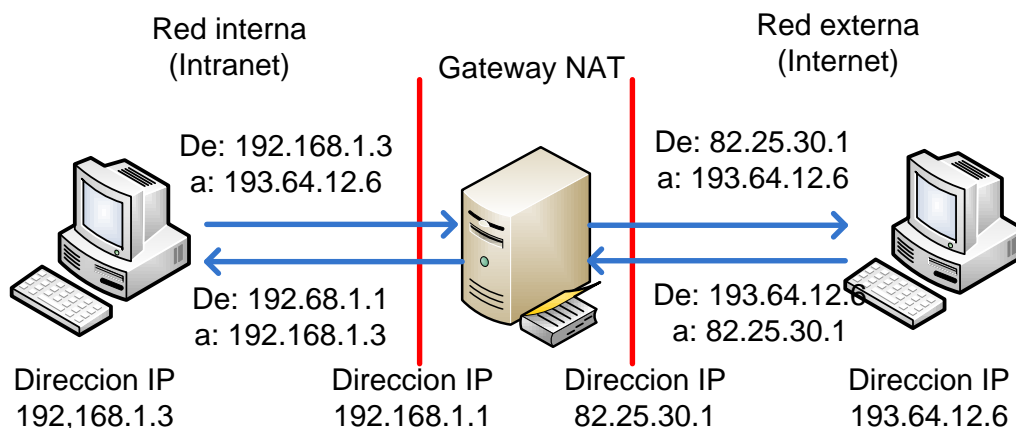


Figura. 3-32 Ejemplo de proceso NAT

Además, el proceso de traducción de direcciones permite a las compañías asegurar la red interna siempre y cuando oculte la asignación de direcciones internas. Para un observador que se ubica fuera de la red, todos los pedidos parecen provenir de la misma dirección IP.

3.1.3.4.4.1 NAT estática

El concepto de NAT estática consiste en hacer coincidir una dirección IP pública con una dirección IP de red privada interna. Un **router** (o, más precisamente, la **pasarela**) hace coincidir una dirección IP privada (por ejemplo, *192.168.0.1*) con una dirección IP pública enrutable en internet y, en cierto sentido, realiza la traducción mediante la modificación de la dirección en el paquete IP.

La traducción de las direcciones estáticas permite conectar máquinas de red interna a internet de manera transparente, aunque no resuelve el problema de escasez de direcciones debido a que se necesitan *n* direcciones IP enrutables para conectar *n* máquinas de la red interna.

3.1.3.4.4.2 NAT dinámica

La NAT dinámica permite compartir una dirección IP enrutable (o una cantidad reducida de direcciones IP enrutables) entre varias máquinas con direcciones privadas. Así, todas las máquinas de la red interna poseen la misma dirección IP virtual en forma externa. Por esta razón, el término "enmascaramiento de IP" se usa en ciertos casos para procesar la NAT dinámica.

Para poder "multiplexar" (compartir) diferentes direcciones IP con una o más direcciones IP enrutables, la NAT dinámica utiliza la traducción de direcciones de puerto, es decir, la asignación de un puerto de origen diferente para cada solicitud, de modo que se pueda mantener una correspondencia entre los pedidos que provienen de la red interna y las respuestas de las máquinas en internet, las cuales están dirigidas a la dirección IP del router.

3.1.3.5 Enrutamiento

A través del protocolo IP se encuentra el enrutamiento, proceso por el cual 2 situaciones que se comunican se encuentran y usan la mejor trayectoria (Ver Figura. 3-33) de una red TCP/IP, sin importar la complejidad. El proceso tiene algunos componentes importantes como determinar las trayectorias disponibles, seleccionar la mejor trayectoria para un propósito específico, alcanzar otros sistemas, además de modificar los formatos de los datagramas lo que permite ajustarse a una nueva tecnología.

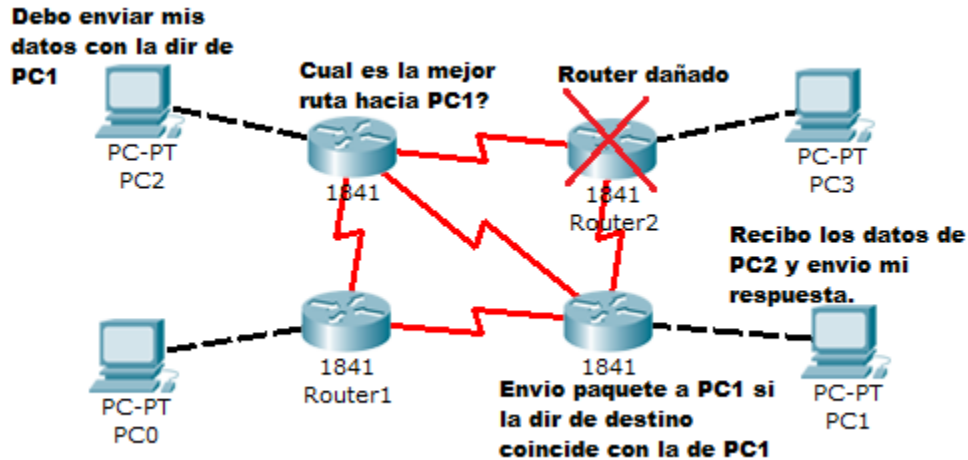


Figura. 3-33 Proceso de enrutamiento IP.

En el proceso de envío la información (Ver Figura. 3-34) esta es fragmentada en pequeñas partes (paquetes) que son enviados por separados y uno por uno. A manera de ejemplo se puede comparar el proceso de envío a una oficina de correos que envía un mueble desarmado (por partes) para que este se vuelva a armar en su destino. IP involucraría esas piezas formando paquetes y rotaría la dirección. TCP se encargaría de ponerles un número secuencial para verificar que llegaron todos y que además están en el orden correcto.

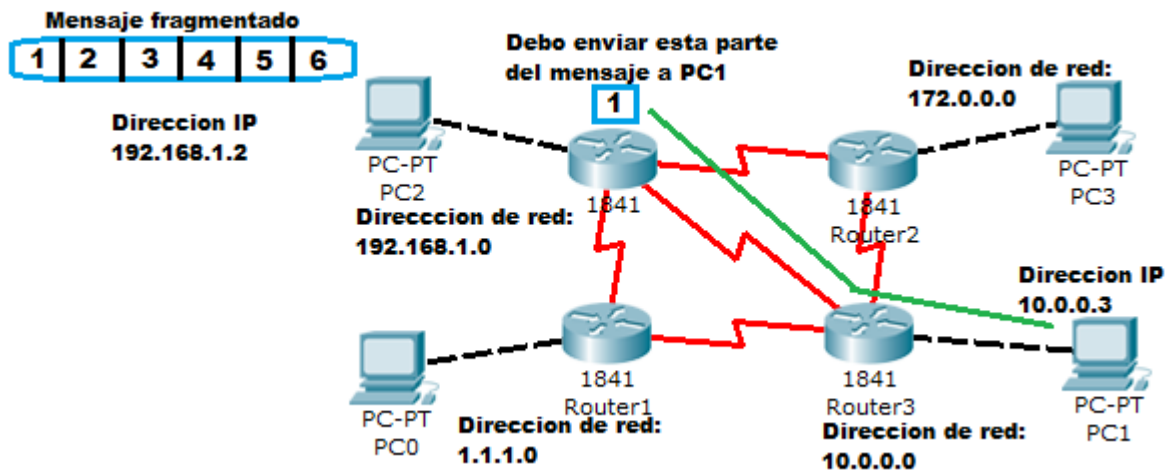


Figura. 3-34 Proceso de direccionamiento.

TCP lleva a cabo el registro del número de puerto. Esto es importante sobre todo para la presentación de servicios de red. Esto puede ser un servidor FTP.

3.1.3.5.1 Principios de enrutamiento.

Existen 3 procesos principales que se ejecutan en un sistema de enrutamiento:

- El nodo final necesita saber cómo y cuándo comunicarse con un ruteador
- EL ruteador necesita saber cuándo determinar una trayectoria adecuada a una red remota.
- El ruteador en la red de destino necesita saber cómo conectarse al nodo final.

3.1.3.5.2 Ventajas de enrutamiento

- Elección de la mejor ruta
- Ajusta tecnologías de diferente nivel de enlace
- Flexibilidad y control
- Reporte de errores

3.1.3.5.3 Tablas de enrutamiento

Todo ruteador tiene la tabla con los números de red y subred que conoce. La tabla registra cuales conexiones del ruteador pueden ser usadas para alcanzar una red en particular, así como algunos indicativos del desempeño o costo de un enlace para alcanzar una red determinada.

Los hosts TCP/IP utilizan una tabla de enrutamiento para mantener información acerca de otras redes IP y hosts IP. Las redes y los hosts se identifican mediante una dirección IP y una máscara de subred. Además, las tablas de enrutamiento son importantes ya que proporcionan la información necesaria a cada host local respecto a cómo comunicarse con redes y hosts remotos.

En cada equipo de una red IP, puede mantener una tabla de enrutamiento con una entrada para cada equipo o red que se comunica con el equipo local. En general, esto no es práctico y se utiliza una puerta de enlace predeterminada (enrutador IP) en su lugar.

Cuando un equipo se prepara para enviar un datagrama IP, inserta su propia dirección IP de origen y la dirección IP de destino del destinatario en el encabezado IP. A continuación, el equipo examina la dirección IP de destino, la compara con una tabla de enrutamiento IP mantenida localmente y realiza la acción adecuada según la información que encuentra. El equipo realiza una de las tres acciones siguientes:

- Pasa el datagrama a un nivel de protocolo superior a IP en el host local.
- Reenvía el datagrama a través de una de las interfaces de red conectadas.
- Descarta el datagrama.

IP busca en la tabla de enrutamiento la ruta que más se parezca a la dirección IP de destino. La ruta, en orden de más a menos específica, se localiza de la manera siguiente:

- Una ruta que coincida con la dirección IP de destino (ruta de host).
- Una ruta que coincida con el Id. de red de la dirección IP de destino (ruta de red).
- La ruta predeterminada.

Si no se encuentra una ruta coincidente, IP descarta el datagrama.

3.1.3.5.4 Rutas más comunes en routers.

Una red completamente aislada de otra red TCP/IP requiere solo de rutas mínimas. Las rutas mínimas son creadas por el comando `ifconfig`⁴⁸ al momento de configurar una interfaz. Las rutas mínimas son: la ruta de red local y la ruta para loopback. En sistemas como Linux (Ver Figura. 3-36) es necesario crear la interfaz y la ruta. En el caso de Windows (Ver Figura. 3-35) estas rutas están creadas por defecto.

```
IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red    Puerta de enlace  Interfaz  Métrica
0.0.0.0             0.0.0.0           192.168.71.1     192.168.71.57  20
127.0.0.0           255.0.0.0         En vínculo       127.0.0.1     306
127.0.0.1           255.255.255.255  En vínculo       127.0.0.1     306
127.255.255.255    255.255.255.255  En vínculo       127.0.0.1     306
192.168.71.0       255.255.255.0    En vínculo       192.168.71.57  276
192.168.71.57     255.255.255.255  En vínculo       192.168.71.57  276
192.168.71.255    255.255.255.255  En vínculo       192.168.71.57  276
224.0.0.0          240.0.0.0         En vínculo       127.0.0.1     306
224.0.0.0          240.0.0.0         En vínculo       192.168.71.57  276
255.255.255.255    255.255.255.255  En vínculo       127.0.0.1     306
255.255.255.255    255.255.255.255  En vínculo       192.168.71.57  276
```

Figura. 3-35 Tabla de rutas en Windows

```
# route -n

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface
150.185.162.0 0.0.0.0 255.255.255.128 U 0 0 2 eth0
127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 1 lo
```

Figura. 3-36 Tabla de enrutamiento en Linux

Una entrada es la ruta a la red 150.185.156.0 a través de eth0. La otra entrada es la ruta loopback a localhost establecida cuando lo fue creada. Observe los campos de bandera en cada entrada. Ambas entradas tienen la bandera U (Up), esto indica que la interfaz está lista para ser usada. Ninguna de las entradas tiene la bandera G (Gateway). Esta bandera indica que un gateway externo está siendo usado. La bandera G no aparece pues estas rutas son directas a través de interfaces locales y no a través de Gateway externos.

⁴⁸ Esto en el caso que se utilice Linux.

3.1.3.5.5 Principio de optimización de enrutamiento.

El principio de optimización de enrutamiento establece que si existe un enrutador X y este enrutador se encuentra en medio de la ruta óptima del enrutador Y al enrutador Z, entonces la ruta óptima de X a Z también es la misma ruta (Ver Figura. 3-37

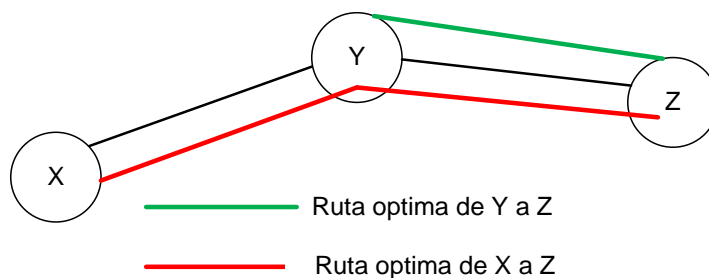


Figura. 3-37 Principio de optimización.

Si hubiera una ruta mejor de Y a Z esto afectaría directamente a la ruta establecida de X a Z, por lo cual la sección entre X y Y se mantendría pero cambiaría la sección entre Y y Z pues se ha encontrado una ruta más propicia para el envío de paquetes entre estos dos nodos.

Como consecuencia directa del principio de optimización, se observa que las rutas de óptimas de todos los orígenes a un destino dado forman un árbol con raíz en el destino. Este tipo de árbol se le conoce como **árbol sumidero**. La ventaja de este sistema es que un árbol, se comporta como una topología jerárquica por lo cual no contiene ciclos, obligando a cada paquete a recorrer un número de saltos finitos y limitados.

3.1.3.5.6 Algoritmos de enrutamiento

3.1.3.5.6.1 Enrutamiento por la ruta más corta

Existen distintas maneras de medir la longitud entre dos nodos. Algunas de ellas son: distancias geográficas, números de saltos, anchos de banda, etc. Uno de los algoritmos de búsqueda de ruta más corta es el planteado por Dijkstra (1959) (Tanenbaum, 2003).

El procedimiento plantea que cada nodo debe ser etiquetado entre paréntesis con su distancia al nodo de origen a través de la mejor ruta conocida. Inicialmente no se conocen las distancias entre los nodos, por ende sus marcas se deben colocar en infinito. A medida que avanza el proceso de etiquetado, las rutas se revelan, por lo que las etiquetas pueden cambiar reflejando mejores rutas a un nodo.

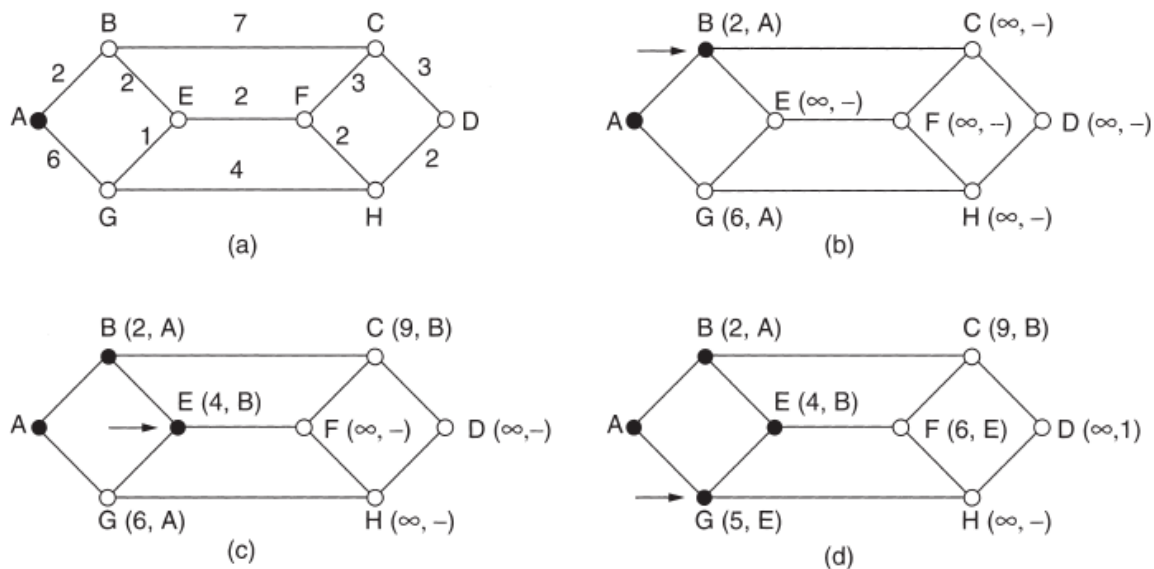


Figura. 3-38 Pasos del algoritmo de ruta más corta.

La Figura. 3-38 muestra un ejemplo en donde se pretende encontrar la ruta más corta desde el punto A hasta el punto D.

Pasos:

1. Marque el nodo inicial (en este caso A) como permanente.
2. Etiquete cada uno de los nodos cercanos al nodo A en función del número de saltos que deben llevarse a cabo hasta llegar al nodo en evaluación.
3. Se evalúan cada uno de los nodos etiquetados. Es decir para llegar al nodo E desde A existen 2 rutas ABE y AGE, sin embargo el número de saltos que deben ser realizados es menor al cruzar ABE. Lo que indica que hasta el momento es la ruta más corta.
4. De igual forma la ruta de A hasta G es evaluada, dando como resultado una mejor ruta cruzando ABEG.
5. Una vez fijados los nodos cercanos se procede a evaluar los nodos distantes desde los nodos cercanos al nodo A. Es decir, se utilizaran los puntos B, E y G como nodos permanentes así como lo fue A en la etapa anterior. Esto se realiza hasta que todas las rutas posibles a D han sido evaluadas y seleccionada la más corta.

3.1.3.5.6.2 Enrutamiento por inundación

En este algoritmo si un nodo recibe un paquete de datos debe reenviarlo a todos sus vecinos, excepto a aquel router vecino que envió el paquete. El algoritmo resulta ser muy sencillo y garantiza cierto grado de confiabilidad en la entrega del paquete, es posible incluso que múltiples copias lleguen a la red de destino.

Tiene la ventaja de no necesitar información sobre la red para funcionar por lo tanto el tráfico de paquetes de control entre routers es casi nulo. Sin embargo, puede que un paquete sea recibido en múltiples ocasiones por lo cual es necesario colocar un número de secuencia.

Un inconveniente que sobresale en este tipo de enrutamiento es la creación de ciclos de tráfico infinito. Estos pueden ser limitados al guardar un registro de los mensajes que ya han sido enviados y cuáles no.

Si bien guardar un registro de los paquetes enviado resulta una buena solución, también presenta una carga para el router pues esto consume espacio en memoria. Es por ello recordar la importancia del campo TTL de forma que el paquete eventualmente sea eliminado de la red, si este cruza un número determinado de saltos.

3.1.3.5.6.3 Enrutamiento por difusión

En algunas situaciones los usuarios necesitan enviar mensajes a varias computadoras o incluso a todas en una red. Ejemplo de estos son los servicios de noticias o radios online. El envío simultáneo de un paquete como se plantea, se le conoce como difusión.

Una de las formas para lograr este objetivo es que el origen o transmisor envíe un paquete distinto a todos los destinos, es decir, tantos paquetes como el número de usuario a los que desea transmitir la información. Esto se llevara a cabo cambiando las direcciones de destino en los paquetes por las direcciones de los usuarios receptores.

El problema de esta práctica es que se desperdicia el ancho de banda de la red y a su vez, el método demanda que el origen tenga una lista de todos los usuarios que reciben la transmisión. Anteriormente se planteó otro algoritmo conocido como **Inundación** pero que tiene la particularidad de difundir los paquetes en todos los sentidos. Por lo tanto, si se llegara a dar la situación de que el receptor se ha reducido a 1(en el peor de los casos) se estaría desperdiciando ancho de banda.

3.1.3.5.6.4 Enrutamiento por multidifusión

En este método, cada paquete contiene una lista de destinos o un mapa de bits que indica los destinos deseados. Cuando un paquete llega al enrutador, éste revisa todos los destinos para determinar el grupo de líneas de salida que necesitará.

El enrutador genera una copia nueva del paquete para cada línea de salida que se utilizará, e incluye en cada paquete sólo aquellos destinos que utilizarán la línea. En efecto, el grupo de destinos se divide entre las líneas de salida. Después de una cantidad suficiente de saltos, cada paquete llevará sólo un destino, así que puede tratarse como un paquete normal. El enrutamiento multidestino es como los paquetes con direccionamiento individual, excepto que, cuando varios paquetes deben seguir la misma ruta, uno de ellos paga la tarifa completa y los demás viajan gratis.

Para realizar enrutamiento de multidifusión, cada enrutador calcula un árbol de expansión que cubre a todos los demás enrutadores de la subred.

En la figura se muestra una subred con dos grupos para difusión. Algunos de los routers de la red están conectados a computadoras que pertenecen a ambos grupos. La Figura. 3-39 presenta 2 árboles de expansión para el router de la izquierda. Al ser enviado un paquete de multidifusión el router es el encargado de examinar su árbol de sumidero y recortarlo, eliminando aquellas líneas que se conecten a host que no pertenezcan al grupo (Ver Figura. 3-39 (c)).

De la misma manera, en la Figura. 3-39 (d) se presenta el árbol de expansión recortado del grupo 2. Los paquetes de multidifusión se reenvían sólo a través del árbol de expansión apropiado.

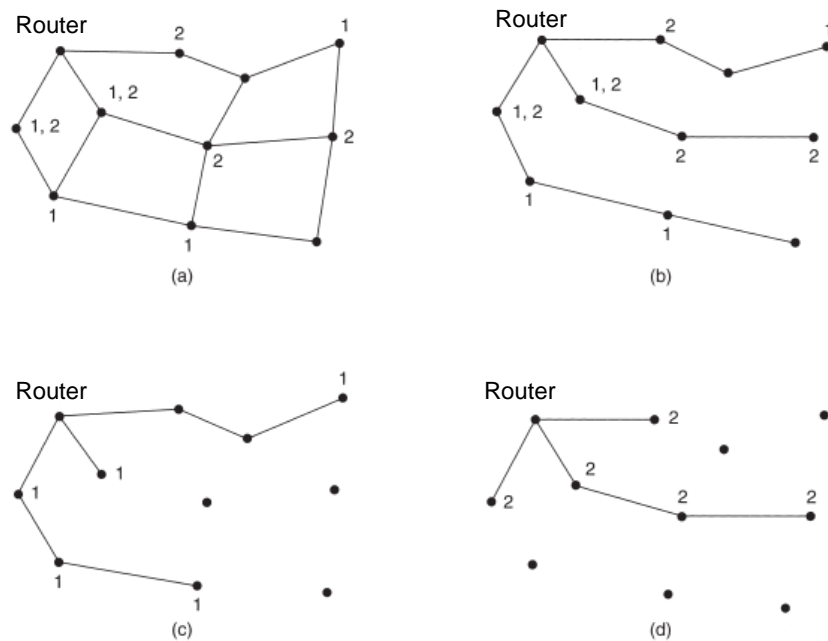


Figura. 3-39 Árboles de expansión o sumidero

3.1.3.6 Protocolo de enrutamiento OSPF

OSPF son las siglas de Open Shortest Path First, o bien Abrir primero la ruta más corta es un protocolo de enrutamiento jerárquico de pasarela interior (IGP), que emplea el algoritmo de Dijkstra de enlace estado para calcular la ruta más corta posible.

Se mencionaba en la sección de algoritmos por rutas más corta que la métrica de distancia podía variar. En este caso, la métrica de ruta más corta está dada por el “*costo*”. El protocolo permite construir una base de datos de enlace – estado idéntica en todos los enrutadores de la zona.

OSPF es probablemente el tipo de protocolo IGP más utilizado en grandes redes. Puede operar con seguridad usando MD5 para autenticar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. Como sucesor natural de RIP, acepta VLSM o sin clases CIDR desde su inicio.

Existen nuevas versiones como OSPFv3 que soportan protocolos de red nuevos como IPv6 o las extensiones multidifusión para OSPF (MOSPF). El protocolo OSPF puede “etiquetar” rutas y propagar esas etiquetas por otras rutas.

Las redes OSPF tiene la particularidad de descomponerse en regiones o bien áreas mas pequeñas. Existen áreas especiales llamadas áreas de backbone que forman la parte central de al red. Es aquí donde se interconectan las otras áreas de la red.

Las rutas entre diferentes áreas de la red circulan siempre en el backbone, por consiguiente todas las áreas están conectadas al backbone. En algunos casos no es posible realizar una conexión directa al backbone por lo que es necesario realizar un enlace virtual entre redes.

En este tipo de redes, los router en el mismo dominio de multidifucion forman enlaces cuando se descubren los unos a los otros. En un segmento de red Ehternet los routers eligen a un “encaminador” designado primero y secundario. El secundario actua como concentrador para reducir el tráfico entre los diferentes encaminadores.

OSPF puede usar tanto multidifusión como unidifusión para enviar paquetes de bienvenida y actualizaciones de enlace – estado. Las direcciones multidifusión usadas son 224.0.0.5 y 224.0.0.6. Al contrario de otros protocolos como RIP o BGP, OSPF no usa ni TCP ni UDP, sino que usa IP directamente, mediante el protocolo IP 89.

OSPF mantiene siempre actualizada la capacidad de enrutamiento entre los nodos de una red mediante la difusión de la topología de red y la información de estado – enlace

de sus distintos nodos. Esta difusión se puede llevar a cabo a través de varios tipos de paquetes como son (Wikipedia, 2011):

- Paquetes Hello (tipo 1). Cada router envía periódicamente a sus vecinos un paquete que contiene el listado de vecinos reconocidos por el router, indicando el tipo de relación que mantiene con cada uno.
- Paquetes de descripción de base de datos estado-enlace (DataBase Description, DBD) (tipo 2). Se emplean en el intercambio de base de datos enlace-estado entre dos nodos, y permiten informar al otro nodo implicado en la sincronización acerca de los registros contenidos en la LSDB propia, mediante un resumen de estos.
- Paquetes de estado-enlace o Link State Advertisements (LSA). Los cambios en el estado de los enlaces de un router son notificados a la red mediante el envío de mensajes LSA. Dependiendo del estatus del router y el tipo de información transmitido en el LSA, se distinguen varios formatos (entre paréntesis, las versiones de OSPF en que se utilizan):
 - (OSPFv2 y v3) Router-LSA o LSA de encaminador.
 - (OSPFv2 y v3) Network-LSA o LSA de red.
 - (OSPFv2 y v3) Summary-LSA o LSA de resumen. En OSPFv2 se distinguen dos tipos: tipo 3, dirigidos a un router fronterizo de red; y tipo 4, dirigidos a una subred interna. En OSPFv3, los Summary-LSA tipo 3 son renombrados como Inter-Area-Prefix-LSA, y los tipo 4 pasan a denominarse Intra-Area-Prefix-LSA.
 - (OSPFv2 y v3) AS-External-LSA o LSA de rutas externas a la red.
 - (OSPFv3) Link-LSA o LSA de enlace, que no se retransmite más allá del link del origen.

3.1.3.6.1.1 Tipos de router OSPF

Los router de OSPF clásicos son capaces de enrutar cualquier paquete destinado a cualquier punto del área en el que se encuentra. Para el enrutamiento entre distintas áreas de la red y e incluso fuera del área, OSPF utiliza routers especiales que mantienen una información topológica más completa que la del área en la se sitúan.

Se mencionan 2 tipos de router fundamentales que son:

- Routers fronterizos de área o ABRs (Area Border Routers), que mantienen la información topológica de su área y conectan ésta con el resto de áreas, permitiendo enrutar paquetes a cualquier punto de la red (inter-area routing).
- Routers fronterizos del AS o ASBRs (Autonomous System Border Routers), que permiten encaminar paquetes fuera del AS en que se alojen, es decir, a otras redes conectadas al Sistema Autónomo o resto de Internet (external routing).

Un paquete que se ha generado en la red, deberá ser enviado de forma jerárquica, a través del área si su destino es conocido por el emisor; al ABR del área correspondiente si el destino se encuentra cruzando distintas áreas de la red. Luego este deberá enviarlo al router del área de destino, si este se encuentra en el AS, o al ASBR si la destinación del paquete es exterior a la red.

3.1.3.6.1.2 Áreas de red OSPF

Área Backbone

El backbone, también denominado área cero, forma el núcleo de una red OSPF. Es la única área que debe estar presente en cualquier red OSPF, y mantiene conexión, física o lógica, con todas las demás áreas en que esté particionada la red. La conexión entre un área y el backbone se realiza mediante los ABR, que son responsables de la gestión de las rutas no-internas del área (esto es, de las rutas entre el área y el resto de la red).

Área stub

Un área stub es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron inyectadas en OSPF desde otro protocolo de enrutamiento. Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento.

Área not-so-stubby

También conocidas como NSSA, constituyen un tipo de área stub que puede importar rutas externas de sistemas autónomos y enviarlas al backbone, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas.

3.1.3.7 Protocolos externos de pasarela

Los protocolos de enrutamiento exterior fueron creados para controlar la expansión de las tablas de enrutamiento y para proporcionar una vista más estructurada de Internet mediante la división de dominios de enrutamiento en administraciones separadas, llamadas **Sistemas Autónomos (SA)**, los cuales tienen cada uno sus propias políticas de enrutamiento. Durante los primeros días de Internet, se utilizaba el protocolo **EGP** (no confundirlo con los protocolos de enrutamiento exterior en general). NSFNET utilizaba EGP para intercambiar información de accesibilidad entre el backbone y las redes regionales. Actualmente, **BGP-4** es el estándar de hecho para el enrutamiento entre dominios en Internet.

3.1.3.8 Protocolo de Gateway externo- BGP

Es un protocolo de enrutamiento por vector de distancia usado comúnmente para enrutar paquetes entre dominios, estándar en Internet. BGP gestiona el enrutamiento entre dos o más routers que sirven como routers fronterizos para determinados Sistemas Autónomos. BGP versión 4 (BGP-4), es el protocolo de enrutamiento entre dominios elegido en Internet, en parte porque administra eficientemente la agregación y la propagación de rutas entre dominios. Aunque BGP-4 es un protocolo de enrutamiento exterior, también puede utilizarse dentro de un conjunto de redes (SA⁴⁹) como un conducto para intercambiar actualizaciones BGP. Las conexiones BGP dentro de un SA son denominadas BGP interno⁵⁰, mientras que las conexiones BGP entre routers fronterizos (distintos SA) son denominadas BGP externo⁵¹. BGP-1, 2 y 3 están obsoletos. Para la configuración de OSPF se requiere un número de Sistema Autónomo, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. BGP se especifica en las RFC 1163, 1267 y 1771, que definen las versiones 2, 3 y 4 de BGP, respectivamente.

Los routers BGP se configuran con la información del vecino a fin de que puedan formar una conexión TCP fiable sobre la que transportar información de la ruta de acceso del sistema autónomo y la ruta de la red. Tras establecer una sesión BGP entre vecinos, ésta sigue abierta a menos que se cierre específicamente o que haya un fallo en el enlace. Si dos routers vecinos intercambian información de ruta y sesiones BGP, se dice que son iguales BGP. En principio, los iguales BGP intercambian todo el contenido de las tablas de enrutamiento BGP. Posteriormente, sólo se envían actualizaciones incrementales entre los iguales para avisarles de las rutas nuevas o eliminadas.

Todas las rutas BGP guardan el último número de versión de la tabla que se ha publicado a sus iguales, así como su propia versión interna de la tabla. Cuando se recibe un cambio en un igual, la versión interna se incrementa y se compara con las versiones de los

⁴⁹ SA = Sistemas autónomos. Es un conjunto de redes, o de routers, que tienen una única política de enrutamiento y que se ejecuta bajo una administración común.

⁵⁰ IBGP = Internal BGP – BGP interno

⁵¹ EBGp = External BGP – BGP externo

iguales, para asegurar que todos los iguales se mantienen sincronizados. BGP también guarda una tabla de rutas BGP independiente que contiene todas las rutas de acceso posibles a las redes publicadas.

Los iguales BGP se dividen en dos categorías: Los iguales BGP de distintos sistemas autónomos que intercambian información de enrutamiento son iguales BGP externos (EBGP). Los iguales BGP del mismo sistema autónomo que intercambian información de enrutamiento son iguales BGP internos (IBGP).

La selección de ruta óptima BGP se basa en la longitud de la ruta de acceso del sistema autónomo para una ruta de red. La longitud se define como el número de sistemas autónomos distintos necesarios para acceder a la red. Cuanto menor sea la distancia, más apetecible será la ruta de acceso. A través del uso de controles administrativos, BGP es uno de los protocolos de enrutamiento más flexibles y totalmente configurables disponibles.

Un uso típico de BGP, para una red conectada a Internet a través de varios ISP, es el uso de EBGP con los ISP, así como el uso de IBGP en la red interna, para así ofrecer una óptima selección de rutas. Las redes conocidas de otros sistemas autónomos a través de EBGP se intercambiarán entre los iguales IBGP. Si sólo hubiera un ISP, valdría con utilizar una ruta resumen o predeterminada para la salida a internet.

Tenga en cuenta que los routers BGP publican las rutas conocidas de un igual BGP a todos sus otros iguales BGP. Por ejemplo, las rutas conocidas a través de EBGP con un ISP se volverán a publicar a los iguales IBGP, que a su vez volverán a publicarlos a otros ISP a través de EBGP. Mediante la publicación reiterada de rutas, la red puede pasar a ser una red de tránsito entre los proveedores con los que se conecte. BGP puede parametrizarse tanto para que la red interna actúe como una red de tránsito, como para que no.

3.1.4 Capa de Transporte

3.1.4.1 Protocolos orientados a la conexión

Un protocolo orientado a conexión funciona como un proceso implementado al servicio telefónico. Este proceso involucra 3 aspectos:

- Establecer la conexión
- Transferencia de los datos
- Finalizar la conexión.

Estos 3 aspectos incluyen 2 formas de comunicación asociada y, en ellas mismas el servicio de transferencia de datos. El intercambio de mensajes implementa un procedimiento llamado *handshake*, que por lo general está ubicado en el protocolo del proceso de desarrollo de cada una de las terminales de la red.

El utilizar un protocolo orientado a la conexión, en algunos casos para la transferencia de archivos solamente es necesaria la transferencia de un par de

comunicaciones asociadas al protocolo de conexión, ya que el receptor solo necesita para ser completamente identificado el tiempo que tarda en ser establecida la conexión.

Los protocolos orientados a la conexión son frecuentemente descritos como un servicio fiable y secuencial en la transferencia de datos. La conexión puede ser deshabilitada en cualquier tiempo por otra de las partes involucradas en la comunicación o por el mismo protocolo.

3.1.4.2 Protocolo no orientado a la conexión

Este tipo de protocolo puede asemejarse más a un sistemas postal, porque al igual que este el proceso de envío de un paquete es en un sentido. Esto quiere decir que no existe la confirmación o verificación de entrega que se envía al transmisor una vez que el receptor recibe el paquete. Con un protocolo no orientado a la conexión, la comunicación toma el lugar de una fase simple pues no se debe establecer una conexión lógica entre el transmisor y receptor. EL proceso de usuario toma un mensaje para implementar el proceso del protocolo e identificar el destino del proceso en el mensaje enviado.

Al utilizar este tipo de protocolo se implementa el servicio de datagramas. Este tipo de protocolo no presenta un servicio confiable.

3.1.4.3 Protocolo TCP y UDP

3.1.4.3.1 Introducción

El protocolo de control de transmisión es uno de los principales protocolos de la suite de protocolos de internet. TCP provee el servicio de intercambio de archivos entre las redes. En particular, TCP garantiza la entrega de las tramas de datos en forma ordenada a los programas que se ejecutan en los host de red. El protocolo sirve como soporte como la mayoría de las aplicaciones de internet tal como los buscadores www, e-mail y transferencia de archivos. Otras aplicaciones que no requieren de un servicio confiable para la transmisión de sus datos, pueden utilizar el protocolo conocido como UDP o protocolo de datagramas el cual provee el servicio de datagramas que se enfoca en la reducción de la latencia de seguridad.

3.1.4.3.2 Estructura del encabezado TCP.

La Figura. 3-40 muestra los campos del encabezado TCP de un paquete (Wikipedia, 2010).

+	Bits 0 - 3	4 - 7	8 - 15	16 - 31
0	Puerto Origen			Puerto Destino
32	Número de Secuencia			
64	Número de Acuse de Recibo (ACK)			
96	longitud cabecera TCP	Reservado	Flags	Ventana
128	Suma de Verificación (Checksum)			Puntero Urgente
160	Opciones + Relleno (opcional)			
224	Datos			

Figura. 3-40 Campos del encabezado TCP

- ▶ Puerto de origen (16 bits): Identifica el puerto a través del que se envía.
- ▶ Puerto destino (16 bits): Identifica el puerto del receptor.
- ▶ Número de secuencia (32 bits): Sirve para comprobar que ningún segmento se ha perdido, y que llegan en el orden correcto. Su significado varía dependiendo del valor de SYN:
 - ▶ Si el flag SYN está activo (1), entonces este campo indica el número inicial de secuencia (con lo cual el número de secuencia del primer byte de datos será este número de secuencia más uno).
 - ▶ Si el flag SYN no está activo (0), entonces este campo indica el número de secuencia del primer byte de datos.
- ▶ Número de acuse de recibo (ACK) (32 bits): Si el flag ACK está puesto a activo, entonces en este campo contiene el número de secuencia del siguiente paquete que el receptor espera recibir.
- ▶ Longitud de la cabecera TCP (4 bits): Especifica el tamaño de la cabecera TCP en palabras de 32-bits. El tamaño mínimo es de 5 palabras, y el máximo es de 15 palabras (lo cual equivale a un tamaño mínimo de 20 bytes y a un máximo de 60 bytes). En inglés el campo se denomina “Data offset”, que literalmente sería algo así como “desplazamiento hasta los datos”, ya que indica cuántos bytes hay entre el inicio del paquete TCP y el inicio de los datos.
- ▶ Reservado (4 bits): Bits reservados para uso futuro, deberían ser puestos a cero.
- ▶ Bits de control (flags) (8 bits): Son 8 flags o banderas. Cada una indica “activa” con un 1 o “inactiva” con un 0.
 - CWR o “Congestion Window Reduced”
 - ECE o “ECN-Echo” (1 bit)
 - URG o “urgent” (1 bit)
 - ACK o “acknowledge” (1 bit)
 - PSH o “push” (1 bit)
 - RST o “reset” (1 bit)
 - SYN o “synchronize” (1 bit)
 - FIN (1 bit)

3.1.4.3.3 ¿Cómo funciona TCP?

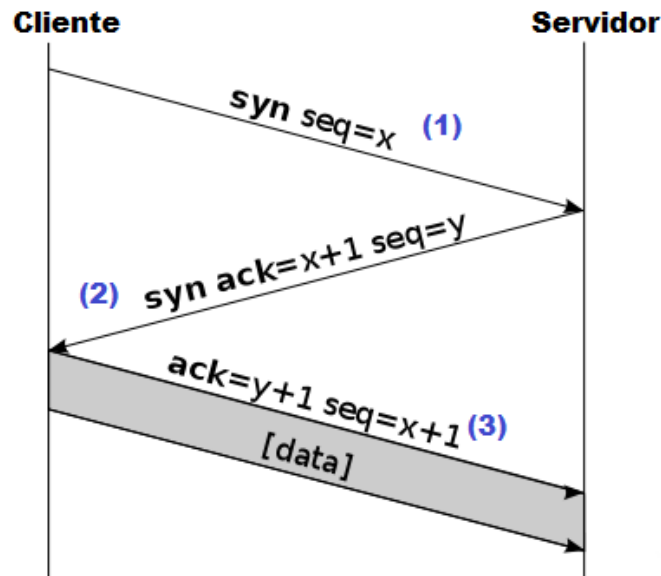


Figura. 3-41 Establecimiento de una sesión TCP.

La Figura. 3-41 muestra el proceso que lleva a cabo para el establecimiento o inicio de transmisión de datos utilizando el protocolo TCP. En este caso el cliente envía un mensaje SYN con un valor de secuencia X para indicar el inicio de envío de paquete. Luego el servidor responde ante esta petición con un mensaje SYN ACK, este mensaje debe contener el valor de secuencia inicial incrementado en 1 y a la vez el servidor envía su propio valor de secuencia. Finalmente, el cliente responde enviando una respuesta ACK que contiene el valor de secuencia enviado por el servidor y un valor de secuencia SEQ que es igual al valor de secuencia inicial incrementada en 2.

Una vez que estos mensaje han sido enviados se procede a enviar los paquetes de datos al servidor.

3.1.4.3.4 Liberación de una conexión TCP

Las conexiones TCP son dúplex total, para entender la manera en que se liberan las conexiones es mejor visualizarlas como un par de conexiones simplex. Cada conexión simplex se libera independientemente de su igual. Para liberar una conexión, cualquiera de las partes puede enviar un segmento TCP con el bit *FIN* establecido, lo que significa que no tiene más datos por transmitir. Al confirmarse la recepción del *FIN*, ese sentido se apaga. Sin embargo, puede continuar un flujo de datos indefinido en el otro sentido. Cuando ambos sentidos se han apagado, se libera la conexión. Normalmente se requieren cuatro segmentos TCP para liberar una conexión, un *FIN* y un *ACK* para cada sentido. Sin embargo, es posible que el primer *ACK* y el segundo *FIN* estén contenidos en el mismo segmento, reduciendo la cuenta total a tres.

Al igual que con las llamadas telefónicas en las que ambas partes dicen adiós y cuelgan el teléfono simultáneamente, ambos extremos de una conexión TCP pueden enviar segmentos *FIN* al mismo tiempo. La recepción de ambos se confirma de la manera normal, y se apaga la conexión.

De hecho, en esencia no hay diferencia entre la liberación secuencial o simultánea por parte de los *hosts*. Para evitar el problema de los dos ejércitos, se usan temporizadores. Si no llega una respuesta a un *FIN* en un máximo de dos tiempos de vida de paquete, el emisor del *FIN* libera la conexión. Tarde o temprano el otro lado notará que, al parecer, ya nadie lo está escuchando, y también expirará su temporizador.

Aunque esta solución no es perfecta, dado el hecho de que teóricamente es imposible una solución perfecta tendremos que conformarnos con ella. En la práctica, pocas veces ocurren problemas.

3.1.4.3.5 Transmisión de datos utilizando TCP

TCP permite enviar datos utilizando “ventanas”, estas ventanas representan el número de bytes que pueden ser enviados de forma consecutiva desde el transmisor al receptor. La administración de ventanas en el TCP no está vinculada directamente a las confirmaciones de recepción como en la mayoría de los protocolos de enlace de datos.

Por ejemplo, suponga que el receptor tiene un búfer de 4096 bytes, como se muestra en la Figura. 3-42. Si el emisor envía un segmento de 2048 bytes que se recibe correctamente, el receptor enviará la confirmación de recepción del segmento. Sin embargo, dado que ahora sólo tiene 2048 bytes de espacio de búfer (hasta que la aplicación retire algunos datos de éste), anunciará una ventana de 2048 comenzando con el siguiente byte esperado (Tanenbaum, 2003).

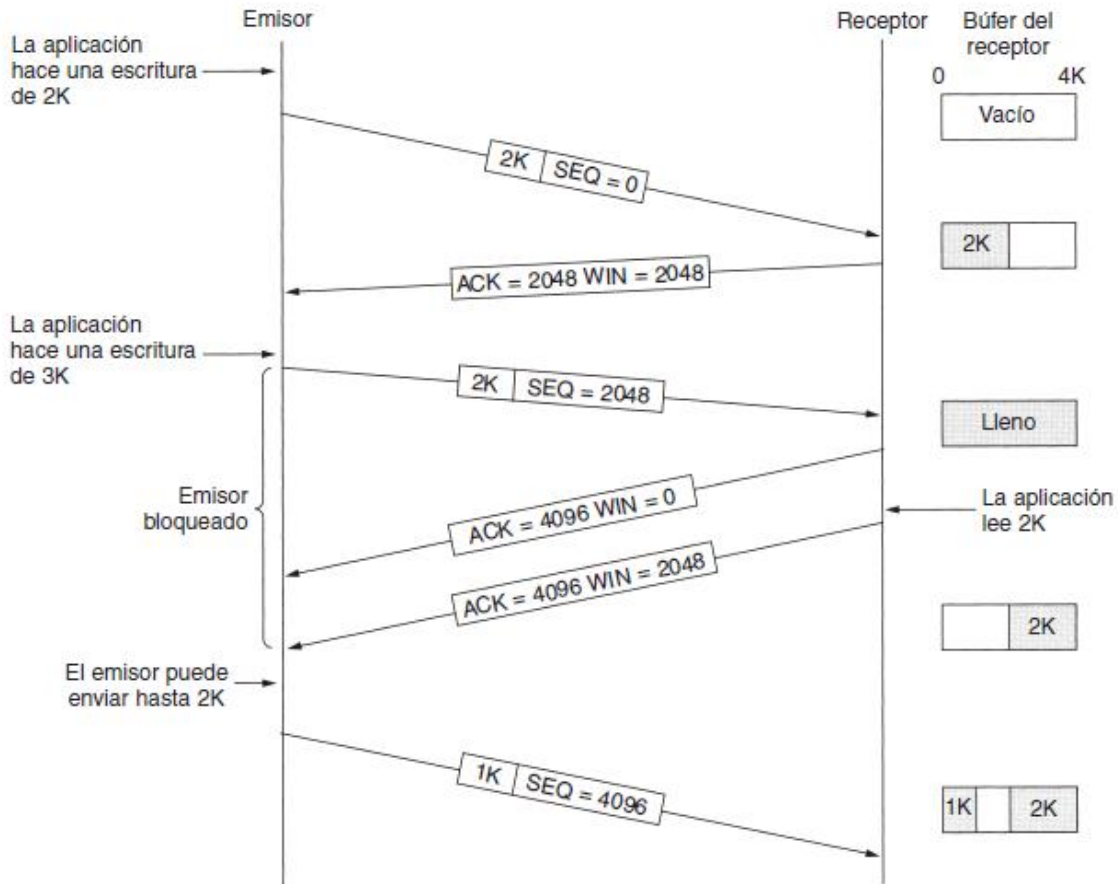


Figura. 3-42 Administración de ventanas de transmisión en TCP

Ahora el emisor envía otros 2048 bytes, para los cuales el receptor envía la confirmación de recepción, pero la ventana anunciada es de 0. El emisor debe detenerse hasta que el proceso de aplicación del *host* receptor retire algunos datos del búfer, en cuyo momento el TCP puede anunciar una ventana más grande.

Cuando la ventana es de 0, el emisor normalmente no puede enviar segmentos, salvo en dos situaciones. Primera, pueden enviarse datos urgentes (por ejemplo, para permitir que el usuario elimine el proceso en ejecución en la máquina remota). Segunda, el emisor puede enviar un segmento de 1 byte para hacer que el receptor reanuncie el siguiente byte esperado y el tamaño de la ventana. El estándar TCP proporciona explícitamente esta opción para evitar un bloqueo irreversible si llega a perderse un anuncio de ventana.

3.1.4.3.6 Retransmisión de datos utilizando TCP

El TCP usa varios temporizadores (al menos conceptualmente) para hacer su trabajo. El más importante de éstos es el temporizador de retransmisión. Al enviarse un segmento, se inicia un temporizador de retransmisiones. Si la confirmación de recepción del segmento llega antes de expirar el temporizador, éste se detiene. Si, por otra parte, el temporizador termina antes de llegar la confirmación de recepción, se retransmite el segmento (y se inicia nuevamente el temporizador).

3.1.4.3.7 Reensamblaje de segmentos con TCP.

En una red, siempre se producirán pérdidas ocasionales de datos. Por lo tanto, TCP cuenta con métodos para gestionar dichas pérdidas de segmentos. Un servicio de host de destino que utiliza TCP, por lo general sólo reconoce datos para secuencias de bytes contiguas. Si uno o más segmentos se pierden, sólo se acusa recibo de los datos de los segmentos que completan el stream. Por ejemplo, si se reciben los segmentos con los números de secuencia desde 0 a 1023 y de 2048 a 3071, el número de acuse de recibo será 1024. Esto sucede porque existen segmentos con números de secuencia de 1024 a 2047 que no se recibieron (Tanenbaum, 2003). Cuando TCP en el host de origen no recibe un acuse de recibo pasado un tiempo predeterminado, volverá al último número de acuse de recibo que recibió y retransmitirá los datos a partir de éste.

3.1.4.3.8 Control de congestión utilizando TCP

Cuando la carga ofrecida a cualquier red es mayor que la que puede manejar, se genera una congestión. Internet no es ninguna excepción. El primer paso del manejo de la congestión es su detección. La expiración de un temporizador causada por un paquete perdido podía deberse a el ruido en la línea de transmisión o al descarte de paquetes en el enrutador congestionado.

TCP también provee mecanismos para el control del flujo. El control del flujo contribuye con la confiabilidad de la transmisión TCP ajustando la tasa efectiva de flujo de datos entre los dos servicios de la sesión. Cuando el origen advierte que se recibió la cantidad de datos especificados en los segmentos, puede continuar enviando más datos para esta sesión.

El campo *Tamaño* de la ventana en el encabezado TCP especifica la cantidad de datos que puede transmitirse antes de que se reciba el acuse de recibo. El tamaño de la ventana inicial se determina durante el comienzo de la sesión a través del enlace de tres vías. El mecanismo de retroalimentación de TCP ajusta la tasa de transmisión de datos efectiva al flujo máximo que la red y el dispositivo de destino pueden soportar sin sufrir

pérdidas. TCP intenta gestionar la tasa de transmisión de manera que todos los datos se reciban y se reduzcan las retransmisiones.

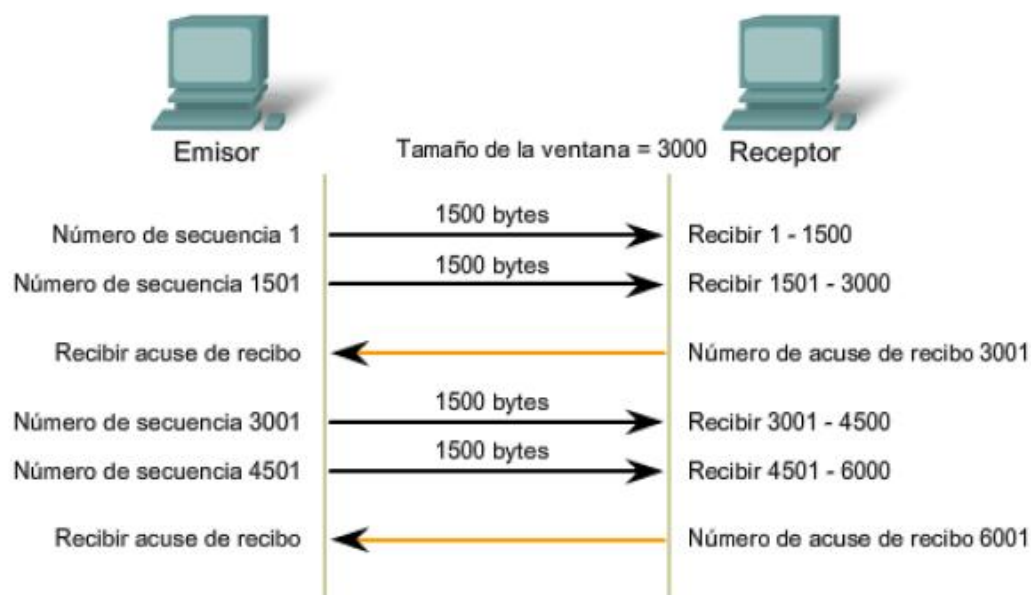


Figura. 3-43 Tamaño de ventana de una sesión TCP

En la Figura. 3-43 se utiliza un tamaño de la ventana inicial de 3000 bytes. Cuando el emisor transmite 3000 bytes, espera por un acuse de recibo de los mismos antes de transmitir más segmentos para esta sesión. Una vez que el emisor ha recibido este acuse de recibo del receptor, ya puede transmitir 3000 bytes adicionales (CISCO, 2008).

3.1.4.3.9 Reducción de la ventana

Controlar el flujo de datos es utilizar tamaños dinámicos de ventana. Cuando los recursos de la red son limitados, TCP puede reducir el tamaño de la ventana para lograr que los segmentos recibidos sean reconocidos con mayor frecuencia. Esto disminuye de manera efectiva la tasa de transmisión, ya que el origen espera que los datos sean recibidos con más frecuencia. El host receptor TCP envía el valor del tamaño de la ventana al TCP emisor para indicar el número de bytes que está preparado para recibir como parte de la sesión. Si el destino necesita disminuir la tasa de comunicación debido a limitaciones de memoria del búfer o por pérdidas de paquetes en el medio, puede enviar un valor de tamaño de la ventana menor al origen como parte de un acuse de recibo. Este proceso se mencionó en la sección de *transmisión de datos utilizando TCP*.

Después de períodos de transmisión sin pérdidas de datos o recursos limitados, el receptor comenzará a aumentar el tamaño de la ventana. Esto reduce la sobrecarga de la red, ya que se requiere enviar menos acuses de recibo. El tamaño de la ventana continuará

aumentando hasta que haya pérdida de datos, lo que producirá una disminución del tamaño de la ventana.

Estas disminuciones y aumentos dinámicos del tamaño de la ventana representan un proceso continuo en TCP, que determina el tamaño de la ventana óptimo para cada sesión TCP. En redes altamente eficientes, los tamaños de la ventana pueden ser muy grandes porque no se pierden datos. En redes donde se está estresando la infraestructura subyacente, el tamaño de la ventana probablemente permanecerá pequeño.

3.1.4.3.10 Introducción a UDP

Este protocolo proporciona una forma para que las aplicaciones envíen datagramas IP encapsulados sin tener que establecer una conexión a diferencia de TCP que si necesita de estas.

UDP no realiza control de flujo, control de errores o retransmisión cuando se recibe un segmento erróneo. Todo lo anterior le corresponde a los procesos de usuario. Por otro lado, UDP si proporciona una interfaz al protocolo IP con la característica agregada de desmultiplexar varios procesos utilizando puertos.

UDP es especialmente útil en los servicios cliente – servidor. Un cliente puede enviar una solicitud corta al servidor y esperar una respuesta corta. Si se pierde la solicitud o la respuesta, el cliente simplemente puede terminar y probar nuevamente.

Una aplicación que utiliza de esta manera el protocolo UDP es *El sistema de Nombre de Dominio*. Un programa que necesita buscar la dirección IP de algún host, por ejemplo, www.facebook.com, pueden enviar al servidor DNS un paquete UDP que contenga el nombre de dicho host. El servidor responde con un paquete UDP que contiene la dirección IP del host. Este servicio no requiere de configuración por adelantado ni tampoco liberación posterior, simplemente son dos mensajes viajando a través de la red.

3.1.4.3.11 Estructura del encabezado UDP

UDP no garantiza a los protocolos de capa superior la entrega del mensaje. El protocolo no retiene algún estado sobre el mensaje UDP enviado como confirmación de entrega o secuencias. Por esta razón, UDP es algunas veces conceptualizado como un protocolo de datagramas no confiable.

UDP permite realizar una multiplicación y verificar la integridad del encabezado de trama y datos que se envían. Si la transmisión confiable se requiere, este último servicio debe ser implementado por la aplicación del usuario.

En encabezado de UDP contiene 4 campos (Ver Figura. 3-44), cada uno de ellos está constituido por 2 bytes es decir 16 bits. Dos de esos campos resultan opcionales si se desea implementar con protocolos como IPv4.

+	Bits 0 - 15	16 - 31
0	Puerto origen	Puerto destino
32	Longitud del Mensaje	Suma de verificación
64	Datos	

Figura. 3-44 Estructura de una datagrama

➤ Puerto de origen

Este campo identifica el puerto transmisor, pues en el caso que se necesite dar respuesta al mensaje enviado, se utilizaría este número como puerto de destino. En todo caso si no se pretende recibir datos de respuesta el valor contenido en este campo sería 0. Si la fuente es el cliente, el número de puerto debe ser un número de puerto efímero. Si la el transmisor es el servidor, el número de puerto debe ser un numero de puerto muy bien conocido.

➤ Puerto de destino

Este campo identifica el puerto receptor si es necesario conocerle. De igual forma al número de puerto de origen., si el cliente es el host de destino entonces el número de puerto destino deberá ser un numero efímero y el puerto destino es el puerto de la aplicación en el servidor deberá tener un numero de puerto muy bien conocido.

➤ Longitud

El campo especifica la longitud en bytes de un datagrama entero: cabecera y datos. La longitud mínima es de 8 bytes dado que esta es la longitud del encabezado. El tamaño del campo establece el límite teórico de 65,535 bytes para un datagrama UDP. El límite práctico para la longitud de los datos el cual es impuesto por el protocolo IPv4 es 65507 bytes.

➤ Checksum

El campo de checksum es usado para verificación de errores en el encabezado y datos. Si este campo no es generado por el transmisor, el campo contiene el valor de 0. Este campo no es opcional al implementar un protocolo IPv6.

3.1.4.3.12 TCP vs. UDP

Como ya se han mencionado anteriormente los protocolos TCP y UDP son protocolos de capas 3. A modo de repaso se presenta la

Tabla 3-6 que contiene las características fundamentales de cada protocolo.

Tabla 3-6

TCP	UDP
<p>Confiable: TCP utiliza mensajes de confirmación, retransmisión y tiempo excedido. Realiza múltiples intentos para la transmisión de mensajes. Si un mensaje se pierde el servidor solicita la parte faltante. En el caso la pérdida de datos o la existencia de múltiples notificaciones de tiempo de espera excedido la conexión se deshace.</p>	<p>No confiable: cuando un mensaje es enviado, no se puede saber si fue entregado a su destino; el mensaje puede perderse en el camino. No se utiliza ningún concepto sobre confirmación de entrega, retransmisión o tiempo de espera excedido.</p>
<p>Ordenado: Si dos mensajes son enviados en secuencia a un punto y no llegan en el orden en que fueron enviados, el buffer de memoria de TCP se encarga de reordenar los datos para ser entregados posteriormente a la aplicación.</p>	<p>No ordenado: Si dos mensajes son enviados a el mismo receptor, el orden en que ellos sean entregados al receptor no puede ser predicho, determinado o corregido.</p>
<p>Pesado: TCP requiere de tres paquetes para establecer una conexión, antes de eso ningún usuario puede enviar o recibir datos.</p>	<p>Liviano: No hay orden en la entrega de mensajes, no hay seguimientos en la conexión, etc. Es un protocolo de capa de transporte pequeño.</p>
<p>Flujo en tramas: Los datos son leído como tramas, no se distinguen instrucción en la transmisión de señal de mensaje.</p>	<p>Datagramas: Los paquetes son enviados de forma individual y son revisados en cuanto a integridad solamente si ellos llegan. Los paquetes tienen límites definidos que el receptor puede detectar al leer e interpretar el mensaje de tal forma que se traspasa a la aplicación como un mensaje completo.</p>

3.1.4.4 Protocolo RTP y RTCP

3.1.4.4.1 Introducción

El protocolo de transporte en tiempo real (RTP) define el estándar para entrega de paquetes de audio y video en redes IP. RTP es usado en sistemas de entretenimiento y comunicación que involucran cadenas de datos, tal como telefonía, aplicaciones de video conferencias y aplicaciones web Push to talk. Para estos servicios se utilizan protocolos como H.323, MGCP, Megaco, SCCP o Protocolo de iniciación de sesión (SIP) como protocolos de señalización, siendo estos la base técnica de voz sobre IP.

RTP es usualmente usado en conjunto con el protocolo de control de RTP (RTCP). Mientras que las portadoras RTP es utilizado para transmitir las tramas en los medio, RTCP es usado para monitorear las transmisiones estáticas, calidad de servicio y la sincronización de múltiples tramas. Cuando ambos protocolos son usados en conjunción, RTP es originado y recibido utilizan números de puertos y los puertos asociados a la comunicación RTCP usan el número de puerto inmediato máximo.

3.1.4.4.2 Protocolo RTP

Fue desarrollado por un grupo de trabajo enfocado en el transporte de señales de audio y video de la organización IETF de estándares. RTP es usado en conjunto con otros protocolos tales como H.323 y RSTP. Este estándar define el par de protocolos mencionados RTP y RTCP.

RTP es diseñado para redes end-to-end, sistemas de tiempo real y transferencia de archivos en streams de datos. El protocolo provee facilidades para compensaciones de jitter y detección de errores en la secuencia de los paquetes que llegan. Problema que es muy común mientras se realizan las transmisiones en una red IP. RTP suporta la transferencia de archivos a múltiples destinos a través de multicast. RTP es reconocido como el principal estándar para transporte de audio y video en redes IP, poseyendo un carga de datos con un formato específico.

Las aplicaciones de tramas multimedia en tiempo real requieren un tiempo de entrega de información máximo y pueden tolerar pérdidas de algunos paquetes. Por ejemplo, si se pierde un paquete en una aplicación de audio esto puede resultar en pérdidas de una fracción de un segundo, lo cual puede pasar desapercibido con la implementación de un algoritmo de sustitución para evitar errores. El protocolo de control de transmisión, también se estandarizo para uso de RTP, pero no es normalmente usado en este tipo de aplicaciones por que una latencia inherente puede ser presentada por el establecimiento de una conexión y un error podría ocurrir. Es decir, si la conexión se pierde se deben cerrar sesión e iniciar una nueva conexión para enviar los paquetes faltantes. En el caso de la mayoría de los casos de aplicaciones RTP estos utilizan el protocolo UDP, que no está orientado a la conexión.

3.1.4.4.3 Estructura de encabezado RTP

bit offset	0-1	2	3	4-7	8	9-15	16-31
0	Version	P	X	CC	M	PT	Numero de secuencia
32	sello de tiempo						
64	Identificador SSRC						
96	Identificador CSRC						
96+32×CC	Extencion especifica de ID de cabecera					Longitud de extension de cabecera	
128+32×CC	Extension de cabecera ...						

Figura. 3-45 Encabezado de paquete RTP

En encabezado RTP (Ver Figura. 3-45) tiene un mínimo de tamaño de 12 Bytes. Luego del encabezado, se pueden utilizar extensiones opcionales del mismo. A continuación se presentan algunos de los componentes de un encabezado RTP.

- ✚ **Versión:** Ocupa 2 bites e indica la versión del protocolo utilizado.
- ✚ **P (relleno):** Es usado para indicar si existen bytes extras de relleno al final del paquete RTP. Un byte de relleno puede ser usado para llenar un bloque de cierto tamaño. Tiene un tamaño de un bit.
- ✚ **X (extensión):** Indica la presencia de una extensión en el encabezado entre la cabecera estándar y la carga de datos.
- ✚ **CC (cuenta CSRC):** Este campo contiene el número de identificador CSRC que sigue al encabezado de corrección. Esta sección contiene 4 bits.
- ✚ **M (marcador):** Usado en el nivel de aplicación y definido como un perfil. Si esta se establece en 1, significa que los datos actuales tienen alguna relevancia especial para la aplicación.
- ✚ **PT(tipo de carga):** Indica el formato de la carga y determina la interpretación para la aplicación. Esto es especificado por el perfil RTP. Utiliza 7 bits.
- ✚ **Numero de secuencia:** El número de secuencia es incrementado para cada paquete de datos RTP que es enviado y es usado por el receptor para detectar la pérdida de

paquetes y el reordenamiento de la secuencia. RTP no realiza ninguna acción si el paquete se pierde; queda a decisión de la aplicación el que tomar acción tomar respecto a esto.

- ✚ **Fecha y hora (timestamp):** Es usado para que el receptor pueda reproducir las muestras recibidas en los intervalos apropiados. Cuando las tramas de media es presentada, los timestamp son independientes en cada sentido, y no pueden ser utilizadas para la sincronización de los medios de comunicación.

3.1.4.4.4 Protocolo RTCP

El protocolo de control de RTP proporciona información de control en el flujo de datos que una aplicación multimedia genera o recibe. Sirve de soporte a RTP para el transporte de datos y empaquete de los mismos. Los paquetes de control son enviados a los participantes de la conversación multimedia. La función principal es informar la calidad de servicio proporcionada por RTP. RTCP recoge estadísticas de la conexión. Una aplicación puede utilizar esta información para mejorar la calidad del servicio, ya sea limitando el flujo de datos, utilizando un códec de compresión.

3.1.4.4.5 Estructura del encabezado RTCP

Versión: 2 bits. Indica la versión RTP, que es la misma en los paquetes RTCP que en los RTP

Relleno: 1 bit. Si está activado quiere decir que el paquete contiene algunos bits de relleno al final que no forman parte de la información de control. El último byte del relleno indica cuántos bytes de relleno se tiene que ignorar.

Conteo: 5 bits. Indica el número de bloques de informes de receptor contenidos en este paquete.

Tipo: 8 bits. Indica el tipo de paquete RTCP

Longitud: 16 bits. Indica la longitud del paquete RTCP

3.1.4.4.6 Tipos de paquetes

RTCP define varios tipos de paquetes que incluyen:

- Informes de emisor: Permiten al emisor activo en una sesión informar sobre estadísticas de recepción y transmisión.
- Informes de receptor: Los utilizan los receptores que no son emisores para enviar estadísticas sobre la recepción.

- Descripción de la fuente: Contiene los CNAMEs y otros datos que describen la información de los emisores.
- Paquetes de control específicos de la aplicación. Varios paquetes RTCP pueden ser enviados en un mismo mensaje UDP.

3.1.5 Capa de aplicación

La capa de aplicación del modelo TCP/IP contiene los conceptos presentes en las capas de sesión, presentación y aplicación del modelo OSI. Por lo tanto, los aspectos de representación, codificación y control de dialogo se administran en esta capa.

La capa de aplicación utiliza una serie de protocolos como HTTP⁵²_{xxii}, DNS⁵³_{xxiii}, FTP, SMTP⁵⁴_{xxiv}, SNMP⁵⁵_{xxv} y Telnet⁵⁶_{xxvi}. A cada uno de estos protocolos se les asigna un número de puerto (Ver Figura. 3-46) que se agrega en el paquete de tal forma que se pueda reconocer a que aplicación corresponde el paquete.

PROTOCOLO	PUERTO
HTTP	80
DNS	53
FTP	21
SMTP	25
SNMP	161
TELNET	23

Figura. 3-46 Protocolos de capa de aplicación.

La capa de aplicación ofrece una variedad de servicios como: administración de archivos, conexión a la red, conexiones remotas a los servidores y una variedad de utilidades de internet. (Ronces & Reyes Santos, 2009)

3.1.5.1 Servicios de capa de Aplicación de TCP/IP

⁵² HTTP = Hypertext Transfer Protocol – Protocolo de Transferencia de HyperTexto.

⁵³ DNS = Domain Name Server – Servidor de Nombre de Dominio

⁵⁴ SMTP = Simple Mail Transfer Protocol – Protocolo Simple de Transferencia de Correo.

⁵⁵ SNMP = Simple Network Management Protocol – Protocolo Simple de Administración de Red.

⁵⁶ Telnet = Telecommunication Network – Red de Telecomunicación

El protocolo de transferencia de archivos provee transferencia de archivos. Basado en el FTP un cliente local se puede conectar a otro servidor en la internet para enviar o recibir archivos, enlistar directorios y ejecutar comandos sencillos en la maquina remota. Al igual que Telnet, FTP se implanta dentro de una sesión de terminal.

NFS⁵⁷_{xxvii} fue desarrollado por Sun Microsystems, el NFS ofrece acceso directo a datos almacenados en un servidor remoto. NFS hace que una carpeta o directorio en el servidor NFS aparezca como un volumen local en el escritorio del cliente, de forma que los archivos en el servidor NFS puedan utilizarse como si estuvieran en el disco local.

POP⁵⁸_{xxviii} Las instrucciones generadas utilizando este protocolo permiten recuperar un elemento del servidor específicamente permite acceder el correo electrónico almacenado en un servidor.

El protocolo HTTP asociado a WWW⁵⁹_{xxix} Permite acceder a información almacenada en muchos nodos diferentes, pero además ofrece una elegante interface con fuentes, graficas, sonidos y ligas de tipo hipertexto a otros documentos.

La siguiente sección se enfoca en el estudio de los protocolos propios de cada de aplicación asociados a los tipos de servidores en que estos se implementan.

3.1.5.2 Servidores

Un servidor de internet es una computadora que ofrece servicios a los usuarios de una red o de Internet, dependiendo del alcance y el uso que se le desea dar. Por lo general son configurados con capacidades de procesamiento adicionales y memoria. La capacidad de almacenamiento en estos equipos depende del servicio que se pretende brindar. Un servidor de tipo DHCP no requiere de gran memoria, en cambio un servidor de FTP y correo electrónico, necesitan de discos duros grandes para almacenar la información. Incluso un servidor de multimedia como el necesario para páginas como youtube requiere de disco duros de gran capacidad. En la mayoría de los casos los servidores se configuran para que operen como:

- ✓ Servidores Web
- ✓ Firewalls
- ✓ Servidores FTP
- ✓ Servidores DNS
- ✓ Servidores de juegos en línea
- ✓ Servidores DHCP
- ✓ Servidor E-mail

⁵⁷ NFS = Network File System - Sistema de archivos Vía Red

⁵⁸ POP = Post Office Protocol – Protocolo de la Oficina de Correo

⁵⁹ WWW = World Wide Web - Red Mundial Amplia.

En este documento solo se desarrollaran los servidores tipo Web y Firewall, pues los primeros son los más utilizados. En el caso del firewall se hablar un poco a fin de dar una cierto enfoque en cuanto a método de seguridad de red para proteger la red LAN.

Muchos de los sistemas utilizados prefieren una configuración de servicio cliente/servidor, esto incluye a los servidores que contiene a los sitios web y correo electrónico. Un modelo alternativo de conexión a servidores, es el enlace punto a punto que permite a todas las computadoras conectadas a una red a funcionar como servidores o clientes según se necesite.

3.1.5.2.1 Servidores Web

Los servidores Web son computadoras en Internet que mantienen o almacenan la información pertinente de la página Web. Se encargan de responde ante las peticiones de entrada de las computadoras (Ver Figura. 3-47). Cada servidor web posee una dirección única de tal forma que las computadoras que se conectan a internet puedan encontrar el sitio. Los servidores deben pagar a los ISP (proveedores de servicios de internet) por el uso de la dirección IP o espacio en la red.

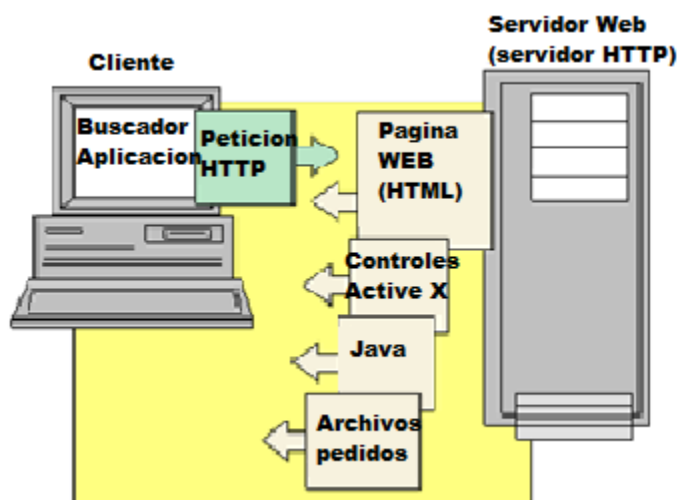


Figura. 3-47 Servidor Web responde ante petición del cliente.

3.1.5.2.2 Servidores de seguridad

Los firewalls son los llamados servidores de seguridad, básicamente se pretende que todo flujo de datos entrante y saliente de la red deba cruzar por este nodo, permitiendo así la revisión del contenido del paquete.

Los firewalls poseen 2 enrutadores que realizan filtrado de paquetes y una puerta de enlace de aplicación. Existen otros tipos de firewalls que solo poseen 1 enrutador que se encarga de las entradas y salidas de paquetes en la red. La ventaja del sistema con dos

enrutadores es que se lleva a cabo una revisión más exhaustiva en los paquetes, y presenta un mejor desempeño en momentos en que el nivel de tráfico es mayor.

Cada filtro de paquete es un enrutador estándar equipado con alguna funcionalidad extra. Los paquetes examinados que cumplan con algún criterio se reenvían de manera normal. Los que fallan la prueba se descartan.

Los filtros de paquetes son manejados por tablas configuradas por el administrador del sistema. Dichas tablas listan orígenes y destinos aceptables, orígenes y destinos bloqueados y reglas predeterminadas sobre lo que se debe hacer con los paquetes que van o vienen de otras maquinas.

En el caso común de una configuración TCP/IP, un origen o un destino consiste en una dirección IP y un puerto. Los puertos indican que servicio se desea. Por ejemplo, el puerto TCP 23 es para telnet y el puerto TCP 79 es para directorio. Una empresa podría bloquear los paquetes entrantes de todas las direcciones IP combinadas con uno de esos puertos.

Este tipo de bloqueo incluso puede llevarse a cabo en los routers más modernos, pues estos traen opciones de bloqueo a paquetes TCP o UDP.

Firewall > filtros para IP de clientes

El Router puede ser configurado para restringir el acceso a Internet, al correo electrónico o a otros servicios de red en determinados días y horas. [Más información](#)

IP	Puerto	Tipo	Tiempo de bloqueo	Día	Hora	Activar
192.168.2. <input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> AMBOS	<input type="radio"/> Siempre <input checked="" type="radio"/> Bloqueo	<input type="text"/> DOM <input type="text"/> DOM	<input type="text"/> 12:00 A.M. <input type="text"/> 12:00 A.M.	<input type="checkbox"/>
192.168.2. <input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> AMBOS	<input type="radio"/> Siempre <input checked="" type="radio"/> Bloqueo	<input type="text"/> DOM <input type="text"/> DOM	<input type="text"/> 12:00 A.M. <input type="text"/> 12:00 A.M.	<input type="checkbox"/>
192.168.2. <input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> AMBOS	<input type="radio"/> Siempre <input checked="" type="radio"/> Bloqueo	<input type="text"/> DOM <input type="text"/> DOM	<input type="text"/> 12:00 A.M. <input type="text"/> 12:00 A.M.	<input type="checkbox"/>
192.168.2. <input type="text"/> ~ <input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> AMBOS	<input type="radio"/> Siempre <input checked="" type="radio"/> Bloqueo	<input type="text"/> DOM <input type="text"/> DOM	<input type="text"/> 12:00 A.M. <input type="text"/> 12:00 A.M.	<input type="checkbox"/>

Figura. 3-48 Firewall integrado en router

La Figura. 3-48 muestra un ejemplo de la interfaz Web que presenta un router Belkin para configurar el nivel de acceso que tiene un usuario a la red externa. Esto se lleva a cabo mediante la declaración de puertos que se desean bloquear

según la dirección IP que tiene el usuario. Incluso este tipo de router permite establecer planes de bloqueo según la fecha y día de la semana en que debe ejecutarse el filtro.

3.1.5.2.3 Servidor de nombre de dominio

Inicialmente existía un archivos llamado hosts.txt, en el que se listaban todos los hosts y sus direcciones IP. Cada noche todos los hosts obtenían este archivo del sitio en el que se mantenía. (Tanenbaum, 2003)

Sin embargo, cuando miles de estaciones de trabajo se conectaron a la red, este método se consideró obsoleto. El principal problema era que podrían ocurrir conflictos constantes con los nombre de los hosts a menos que dichos nombres se administraran centralmente, algo indispensable en una red internacional enorme.

Como solución a este problema se inventó el protocolo DNS o bien Sistema de nombre de Dominio. En esencia este sistema es un esquema de nombres jerárquicos basado en dominios y un sistema de base de datos distribuido para implementar este esquema de nombres. El DNS relaciona los nombres de un host y direcciones IP de destino.

A grandes rasgos, el sistema de DNS funciona mediante una aplicación que se sitúa dentro del ordenador del cliente, esta aplicación llama a un procedimiento de biblioteca llamado *resolvidor*, y le pasa el nombre como parámetro. El resolvidor envía un paquete UDP a un servidor DNS local, que después busca el nombre y devuelve la dirección IP al resolvidor, que entonces lo devuelve al solicitante. A pesar de esta mejora, la administración de un grupo grande y continuamente cambiante de nombre es un problema nada sencillo. (Tanenbaum, 2003)

Internet se divide en 200 dominios de nivel superior, cada uno de los cuales abarca muchos hosts. Cada dominio se divide en subdominios, los cuales, a su vez, también se dividen, y así sucesivamente. Todos estos dominios pueden representarse mediante un árbol, como se muestra en la Figura. 3-49. Las hojas del árbol representan los dominios que no tienen subdominios. Un dominio de hoja puede contener un solo host, o puede representar a una compañía y contener miles de hosts.

Los dominios de nivel superior se dividen en dos categorías: genéricos y de país. Los dominios genéricos originales son:

- ✓ **Com:** para aquellos sitios de carácter comercial,
- ✓ **Edu:** en el caso de las instituciones educativas,
- ✓ **Gov:** como siglas a páginas del gobierno,
- ✓ **Int:** ciertas organizaciones internacionales
- ✓ **Mil:** Las fuerzas armadas de Estados Unidos
- ✓ **Net:** Proveedores de red
- ✓ **Org:** Organizaciones no lucrativas

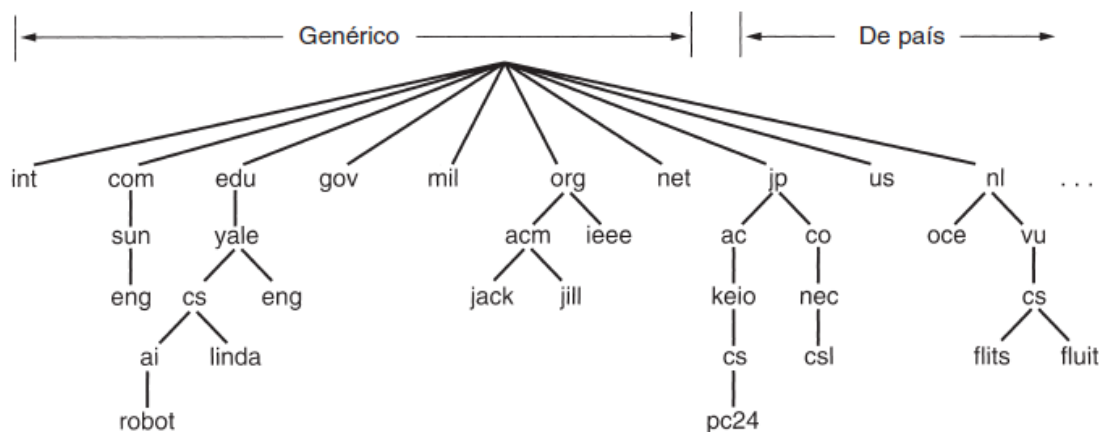


Figura. 3-49 Esquema jerárquico de nombres de dominio

En noviembre del 2000, ICANN aprobó cuatro nuevos dominios de nivel superior y propósito general:

- ✓ **Biz:** negocios
- ✓ **Info:** información
- ✓ **Name:** nombres de personas
- ✓ **Pro:** profesiones

Cada dominio se nombra por la ruta hacia arriba desde el a la raíz. Los componentes se separan con puntos. Por lo tanto, la universidad nacional de Ingeniería en Nicaragua se nombra *uni.edu.ni*. Los nombres de dominio no hacen distinción entre mayúsculas y minúsculas, por lo tanto se podría escribir *UNI.EDU.NI* y no había problemas al asociar este nombre a su dirección IP.

Cada dominio controla el cómo se asignan los dominios que están debajo de él. Por ejemplo Japón tiene los dominios *ac.jp* y *co.jp* que son espejos de *edu* y *com*. Esto nos muestra que puede existir más de un servidor de DNS ya sea por país o dominio.

En la práctica, un solo servidor no podría brindar servicio a la red mundial, este servidor se sobrecargaría y sería inservible. En el peor de los casos si el servidor tuviera una falla, el Internet global quedaría inhabilitado. Para evitar este tipo de problema, el espacio de DNS se divide en zonas no traslapantes. Cada zona debería contener una parte del árbol y también servidores de nombres que tienen la información de autorización correspondiente a esa zona.

Una zona debería tener un servidor primario, que obtiene su información de un archivo en su disco, y uno o más servidores secundarios, que obtienen su información del primario. No necesariamente el servidor primario debe estar situado en la zona a la que brinda servicio. Esto aumenta la confiabilidad en el sistema DNS.

3.1.5.2.4 Servidores DHCP

DHCP son las iniciales de Dynamic Host Configuration Protocol o bien protocolo de configuración dinámica de host. Este protocolo se instala en un servidor de una red local, permitiendo la configuración automática del protocolo TCP/IP de todos los clientes de dicha red. Nos permite evitar el tedioso trabajo de tener que configurar el protocolo TCP/IP cada vez que agregamos una nueva máquina a la red, por ejemplo, dirección IP, servidores DNS y gateways. Con un servidor DHCP tendremos una red con máquinas "plug-and-play", con sólo conectarlas podrá dialogar con red.

La configuración de DHCP se basa en un fichero de texto, `/etc/dhcp.conf` que el proceso servidor lee en el inicio. La lectura del fichero de configuración sólo se realiza durante el inicio, nunca cuando ya está en ejecución, por tanto cualquier modificación requiere detener el servicio DHCP y volverlo a iniciar. En este fichero se especifican las características de comportamiento como son el rango de direcciones asignadas, el tiempo de asignación de direcciones, el nombre del dominio, los gateways, etc. DHCP almacena en memoria la lista de direcciones de cada su red que está sirviendo. Cuando se arranca un cliente DHCP le solicita una dirección al servidor, éste busca una dirección disponible y se la asigna. En caso de necesidad, el servidor DHCP también puede asignar direcciones fijas a determinados equipos de la red.

La asignación de los datos TCP/IP al cliente se realiza para un determinado espacio de tiempo que se define en la configuración del servidor. Si no se especifica otro valor, la asignación predeterminada es por un día. También los clientes pueden solicitar datos de una duración especificada, aunque para evitar que un cliente tenga una dirección fija se puede prefijar un tiempo máximo de asignación.

Si tenemos varias subredes en nuestra instalación, también se pueden diferenciar las asignaciones que otorga el servidor DHCP según el interfaz en el que se realice.

Como el servidor DHCP puede pararse y reiniciarse, necesita mantener la lista de direcciones asignadas. El fichero `/var/lib/dhcp/dhcpd.leases` o `/var/state/dhcp/dhcpd.leases` mantiene esta lista de asignaciones. Cuando se inicia el servidor, primero lee el fichero de configuración `dhcpd.conf`, después el fichero `dhcpd.leases` y marca qué sistemas tienen asignaciones activas.

Cuando el cliente DHCP arranca resulta evidente que ignora la configuración de red por lo que necesita realizar las primeras comunicaciones mediante mensajes de difusión o broadcast. Esta difusión y el resto de las comunicaciones se basan en 8 tipos de mensajes en DHCP (Fábrega, 2003):

1. **DHCPDISCOVER:** El cliente envía un mensaje de difusión para localizar a los servidores DHCP activos.
2. **DHCPOFFER:** El servidor responde al cliente con una oferta de parámetros de configuración conforme a la situación del cliente.
3. **DHCPREQUEST:** Respuesta del cliente solicitando los parámetros ofertados, en caso de que el mensaje del servidor haya sido aceptado, rechazando la oferta, si el mensaje del servidor ha sido desestimado o confirmando la solicitud de una dirección IP obtenida anteriormente.
4. **DHCPACK:** Mensaje de confirmación y cierre desde el servidor hacia el cliente indicando los parámetros definitivos.
5. **DHCPNACK:** Mensaje que informa desde el servidor al cliente de que la dirección IP que solicita no es válida para la subred en la que se encuentra o la dirección IP ya no la puede asignar porque está asignada a otro equipo.
6. **DHCPDECLINE:** El cliente informa al servidor de que la dirección está en uso, normalmente porque otro usuario ha asignado esa dirección manualmente.
7. **DHCPRELEASE:** El cliente informa al servidor de que ha finalizado el uso de la dirección IP.
8. **DHCPINFORM:** El cliente consulta al servidor la configuración local. El cliente ya está configurado cuando envía este mensaje.

3.1.5.2.5 Servidores de correo electrónico

Es probable que uno de los usos más frecuentes en la red (Internet) sea la recepción y transmisión de correos electrónicos. Cuando un usuario envía un correo electrónico, el mensaje se enruta de servidor a servidor hasta llegar al servidor de correo del receptor. Es decir el servidor de correo electrónico no es único, existe un gran número de replicas facilitando así el acceso y disponibilidad del servicio a una zona específica.

A estos servidores se les llama Agentes de transporte de Correo o MTA⁶⁰_{xxx}, ellos tiene la tarea de transportar los correos hasta el MTA más cercano al usuario que solicita la información.

⁶⁰ MTA = Mail Transport Agent – Agente de Transporte de Correo

Los MTA se comunican entre ellos (Ver Figura. 3-50) en Internet utilizando el protocolo SMTP⁶¹ y por lo tanto se les llama servidores SMTP.

Luego el MTA más cercano al destinatario entrega el correo electrónico al servidor del correo entrante que se le conoce como Agente de Entrega de Correo o MDA⁶²_{xxx}. Este MDA almacena el correo electrónico hasta que el usuario lo acepte. Existen dos protocolos principales utilizados para recuperar correo electrónico de un MDA (Kioskea.net, 2008):

- El protocolo de oficina de correo (POP3), es el más antiguo de los dos. Se utiliza para recuperar correo electrónico y en algunos casos permite dejar una copia en el servidor.
- El protocolo de Acceso a Mensajes de Internet (IMAP), el cual se usa para coordinar el estado de los correos electrónicos a través de múltiples clientes de correo electrónico. Con IMAP, se guarda una copia de cada mensaje en el servidor, de manera que esta tarea de sincronización se pueda completar.

Por esta razón los servidores de correo entrante se llaman servidores POP o servidores IMAP, según el protocolo usado.

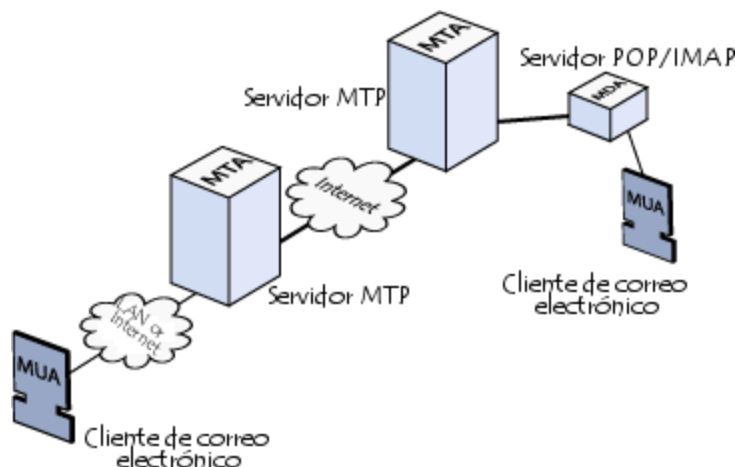


Figura. 3-50 Estructura de sistemas para servicio de correo electrónico

Tratando de hacer una analogía podríamos decir que los MTA son las oficinas de correo de cada pueblo, en cambio los MDA representan las casillas de correo de cada hogar, hasta que el usuario llegue a su buzón y retire el correo recibido. Por lo cual, se observa que no es necesario que los usuarios estén conectados para recibir un correo.

Para brindar seguridad a los clientes de correo electrónico, los MDA están protegidos por un nombre de usuario y una contraseña.

⁶¹ SMTP es un protocolo de capa de aplicación.

⁶² MDA = Mail Delivery Agent – Agente de entrega de correo.

Sin embargo no se ha mencionado el proceso o protocolo por el cual el usuario puede llegar a su buzón de correo en su hogar. El programa utilizado para llevar a cabo este proceso es un agente de usuario de correo o MUA⁶³. Cuando este MUA se instala en el sistema del usuario, se llama cliente de correo electrónico. En cambio cuando se usa una interfaz de web para interactuar con el servidor de correo entrante, se llama correo electrónico.

3.1.5.2.6 Servidores FTP

Uno de los servicios más antiguos de Internet, es el protocolo de transferencia de archivos, el cual permite mover uno o más archivos con seguridad entre distintos ordenadores proporcionando seguridad y organización de los archivos así como control de la transferencia.

La seguridad de red ha tomado una gran importancia desde ya hace varios años. Los servidores ftp comunicaban con los clientes "en abierto," es decir, que la información de la conexión y de la contraseña, eran vulnerables a la interceptación. Ahora, los servidores ftp, tales como BulletProof FTP, SecureFTP, SurgeFTP, TitanFTP, y WS_FTP, soportan SSL/TLS y utilizan el mismo tipo de cifrado presente en los sitios web seguros. Con SSL/TLS, los servidores ftp pueden cifrar los comandos de control entre los clientes del ftp y el servidor, así como los datos del archivo. Con la ayuda del PGP, como en WS_FTP pro, los datos del archivo se aseguran todavía más con el cifrado público. (Masadelante, 2011)

3.1.5.2.6.1 Modelo FTP

El protocolo FTP está incluido dentro del modelo cliente-servidor, es decir, un equipo envía órdenes (el cliente) y el otro espera solicitudes para llevar a cabo acciones (el servidor).

Durante una conexión FTP, se encuentran abiertos dos canales de transmisión (Ver Figura. 3-51 Modelo FTPFigura. 3-51):

- Un canal de comandos (canal de control)
- Un canal de datos

⁶³ MUA= Mail User Agent – Agente de correo de usuario.

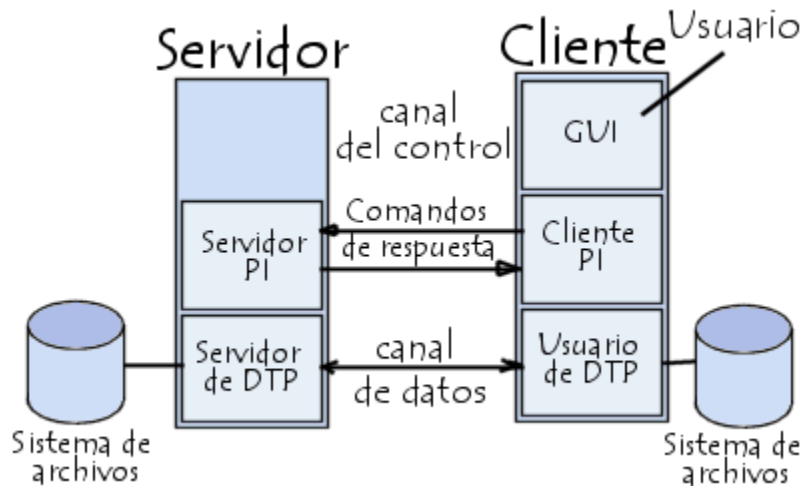


Figura. 3-51 Modelo FTP

Por lo tanto, el cliente y el servidor cuentan con dos procesos que permiten la administración de estos dos tipos de información:

- **DTP** (*Proceso de transferencia de datos*) es el proceso encargado de establecer la conexión y de administrar el canal de datos. El DTP del lado del servidor se denomina *SERVIDOR DE DTP* y el DTP del lado del cliente se denomina *USUARIO DE DTP*.
- **PI** (*Intérprete de protocolo*) interpreta el protocolo y permite que el DTP pueda ser controlado mediante los comandos recibidos a través del canal de control. Esto es diferente en el cliente y el servidor:

→ El **SERVIDOR PI** es responsable de escuchar los comandos que provienen de un **USUARIO PI** a través del canal de control en un puerto de datos, de establecer la conexión para el canal de control, de recibir los comandos FTP del **USUARIO PI** a través de éste, de responderles y de ejecutar el **SERVIDOR DE DTP**.

→ El **USUARIO PI** es responsable de establecer la conexión con el servidor FTP, de enviar los comandos FTP, de recibir respuestas del **SERVIDOR PI** y de controlar al **USUARIO DE DTP**, si fuera necesario.

Cuando un cliente FTP se conecta con un servidor FTP, el **USUARIO PI** inicia la conexión con el servidor de acuerdo con el protocolo Telnet. El cliente envía comandos FTP al servidor, el servidor los interpreta, ejecuta su DTP y después envía una respuesta estándar. Una vez que se establece la conexión, el servidor PI proporciona el puerto por el cual se enviarán los datos al **Cliente DTP**. El cliente DTP escucha el puerto especificado para los datos provenientes del servidor.

Es importante tener en cuenta que, debido a que los puertos de control y de datos son canales separados, es posible enviar comandos desde un equipo y recibir datos en otro. Entonces, por ejemplo, es posible transferir datos entre dos servidores FTP mediante el paso indirecto por un cliente para enviar instrucciones de control y la transferencia de información entre dos procesos del servidor conectados en el puerto correcto (Ver Figura. 3-52).

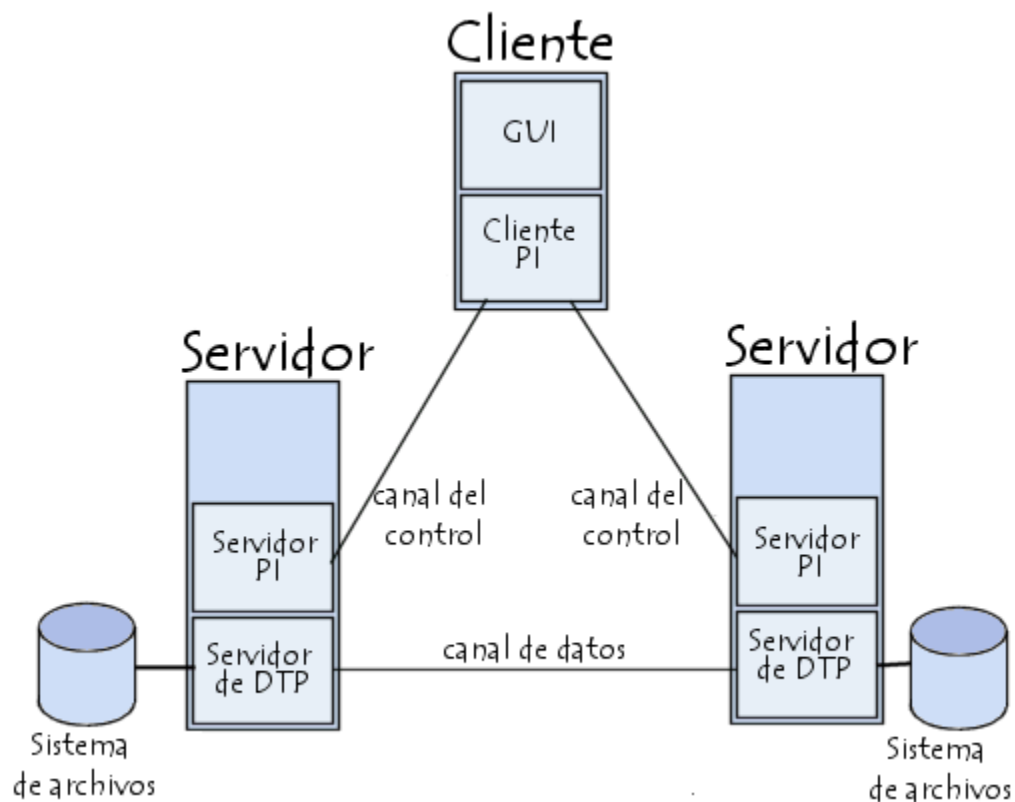


Figura. 3-52 Ejemplo de transferencia de archivos entre servidores FTP.

En esta configuración, el protocolo indica que los canales de control deben permanecer abiertos durante la transferencia de datos. De este modo, un servidor puede detener una transmisión si el canal de control es interrumpido durante la transmisión.

3.2 Preguntas de control

1. ¿Cuál es la correspondencia de las capas del modelo TCP/IP hacia el modelo OSI?
2. ¿Qué es el estándar V.24? y ¿Cuáles son sus características?
3. Describa el estándar Ethernet.
4. Construya una Tabla que presentando los estándares relacionados a Ethernet y sus características.
5. ¿Qué es CSMA? Y ¿Cuáles son las 2 modificaciones más importantes de este?
6. ¿En qué consiste CSMA/CD?
7. ¿En qué consiste CSMA/CA?
8. Explique brevemente el protocolo HDLC y sus características.
9. ¿Qué es PPP?
10. ¿En qué consiste ATM y Frame Relay? Explique brevemente cada uno de ellos.
11. ¿Cuáles son diferencias entre IPv4 e IPv6?
12. ¿Qué es direccionamiento IP?
13. ¿Cuál es la clasificación de direcciones IP y máscaras de red?
14. ¿Qué es VLSM?
15. ¿Qué es enrutamiento?
16. ¿En qué consiste el principio de optimización de enrutamiento?
17. Explique que es el algoritmo de inundación.
18. ¿Cuál es la diferencia entre difusión y multidifusión? ¿cuáles son las ventajas y desventajas de este método?
19. ¿Qué es OSPF? ¿Cuáles son sus áreas y mensajes?
20. Enumere las funciones de la capa de transporte.
21. ¿Qué procesos se llevan a cabo en la capa de aplicación?
22. ¿En qué consiste el enrutamiento y como se lleva a cabo?
23. ¿Cuáles son las funciones del protocolo IP?
24. Explique las diferencias entre protocolos orientados a conexión y sin conexión.
25. ¿Qué es TCP?
26. Explique cómo se lleva a cabo el proceso de establecimiento de una sesión TCP.
27. ¿Cuáles son los campos del paquete TCP y UDP?
28. ¿Cómo mantiene RTP el control en el envío de sus datagramas?

29. Mencione algunos protocolos de capa de aplicación y los servicios asociados a estos.
30. Resuelva el siguiente ejercicio.
Se pretende dividir una red IP en 4 subredes, las condiciones son las siguientes
Dirección de red general: 172.0.0.0/8
LAN1: Debe tener 14 usuarios
LAN 2: Una cantidad máxima de direcciones usables de 30
LAN 3: Con capacidad de hasta 56 usuarios en línea.
LAN 4: De uso privado, solo debe admitir 6 usuarios.
31. ¿Cómo se realiza el proceso de direccionar tramas a nivel de capa 2?
32. ¿Cuál es la función del tráiler de capa 2?
33. Mencione algunos elementos de red y sus características.
34. ¿Cuál es la ventaja de un switch sobre un hub?
35. ¿Qué es una VLAN?
36. ¿Qué es un servidor?
37. ¿Qué es un servidor WEB?
38. ¿Cuál es la función del sistema DNS?
39. ¿Cuál es la función y cómo opera un servidor DHCP?
40. Explique cómo se realiza el envío y recepción de un correo electrónico.

Unidad IV

MPLS

Objetivos General:

- Brindar al estudiante los conceptos y funcionalidades del protocolo de enrutamiento MPLS.

Objetivos Específicos:

- Identificarlos componentes del encabezado y red MPLS.
 - Determinar el proceso de operación de una red MPLS.
 - Señalar las unidades de datos de protocolo LDP y mensajes LDP.
 - Mencionar las ventajas del etiquetado.
 - Mostrar las facilidades de MPLS para implementar un servicio de telefonía.
-

Unidad 4. MPLS

4.1 Introducción

La conmutación de etiquetas multiprotocolo - MPLS⁶⁴_{xxxii} es un conjunto de protocolos que combina las capacidades de enrutamiento de capa 3 y conmutación de capa 2. MPLS dirige y porta datos de un nodo de red al próximo, y facilita la creación de enlaces virtuales entre nodos distantes.

MPLS es independiente de las tecnologías empleadas para el funcionamiento de capa 2 y 3, de tal forma que permite la integración de las redes con el uso de protocolos distintos a los utilizados en capa 2 y 3.

En el enrutamiento IP convencional (Ver Figura. 4-1) cada router en una línea desde la fuente hasta su destino determina el próximo salto por semejanzas o en las direcciones IP de destino utilizando el prefijo de mayor para compararle con los otros prefijos en su tabla de enrutamiento.

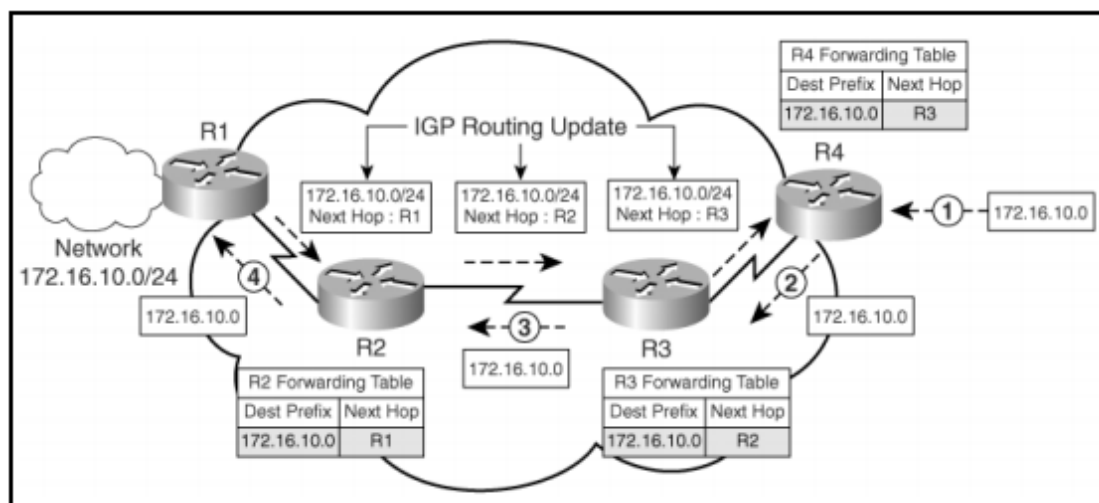


Figura. 4-1 Enrutamiento IP convencional.

En una red MPLS la clasificación está basada en la información de la cabecera de capa 3, por ejemplo, la precedencia IP o en la información no contenida en el paquete como el puerto de ingreso a la red, clasificación no limitada a los resultados de la tabla de enrutamiento. La clasificación se realiza solo una vez y es en el momento en que este ingresa a la red, a través del router MPLS, el cual marca(etiqueta) cada paquete con su “clase” respectiva, los siguientes routers dentro de la red determinan el próximo salto en base a la etiqueta MPLS que se le coloca al paquete.

⁶⁴ MPLS = Multi-Protocol Label Switching – Conmutación de etiquetas multi-protocolos.

Los routers en el interior de la red tienen la capacidad de asignar etiquetas para definir los caminos denominados “rutas de conmutación de etiqueta⁶⁵xxxiii”. En consecuencia solamente los routers de los extremos o contiguos a las redes de los clientes realizan el procedimiento de búsqueda en la tabla de enrutamiento.

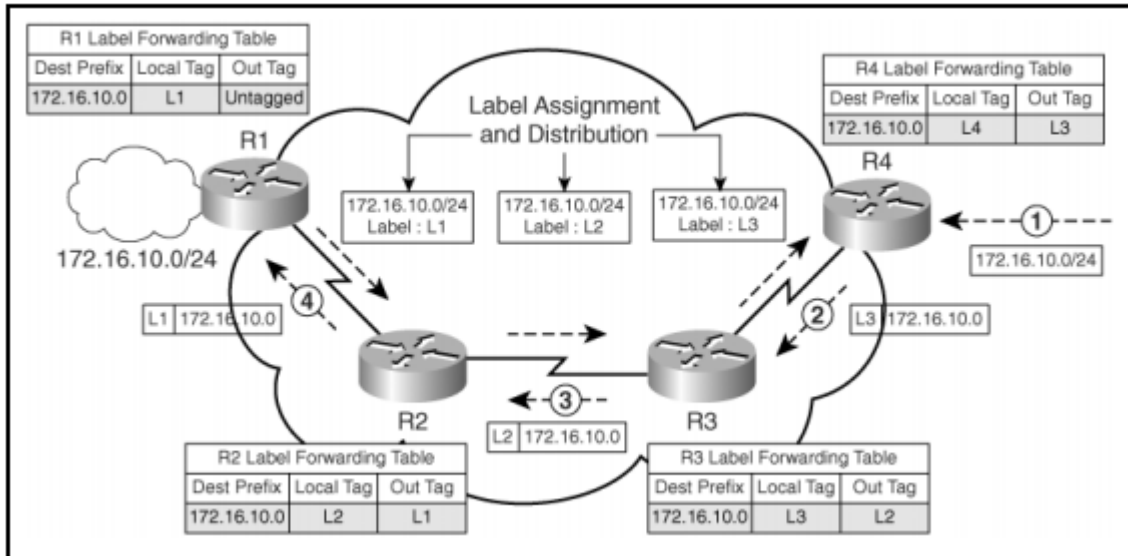


Figura. 4-2 Enrutamiento por etiqueta.

Los routers R1, R2 y R3 de la red MPLS (Ver Figura. 4-2) crean una tabla de enrutamiento de igual forma que una red IP convencional, para ello utilizan el protocolo IGP⁶⁶xxxiv. Los routers tienen la capacidad de asignar etiquetas para alcanzar la red de destino y los propagan en dirección contraria al flujo de datos, hacia los routers vecinos a los que se encuentran directamente conectados, en esta parte se hace uso del protocolo de distribución de etiqueta.

Por ejemplo, R1 asigna una etiqueta local L1 y la propaga al router vecino superior (upstream) R2, es decir en dirección contraria al flujo de datos. De forma similar R2 y R3 asignan etiquetas y las propagan de igual forma a sus vecinos superiores R3 y R4, respectivamente.

Comprender los conceptos de “**upstream y downstream**” es de gran importancia pues se hace uso de ellos en las siguientes secciones del documento para explicar los modos de anuncio de etiqueta (Ver Figura. 4-3). Se le denomina **downstream** al sentido que tiene el flujo planificado para los datos, mientras que la dirección opuesta es denominada **upstream** y es el sentido en el que se transmite la información de los protocolos de enrutamiento o de distribución de etiquetas. (Universidad Politecnica SALESIANA, 2004)

⁶⁵ LSP = Label switched path – rutas de conmutación de etiqueta.

⁶⁶ IGP = Interior Gateway Protocol – Protocolo de Pasarela Interior

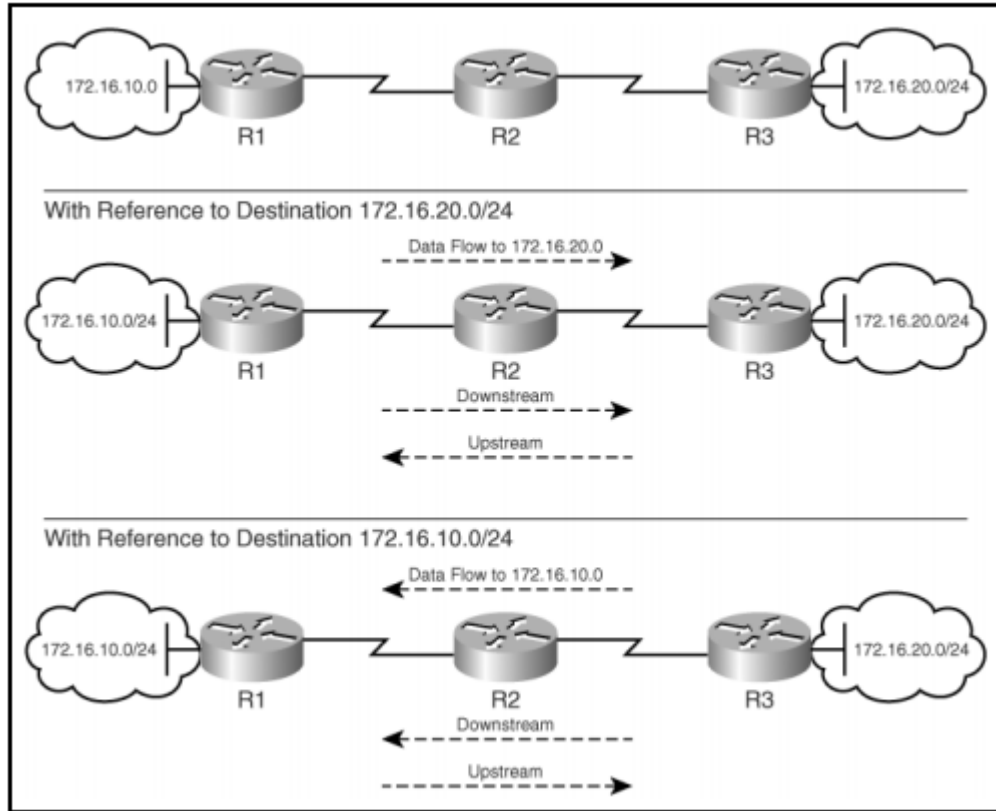


Figura. 4-3 Direcciones de flujo de datos.

4.2 Encabezado MPLS del paquete.

MPLS utiliza una cabecera corta que se introduce entre las porciones de capa 2 y capa 3 del datagrama IP (Ver Figura. 4-4). El encabezado MPLS es adicionado cuando el paquete entra a la red MPLS y es removida una vez que el paquete sale de la red.

Un paquete puede necesitar para cruzar varios dominios anidados MPLS. Un dominio anidado, es un dominio MPLS incluido dentro de otro dominio MPLS, las cabeceras MPLS pueden quedar apiladas, de tal forma que puede haber más de una cabecera de 32 bits en el encabezado del paquete.

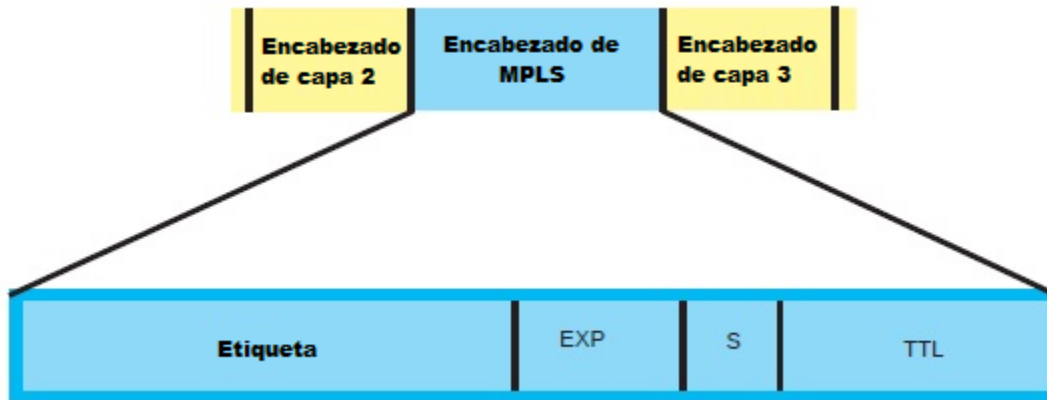


Figura. 4-4 Encabezado MPLS

El encabezado MPLS tiene una longitud de 32 bits.

- En capo de etiqueta tiene un total de 20 bits y porta el valor actual de la etiqueta. Las numeraciones de las etiquetas siguen las siguientes reglas:
 - ▶ 0 – IPv4 etiqueta explicita nula
 - ▶ 1 – Etiqueta de alerta al router
 - ▶ 2 – IPv6 etiqueta explicita nula
 - ▶ 3 – Etiqueta inplicita nula
 - ▶ 4 – 15 – Reservado para uso futuro
 - ▶ 15 – 1, 048,575 son usados para el LSR.
- El campo Exp (Experimental) es de 3 bits, y es usado para identificar la clase de tráfico o congestión. Este campo es usado para implementar calidad de servicio.
- El campo S es de 1 bit, y es usado cuando las cabeceras MPLS son apiladas para soportar múltiples cabeceras dentro del paquete.
 - ▶ 1 – indica que este es el ultimo encabezado MPLS en el paquete
 - ▶ 0 – identifica el encabezado como un encabezado más en la pila.
- El campo TTL⁶⁷ es de 8 bits y muestra el numero restantes de saltos pendientes. Este es igual que el estándar del datagrama IP.

⁶⁷ TTL = Time to Live – tiempo de vida.

4.3 Componentes de MPLS

MPLS como se había mencionado anteriormente opera en el núcleo de las redes. Los componentes fundamentales se muestran en la Figura. 4-5 y explicados a continuación:



Figura. 4-5 Elementos de red MPLS

Router perimetral del cliente (Customer Edge Router): Es un router ubicado en las instalaciones del cliente y está conectado a la red MPLS.

Router de conmutación de etiquetas de ingreso (Ingress LSR): el LSR de ingreso recibe el tráfico IP proveniente de las redes IP del cliente. El router clasifica los paquetes basados principalmente en relación a la dirección IP de destino, de igual forma este puede utilizar otros campos para esto.

Luego el LSR de ingreso genera una encabezado MPLS y asigna una etiqueta basada en la clasificación. Este router encapsula el paquete en una unidad de datos de protocolo MPLS (PDU) y envía el paquete hacia el próximo salto.

Routers de transito de conmutación de etiqueta (Transit LSR): Estos LSRs de transito forman parte de la red MPLS interna. Estos reciben los paquetes MPLS y usan la cabecera MPLS para determinar el envío. El LSR de transito requiere la implementación de el intercambio de etiquetas MPLS (MPLS label swapping)

Router de salida de conmutación de etiquetas (Egress LSR): Este router remueve las etiquetas de MPLS al momento en que el paquete sale de la red MPLS. Finalmente se encarga de enviar el paquete basado en la tabla IP de envío.

4.4 Operación de una red MPLS.

La operación de una red MPLS se resume en los siguientes pasos:

1. Se lleva a cabo la asignación de etiquetas por parte de los routers.
2. Establecimiento de una sesión utilizando los protocolos de distribución de etiqueta entre los routers.
3. Distribución de etiquetas MPLS.
4. Retención de etiquetas asignadas.
5. Reenviar los paquetes recibidos en relación a la asignación de etiquetas retenidas.

El siguiente ejemplo (Ver Figura. 4-6) da una idea global sobre el paso 5 explicando el funcionamiento e interconexión de distintas redes MPLS y apilamiento de etiquetas a medida que cruzan los paquetes.

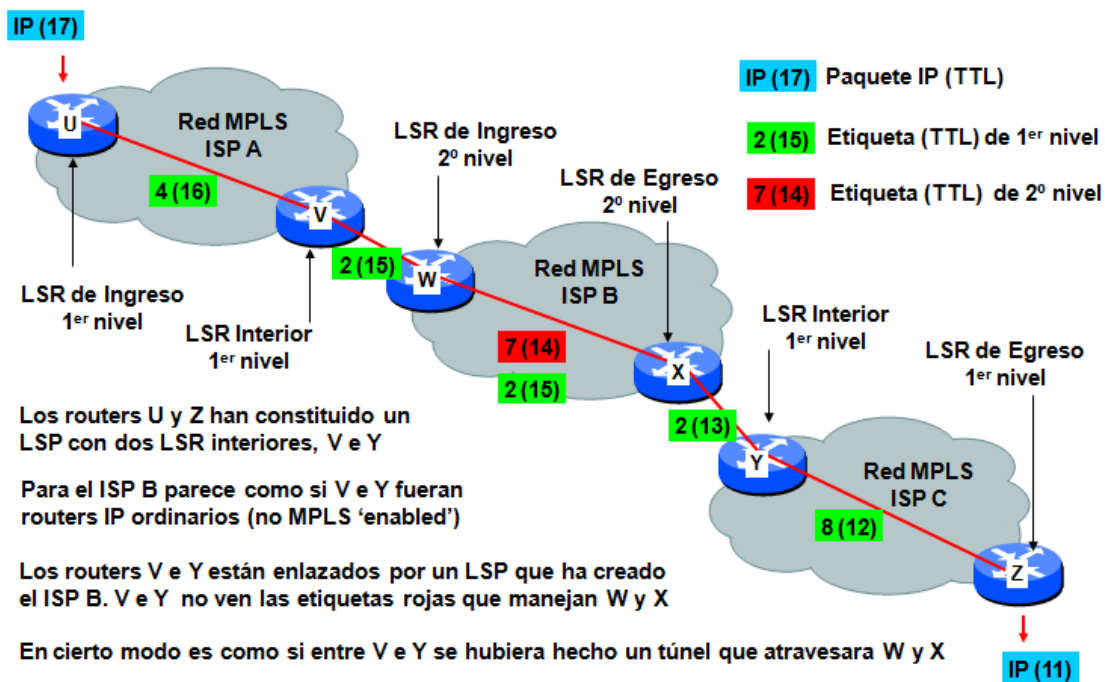


Figura. 4-6 Interconexión de redes MPLS.

Por cada cruce de red MPLS se debe asignar una etiqueta, observe la etiqueta 4 con un TTL de 16 desde U a V. Cuando el paquete deja la red MPLS del ISP A se asigna una nueva etiqueta 2 y si TTL disminuye a 15. Al ingresar al ISP B se agrega una nueva etiqueta 7 por encima de la etiqueta 2, observe que el TTL de esta etiqueta es igual al tiempo TTL de la etiqueta 2 menos 1. Al salir de la red MPLS del ISP 2, la etiqueta 7 es removida y el TTL de la etiqueta 2 se disminuye nuevamente. Finalmente al entrar en la red MPLS del ISP C la etiqueta 2 es sustituida por la etiqueta 8 indicando su destino al router Z, una vez concluido este proceso se utiliza el enrutamiento IP convencional en la red del cliente.

4.5 Creación de etiquetas.

En una red MPLS, un grupo de paquetes que cruzan el mismo camino desde su ingreso a la red hasta su egreso se le conoce como una clasificación de reenvío (FEC⁶⁸_{xxxv}). Los paquetes son clasificados por pareo de la dirección IP de destino en relación a 2 criterios. Estos criterios son:

- El prefijo de dirección que es la porción de dirección que identifica la red en la dirección total del paquete.
- La dirección de host que es la dirección IP total del paquete.

Una etiqueta es un valor único y arbitrario que representa una FEC y es insertada en el paquete. La unión o vinculación de una etiqueta a una FEC es llamado “enlaces”. Estos enlaces se manejan de forma local entre los routers MPLS adyacentes y con intercambiados usando LDP⁶⁹_{xxxvi}.

Una etiqueta es en la mayoría de los casos globalmente única. Sin embargo, un sistema puede enlazar la misma etiqueta a más de una FEC; cuando las FECs son usadas en diferentes aplicaciones, o contexto. El contexto en el cual la etiqueta es usada se denominada “espacio de etiqueta”, y es representado por un valor de 16 bits concatenado con el “identificador de distribución de etiquetas” del LSR.

Existen 2 tipos de Espacio de etiqueta, por interfaz y por plataforma.

- Un espacio de etiqueta por interfaz existe cuando un LSR “enlaza” una etiqueta a más de una FEC y distribuye cada “enlace” a un sistema diferente conectado por un enlace punto a punto.
- Un espacio de etiqueta por plataforma es también conocido como “espacio de etiqueta global”. Existe cuando todos los “enlaces” creados por el sistema son únicos.

MPLS es diseñado de tal forma que solamente un router implemente el proceso de búsqueda en la tabla de enrutamiento, para un prefijo de dirección determinado. Este router luego crea una etiqueta de tal forma que los demás routers conmuten en relación a esta etiqueta. Para LSR busca en su propia para de enrutamiento y decide para cuales prefijos de direcciones creara una etiqueta basada en los “modos de control de etiqueta”

La arquitectura MPLS define dos modos de control de etiqueta. Ambos modos pueden ser usados en la misma red, el modo de control ordenado se logra únicamente cuando todos los LSRs en la red lo utilizan.

⁶⁸ FEC = Forwarding Equivalence Class

⁶⁹ LDP = Label Distribution Protocol. – Protocolo de Distribucion de Etiquetas

El **modo de control de distribución de etiquetas independiente** se lleva a cabo cuando un LSR identifica una FEC, asigna una etiqueta creando una “enlace” y luego procede a distribuir dicho “enlace” por la red.

El **modo de control de distribución de etiquetas ordenado** se realiza cuando un LSR enlaza una etiqueta a una FEC solamente si este LSR es un LSR de egreso de la red o si este ha recibido el “enlace” proviniendo del próximo salto.

Un LSR es de egreso si la FEC de este hace referencia a una ruta como una interfaz directamente conectada (Ver Figura. 4-7, R3) o cuando el próximo salto para la FEC se encuentra fuera de la red MPLS(Ver Figura. 4-7, R2).

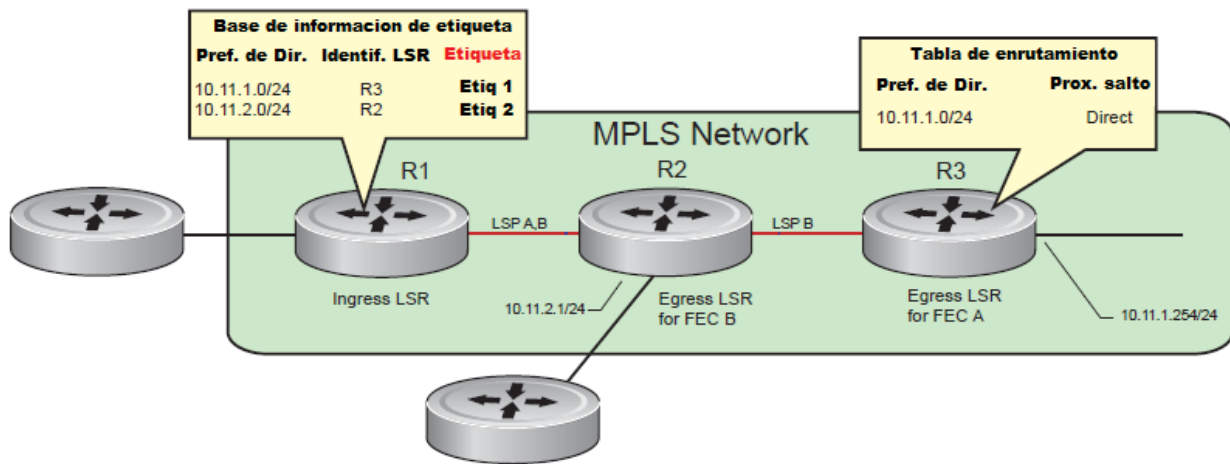


Figura. 4-7 Ejemplos LSRs de egreso

4.6 Distribución de etiquetas

Las etiquetas son distribuidas desde el LSR de egreso hasta el LSR de ingreso a la red, para una FEC dada. El procedimiento de distribución de etiquetas se basa en la combinación de modos de anuncios de etiquetas y modos de control de etiqueta.

4.6.1 Protocolo de distribución de etiquetas - LDP

Es el encargado de distribuir como su nombre lo dice etiquetas entre dos LSRs para el flujo de tráfico entre y a través de ellos. LDP asocia una FEC con cada LSP que este crea, y la FEC asociada con un LSP define cual paquete es asignado a el LSP.

4.6.2 Modos de anuncio de etiqueta

Existen 2 modos para anunciar el uso de una nueva etiqueta, cada uno esta prescripto en la arquitectura de la red MPLS. Ambos métodos pueden ser usados en la misma red MPLS e incluso al mismo tiempo, pero cada proximidad debe utilizar solamente

uno. Es decir, el modo de advertencia de etiquetas debe ser uno de los 2 mencionados. El mismo LSR puede utilizar otro modo en otro enlace a otro LSR.

- El modo “downstream bajo demanda” se lleva a cabo cuando un LSR distribuye la asignación de un “enlace” FEC-etiqueta, solamente si se recibe una solicitud o petición de envío procedente del LSR superior inmediato en el curso de la red.
- El modo “downstream no solicitada” se realiza cuando un LSR avisa a los LSRs la asignación de etiqueta que ha realizado sin petición alguna.

4.6.3 Procedimiento de distribución de etiqueta

Existen 4 métodos para distribuir etiquetas que combinan explícitamente los modos de anuncio y control.

- a) Empuje-incondicional: Combina “Downstream - no solicitada” + Modo de control Independiente. Un LSR avisa la asignación de etiqueta para cualquier FEC que este reconozca, en cualquier momento.
- b) Empuje-condicional: Combina “Downstream - no solicitada” + modo de control ordenado. Un LSR avisa la asignación de etiqueta en cualquier momento solamente si el LSR de egreso es la FEC asignada a la etiqueta o si este recibe el “enlace” de etiqueta proviniendo del próximo salto.
- c) Jalado-incondicional: Combina Downstream bajo demanda + Modo de control independiente. Un LSR responde las peticiones de asociación de etiquetas inmediatamente, sin ser el LSR de egreso o esperando el “enlace” proveniente del próximo salto.
- d) Jalado-condicional: Combina Downstream bajo demanda + Modo de control ordenado. Un LSR responde a una petición de asociación de etiqueta solo si la FEC que se asocia es el LSR de egreso, o si ha recibido este “enlace” proviniendo del próximo salto.

Para realizar el intercambio de “enlaces” creados por los LSR estos deben estar emparejados. Es decir, deben estar de acuerdo en cual modo de advertencia de los mencionados anteriormente se usara. Este “emparejamiento” se llevaba a cabo mediante una sesión TCP entre los LSRs (Ver Figura. 4-8).

Paso 1. Antes de establecer el “emparejamiento”, los LSRs deben identificarse cada uno. Para identificar vecinos directamente conectados, uno de los LSRs envía periódicamente un datagrama Hello solicitando un enlace LDP a todos los routers con direcciones multicast 224.0.0.2. Para que el LSR pueda identificarse con un LSR vecino que no esté directamente conectado entonces se envían periódicamente mensajes Hello usando LDP

dirigidos al LSR específico. El LSR que recibe, decide cuando responder al mensaje. Esto crea una proximidad o lazo entre ambos routers.

Paso 2. Una vez que se crea el lazo de proximidad, el LSR con la mayor dirección IP se convierte en el LSR activo, el cual es responsable de establecer la conexión TCP entre ellos utilizando el puerto LDP 646. La dirección IP usada para comparar puede ser bien la dirección de origen del mensaje hello de “emparejamiento”, o una dirección IP que puede ser opcionalmente especificada con el mensaje hello.

Paso 3. El inicio de sesión se da cuando el LSR negocia los parámetros de LDP tales como los modos de aviso de “enlaces” (etiquetas nuevas), modos de control de etiqueta y tiempo que debe mantener activo o “vivo” una etiqueta.

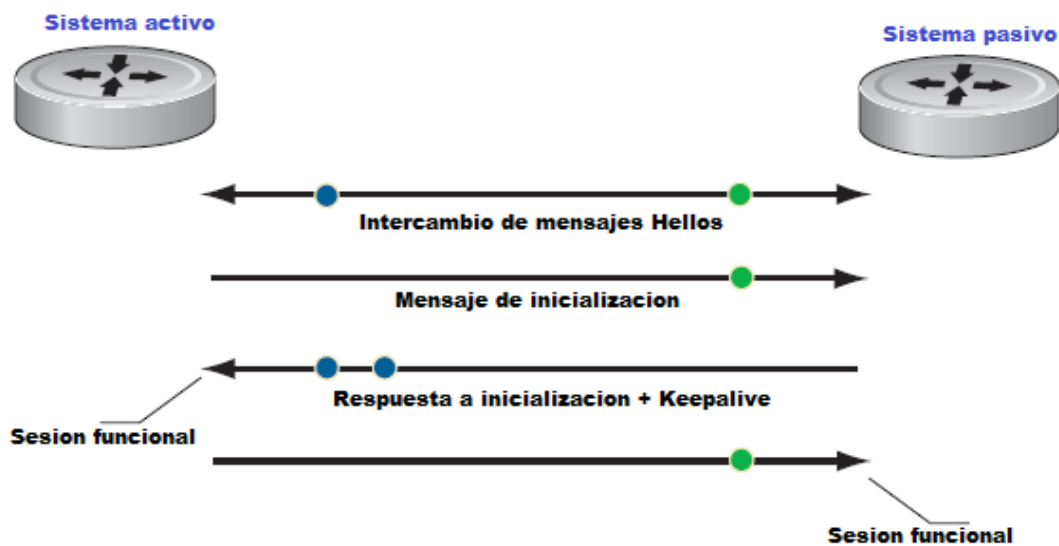


Figura. 4-8 Proceso de reconocimiento de pares entre routers.

4.7 Unidades de datos de protocolo LDP

Los emparejamientos LDP intercambian información utilizando *mensajes* dentro de PDUs sobre una conexión TCP. Cada PDU de LDP porta uno o más mensajes los cuales son: tipo, longitud y un valor de formato.

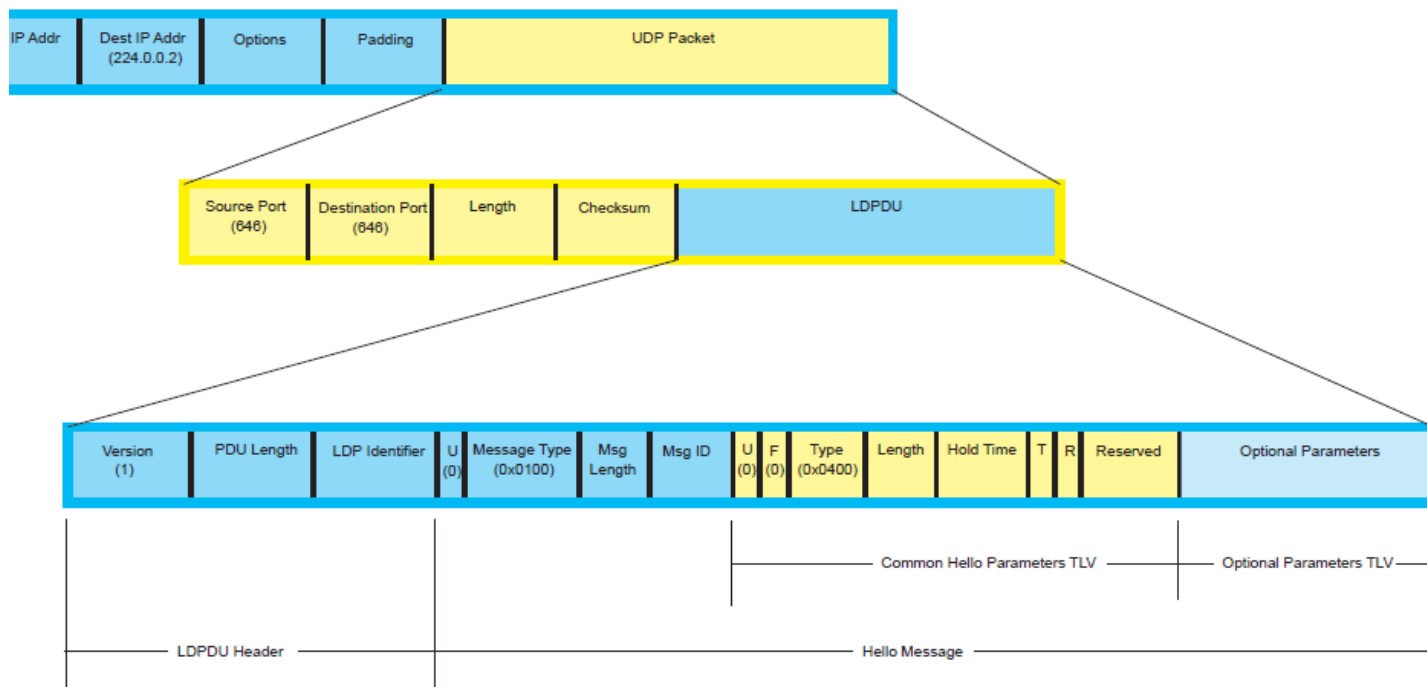


Figura. 4-9 Campos de mensaje LDP

Las PDUs de LDP inician con un encabezado que contiene 3 campos (Ver Figura. 4-9).

El campo versión indica la versión de LDP que se utiliza. La longitud de la PDU especifica el tamaño de la PDU incluyendo el encabezado en octetos. El máximo de longitud por PDU es negociado entre los LSRs. El identificador del LSR es un valor de octeto globalmente único. Los primeros 4 octetos son el ID del router y los 2 últimos identifican el “espacio de etiqueta”. Para una plataforma de espacio de etiqueta abierta, estos 2 octetos son cero.

4.7.1 Mensajes de Emparejamiento.

Este tipo de mensaje son utilizados para determinar y establecer las proximidades y sesiones entre LSRs.

4.7.1.1 Mensaje Hello.

Son utilizados para identificar los LDP vecinos. Los LSRs pueden estar en modo activo o pasivo, como se había mencionado anteriormente. EL encargado de enviar el

mensaje hello es el LSR activo en todas sus interfaces. Los LSRs pasivos solamente responden a los Hellos.

La Figura. 4-9 muestra los campos que se encuentran en el interior del mensaje Hello. La Tabla 4-1 describe la función de cada campo de este mensaje.

Tabla 4-1

Tipo	Parámetro	Descripción
0X0400	Parámetros de hello comunes	
	Hold time	Determina el tiempo que se debe mantener activo el enlace Hello. Estos deben ser enviados periódicamente para refrescar el timer de sesión. Por defecto: 15 segundos para un hellos de enlace, 45 segundos para hellos dirigidos. El por defecto se indica a través de la colocación de un 0 en este campo.
	T (Targeted hello)	1 indica que el mensaje es un hello dirigido 0 indica que el mensaje es un hello de enlace.
	R (Request Send Targeted Hello)	1 indica que el transmisor está solicitando que el receptor envíe un hello dirigido 0 indica que no se realiza ninguna solicitud.
Parámetros opcionales.		
0x0401	Dirección IPv4 de transporte	Especifica la dirección IP a usar durante el establecimiento de la sesión TCP. Si no es usado este campo, la dirección de destino para el hello es usada para la conexión TCP.
0x0402	Numero de secuencia de configuración	Cuando se realice un cambio de configuración en el LSR que envía, este incrementa el número de secuencia de configuración
0x0403	Dirección IPv6 de transporte	Especifica la dirección IP a usar durante el establecimiento de la sesión TCP. Si este campo no es utilizado, la dirección de origen para el hello es usada para la conexión TCP

4.7.1.2 Mensaje de inicialización

Son utilizados para negociar o avisar los parámetros de sesión como los modos de aviso de etiqueta y detección de lazo.

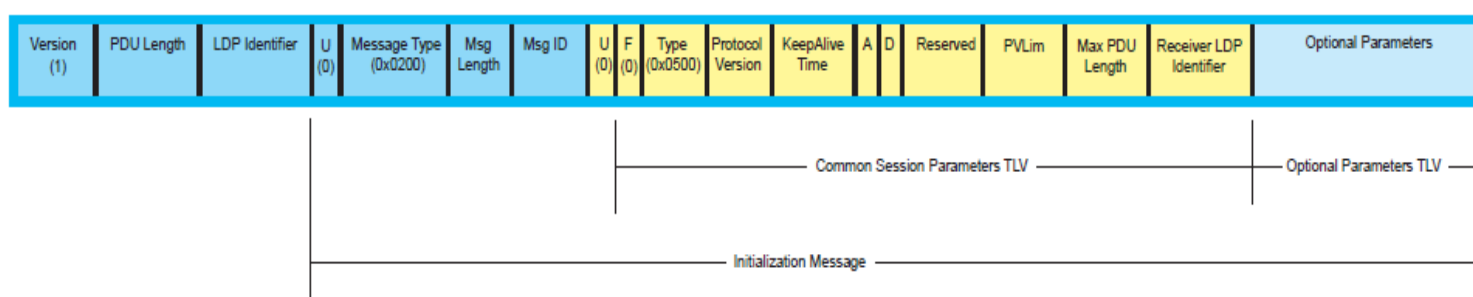


Figura. 4-10 Campos de mensaje de inicialización

La Figura. 4-10 muestra los campos del mensaje de inicialización y la siguiente Tabla 4-2 describe las funciones de cada uno de estos.

Tabla 4-2

Tipo	Parámetros	Descripción
0x0500	Parámetros comunes de sesión	
	KeepAlive Time	Una sesión es creada para un espacio de etiqueta. Este temporizador se reinicia tras la recepción de un mensaje o PDU LDP. La sesión se acaba si el temporizador expira. Este temporizador es aparte del hold time, el cual mantiene las sesión de proximidad.
	A (Disciplina de anuncio de etiqueta)	Indica el modo de anuncio de etiqueta: 0 Downstream – no solicitada 1 Downstream bajo demanda En caso de un conflicto en negociación, el modo de downstream no solicitada es utilizado.
	D (Detección de lazo)	Indica cuando la detección de lazo está habilitada. 0: deshabilitada 1: habilitada
	PVLim	Longitud de vector de línea es usada para detectar lazos. El límite de vector de línea indica la longitud máxima que puede tener la ruta. PVLim es 0 si la detección de lazo esta deshabilitada.
	Longitud max de PDU	Define la longitud máxima permisible para una PDU de LDP para una sesión. Por defecto: 4096 bytes.
	Identificador LDP del receptor.	Identifica el espacio de etiqueta del receptor. Combinado con el identificador de LDP del transmisor, el receptor puede emparejar el mensaje a uno de sus vecinos.

4.7.1.3 Mensaje de notificación

Los mensajes de notificación transmiten el procesamiento de un mensaje LDP o el estado de la sesión LDP, incluyendo:

- Parámetros de inicialización inaceptables
- Detección de lazos
- No ruta (en caso de que la solicitud de una FEC no esté en la tabla de enrutamiento)
- Sesión o desmontaje de vecindad.

La Figura. 4-11 muestra la sección del mensaje completo que contiene los campos de notificación y la Tabla 4-3 describe cada uno de estos campos.

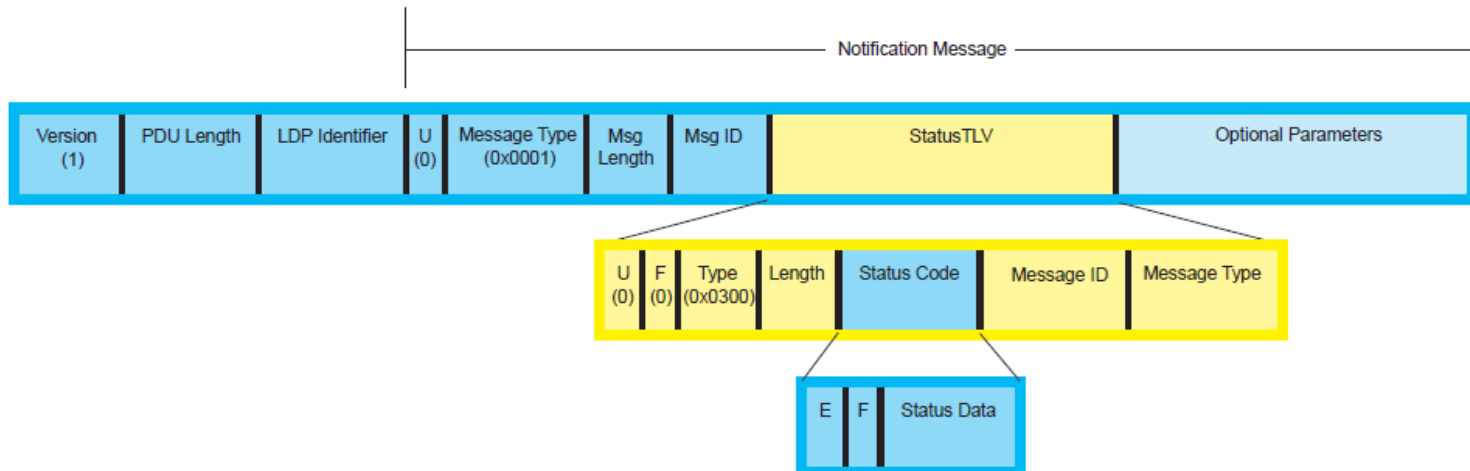


Figura. 4-11 Campos del mensaje de notificación

Tabla 4-3

Tipo	Parámetros	Descripción
Estados de TLV(Tipo-longitud-Valor)		
	U(Desconocido)	Establece a 0 cuando el TLV aparece en un mensaje de notificación. Establece a 1 cuando el TLV es enviado en otro tipo de mensaje.
	F(envió desconocido)	Notifica la ocurrencia de un error grave.
Código de estado (Status Code)		
	E (Error Fatal)	Establece a 0 si el mensaje de notificación es una advertencia. Establece a 1 si el mensaje de notificación señala un error fatal. Errores fatales obliga a ambos LSRs a finalizar la sesión.
	F (Envió)	Establece a 0 si no reenvía Establece a 1 si la notificación debe ser reenviada a un LSR superior o inferior en la ruta.
	Estado de datos	Completo representa el estado. 0 significa exitoso.
	ID del mensaje	Se refiere al ID del mensaje para el cual la notificación responde.
	Tipo de mensaje	Se refiere al tipo de mensaje de pareo para el cual la notificación responde.

4.7.2 Mensajes de distribución de etiquetas

Este tipo de mensaje distribuye las asignaciones de etiquetas a través de las series de LSRs para crear las rutas de conmutación de etiquetas (LSPs) para cada FEC.

4.7.2.1 Mensaje de dirección

Cada LSR envía a su par⁷⁰ de interfaz activa direcciones. Esta lista es usada para determinar cuando el próximo salto para un prefijo de dirección es un par LDP. Cuando un LSR recibe una asignación de etiquetas provenientes del par que se encuentra un paso antes en el flujo downstream, determina si el LSR de origen es el próximo salto para la FEC. Si es este, el LSR instala y usa la etiqueta para reenvío. Si lo no es, el LSR instala, retiene y luego libera la etiqueta basándose en el modo de retención de etiqueta.

Los mensajes de retirada de dirección son usados para señalar a un par que una dirección previamente anunciada ya no es válida. La Figura. 4-12 muestra el campo en el que se sitúa el mensaje de dirección.

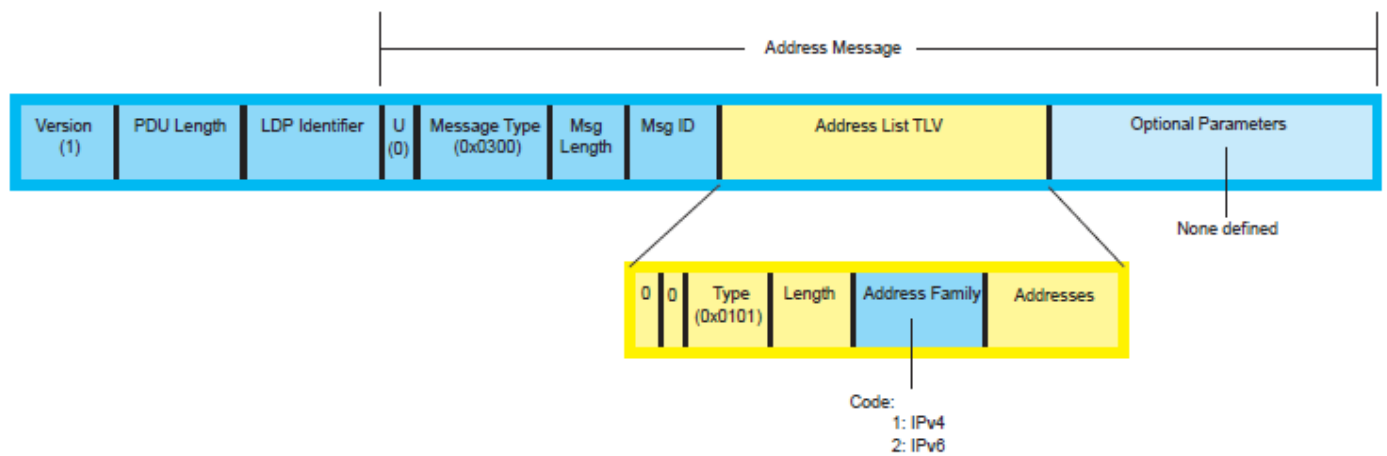


Figura. 4-12 Campos del mensaje de dirección.

4.7.2.2 Mensaje de asignación de etiquetas.

Los LSRs utilizan los mensajes de asignación de etiquetas para anunciar la asignación de etiquetas a los pares con direcciones IP mayores que el transmisor. Un LSR anuncia una asignación de etiqueta a un par cuando:

- Reconoce una nueva FEC en su propia tabla de reenvío, y su modo de distribución es “Downstream no solicitada.”
- Recibe una petición para una asignación de etiqueta

⁷⁰ Un “par” es un LSR vecino emparejado con él.

- Recibe una asignación de un par en el flujo downstream y que todavía no ha sido distribuida a en un flujo upstream.

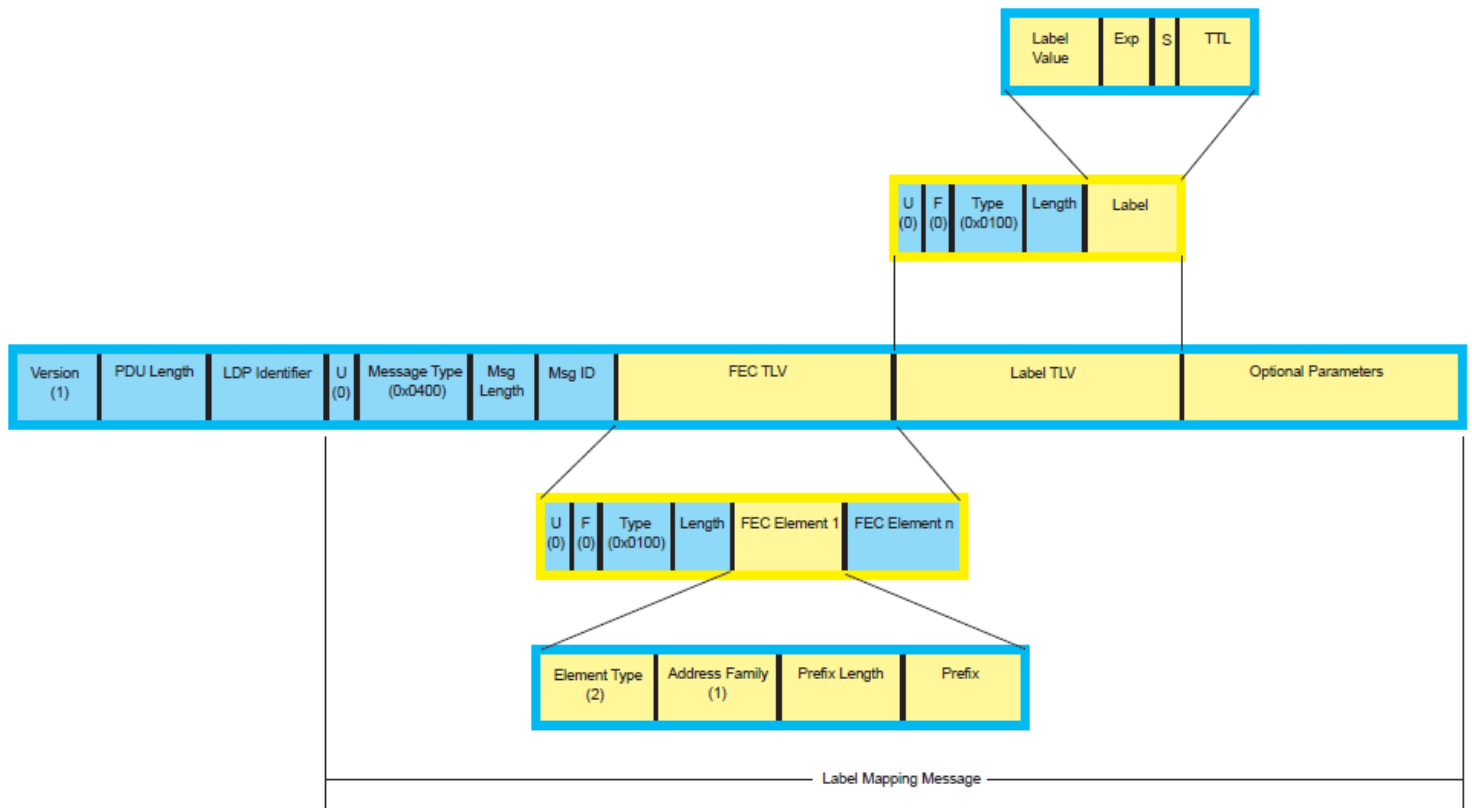


Figura. 4-13 Campos del mensaje de asignación de etiqueta.

La Figura. 4-13 muestra los campos contenidos en un mensaje asignación de etiqueta y la Tabla 4-4 muestra las descripciones de cada campo.

Tabla 4-4

Tipo	Parámetros	Descripción
0x0400	Mensaje de asignación de etiqueta	
0x0100	FEC TLV	
	Tipo de elemento de FEC	0x02: Prefijo de dirección 0x03: Dirección de host
	Dirección de familia	1: IPv4 2: IPv6
	Longitud de prefijo	El numero de bits que comprende la dirección de prefijo.
	Prefijo	El prefijo de dirección
0x0200	Tabla TLV genérica	
	Valor de etiqueta	Un número de 8 bits arbitrarios en un campo de 20 bits. Los bits de 4-15 están reservados
	Experimental	Reservado
	S	Establece a 1 si las etiquetas es la última entrada en la pila de etiquetas. Cero para todas las otras posiciones.
	Time-to-live	Cuando una etiqueta es insertada en un paquete, el valor TTL es el mismo que el campo TTL IP. El TTL es reducido por uno en cada LSR.
Parámetros operacionales		
	Mensaje ID TLV para solicitud de etiqueta.	Si el mensaje de asignación de etiqueta es una respuesta a una petición, el mensaje ID de petición de etiqueta debe ser incluido. Este tipo de campo TLV es 0x0600.
	Cuenta de salto TLV	Usado para contar el numero de LSRs en el LSP.
	Vector de camino TLV	Usado para la detección de lazo.

4.7.2.3 Mensaje de solicitud de etiqueta.

Un LSR solicita la asignación de una etiqueta a un par LSR en dirección downstream:

- El LSR reconoce una nueva FEC por medio de la tabla de enrutamiento.
- El LSR recibe una solicitud para una FEC proveniente de un par LSR con una dirección IP mayor y el primer LSR no ha realizado dicha asignación.

El LSR que receptor busca dentro de su tabla de enrutamiento para determinar la asignación de la etiqueta. Este responde al mensaje de asignación con el “enlace” o con un

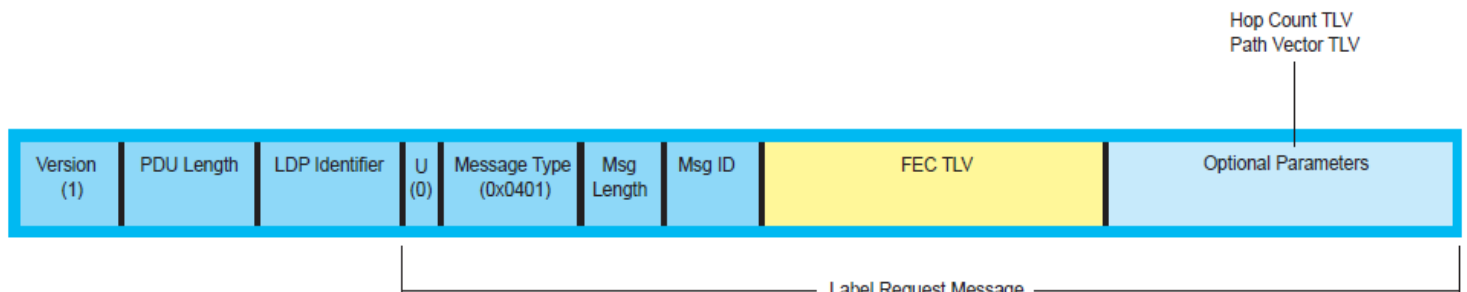


Figura. 4-14 Campos del mensaje de solicitud de etiqueta

mensaje de notificación (Ver Figura. 4-14) indicando el por qué no puede responder a la petición.

4.7.2.4 Mensaje de liberación de etiqueta.

Este tipo de mensaje indica a un par que el LSR no continua utilizando una de las asignaciones de etiquetas que este no haya solicitado o que tampoco ha sido anunciada a él. Una etiqueta es liberada cuando:

- El LSR que anuncio no es más el próximo salto para la FEC anunciada, y el LSR que libera esta en modo de retención de conservación de etiqueta⁷¹.
- Un LSR recibe una asignación de etiqueta proveniente de un LSR que no es más el próximo salto de la FEC.
- Un LSR recibe un mensaje de liberación de etiqueta.

4.7.2.5 Mensaje de retiro de etiqueta

Este mensaje informa a un par que la asignación de etiqueta ya no es reconocida por un LSR, esto se anuncia previamente.

4.8 Clasificación de etiquetas

A diferencia del protocolo IP los paquetes MPLS pueden clasificarse de acuerdo a:

- Direcciones de destino Unicast
- Ingeniería de Trafico
- VPN(Virtual private network – Red virtual privada)
- Calidad de Servicio (QoS)

Por lo tanto, la clase de equivalencia de reenvió o bien Forwarding Equivalence Class (FEC), puede ser representada por:

- El prefijo de dirección de destino
- VPN
- Túneles de Ingeniería de tráfico
- Tipos de servicios.

MPLS trabaja en el núcleo de redes IP. Los routers en el núcleo tienen habilitadas las interfaces MPLS. Las etiquetas son agregadas a los paquetes IP cuando entran a la red IP, y removidas del paquete IP cuando dejan la red.

⁷¹ Conservative label retention mode.

4.9 Intercambio de etiquetas MPLS

Los LSR o routers de conmutación presentes en cada salto dentro de la red tienen la capacidad de alterar la pila de etiquetas que se le es colocada al paquete al ingresar a la red. Debido a esta capacidad se le denomina intercambio de etiquetas al proceso de conmutación basado en MPLS labels.

Para realizar la conmutación basada en etiquetas son necesarias algunas tablas de asignación, como:

- **Mapa de etiquetas entrantes (Incoming Label Map – ILM):** usado en paquetes etiquetados, asigna una etiqueta de llegada a una etiqueta de envío de entrada del próximo salto.(Next Hop Label Forwarding Entry – NHLFE)
- **Asignación de FEC a NHLFE – FTN:** usado para paquete sin etiquetar, asigna una FEC a un NHLFE.

La etiqueta NHLFE contiene, mucha otra información, el próximo salto y una acción que el LSR debe realizar en la pila de etiquetas. Estas acciones pueden ser:

- ✓ Reemplazar la última etiqueta asignada (con una etiqueta nueva que represente una FEC que tenga tanto el mismo LSR de salida en común como la etiqueta reemplazada.)
- ✓ Remover (pop) la etiqueta que ocupe el primer lugar en la pila.
- ✓ Reemplazar la primera etiqueta de la pila e insertar (push) una etiqueta adicional.

4.9.1 Envío de paquetes etiquetados

Cuando llega un paquete etiquetado por un LSP (label switching path – línea de etiquetas conmutadas) e ingresa al LSR, este realiza las siguientes acciones:

1. Busca la etiqueta en el ILM
2. Busca el NHLFE para determinar el próximo salto y acción.

4.9.2 Envío de paquetes sin etiquetar.

Cuando un paquete sin etiquetar llega al LSR, este debe seguir otra serie de procedimientos como son (Ver Figura. 4-15):

1. Determinar la FEC del paquete
2. Asignar la FEC al NHLFE usando FTN (FEC-to-NHLFE)
3. Buscar el NHLFE para determinar el próximo salto y acción a tomar

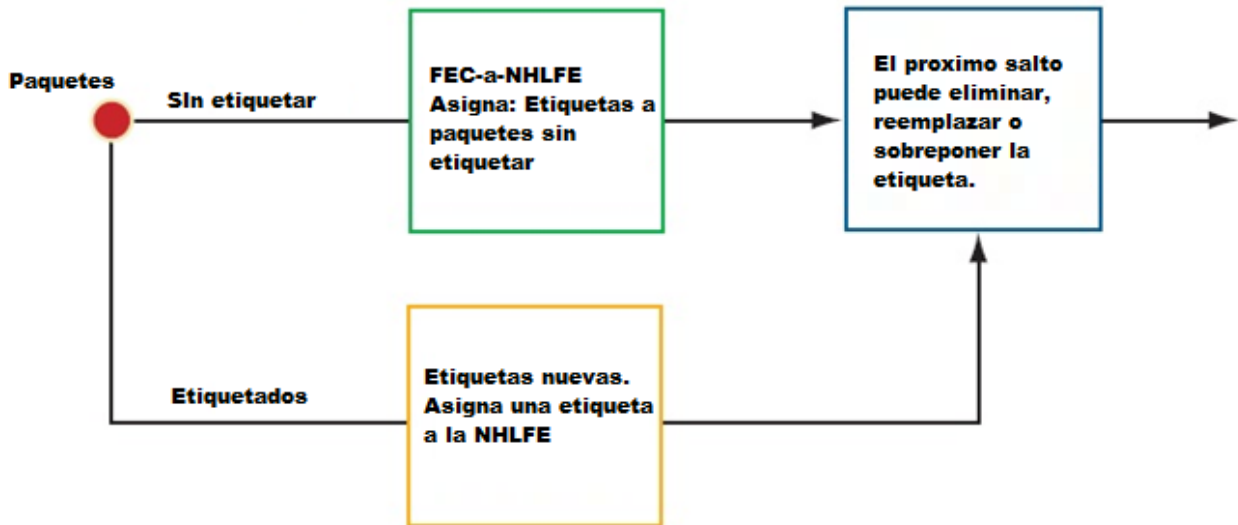


Figura. 4-15 Proceso de envío de paquetes con o sin etiquetas.

4.9.3 Líneas de etiqueta conmutada

Una línea de etiqueta conmutada (LSP) es una secuencia de routers que operan sobre una pila de etiquetas de la misma profundidad (m) desde el ingreso al LSR hasta su salida. Una LSP existe para cada FEC. El LSR de ingreso empuja sobre la pila de etiquetas para crear una profundidad (m), y el penúltimo salto en la línea, es decir el hop antes que la LSP llegue al LSR de salida, remueve la primera etiqueta antes del envío del paquete por la LSP hasta el LSR de salida. En cada salto, la etiqueta colocada de último es usada para referenciar el ILM.

4.10 Ventajas del etiquetado.

Cuando un paquete entra en una red se le es asignado una FEC, la información que no se ha tomado del encabezado de red puede ser utilizada para la asignación de la clase de reenvío. Por ejemplo, la clasificación de paquetes basada en el origen de los paquetes.

Se le puede asignar a los paquetes una etiqueta de prioridad, haciendo posible el control de calidad para Frame Relay y ATM.

Las consideraciones que determinan el cómo al paquete se les asignado una FEC puede volverse muy complejo, sin impactar en afectar a los routers limitándoles meramente a transmitir los paquetes etiquetados.

La carga útil de los paquetes no es examinada por los routers transmisores lo cual permiten el envío para diferentes niveles de tráfico, encriptación y el transporte de protocolos múltiples.

Un paquete puede ser forzado a seguir una ruta específica en lugar de una ruta elegida por el algoritmo dinámico normal mientras el paquete viaja por la red.

4.11 Calidad de servicio

La calidad de servicio de MPLS no define una nueva arquitectura de QoS. Se aprovecha la arquitectura DiffServ⁷² QoS IP y la aplica a la red MPLS. MPLS utiliza el campo EXP en el encabezado en lugar del campo DSCP utilizados por IP.

En DiffServ, el usuario marca los paquetes con un determinado nivel de prioridad; los routers van agregando las demandas de los usuarios y propagándolas por el trayecto. Esto le da al usuario una confianza razonable de conseguir la QoS solicitada.

FTOS⁷³ soporta DSCP⁷⁴ en redes IP y EXP en redes MPLS. Cuando DSCP es configurado, EXP es usado para habilitar y tomar este valor de los parámetros DSCP. Si DSCP no está habilitado, EXP no está habilitado.

El campo EXP ocupa 3bits en el encabezado MPLS mientras que el campo DSCP utiliza 6 bits en el encabezado IP. Esta diferencia es administrada de dos formas que son E-LSP y L-LSP. Ambas pueden usar ya sea LDP o RSVP para señalar y distribuir etiquetas.

Existen tres modelos de túneles: uniforme, Pipa, y Pipa corta. FTOS se pueden implementar utilizando los modelos de pipa corta y uniforme

En el caso de de los modelos de pipa y pipa corta, ningún condicionamiento de trafico afecta el bit EXP mientras el trafico cruzar a través del túnel. En otras palabras, cuando el trafico sale de un LSP o cuando el trafico entra en un LSP, el contador o campo EXP no es cambiado.

Los modelos pipa y pipa corta difieren en el encabezado que el túnel de salida utiliza cuando este determina el PHB (Per-hop behavior, comportamiento por salto) de un paquete entrante. Con el modelo de pipa corta, el túnel de salida usa un encabezado interno que es usado para la retransmisión. Con el modelo de pipa, la etiqueta mas externa es utilizada.

El modelo uniforme es el vecino por defecto de FTOS; el valor DSCP del paquete IP es propagado al el campo experimental de bits de MPLS.

⁷² DiffServ= Servicios Diferencias es un estándar aparte de MPLS.

⁷³ FTOS= Force 10 Operative Systema – Es un sistema operativo.

⁷⁴ DSCP= Differentiated Services Code Point – Servicios diferencias de punto de código. Hace referencia al segundo byte en la cabecera de los paquetes IP que se utiliza para diferenciar la calidad en la comunicación que quieren los datos que se transportan.

4.12 Servicio telefónico implementado en redes MPLS.

MPLS puede ser implementado para transportar paquete de voz sin la necesidad del encabezado típico correspondiente a RTP/UDP/IP. Existen 3 métodos para el transporte de paquetes de voz en la red MPLS, que son:

- A. En el primer método, los datos de voz son transmitidos usando H.323 siendo este el método de encapsulamiento de capa más alto, el proceso de envío involucra el encapsulamiento inicial del dato como paquete IP que luego ingresa a la red MPLS y es dirigido a través de etiquetas.⁷⁵
- B. El segundo método consiste en la encapsulación por medio de H.323 sin involucrar el concepto IP. Se utiliza un mecanismo de tunelización en una red virtual privada MPLS para establecer las bases de LSP.
- C. El tercer método se basa en una configuración muy similar a transmisión de voz sobre una red ATM, donde los bits de voz son llegados directamente en el paquete MPLS.

Cuando distintas comunicaciones de voz son transportadas entre los 2 mismos puntos finales y 2 gateway (Ver Figura. 4-16) concatenan el flujo de paquetes de voz, esto ayuda a la reducción del encabezado de encapsulamiento.

En el caso de paquetes de voz en redes IP, los encabezados RTP/UDP/IP pueden ser comprimidos usando diferentes algoritmos como IP Header Compression⁷⁶, Compressed RTP⁷⁷, Enhanced Compressed RTP⁷⁸, Robust Header Compression⁷⁹, y otros definidos en RFCs o borradores de Internet.

La concatenación puede ser implementada en diferentes protocolos de capas. Por ejemplo, concatenación IP (CIP) y encapsulación de peso ligero IP (LIPE) concatenan paquetes de voz sobre IP, mientras que la multiplexación de protocolo punto a punto implementa concatenación de capa 2.

⁷⁵ La desventaja de este método es la carga al tráfico que se genera producto de la existencia innecesario del campo de secuencia de H.323

⁷⁶ Compresión de encabezado IP.

⁷⁷ RTP compreso

⁷⁸ RTP a mayor compresión

⁷⁹ Compresión robusta de encabezado

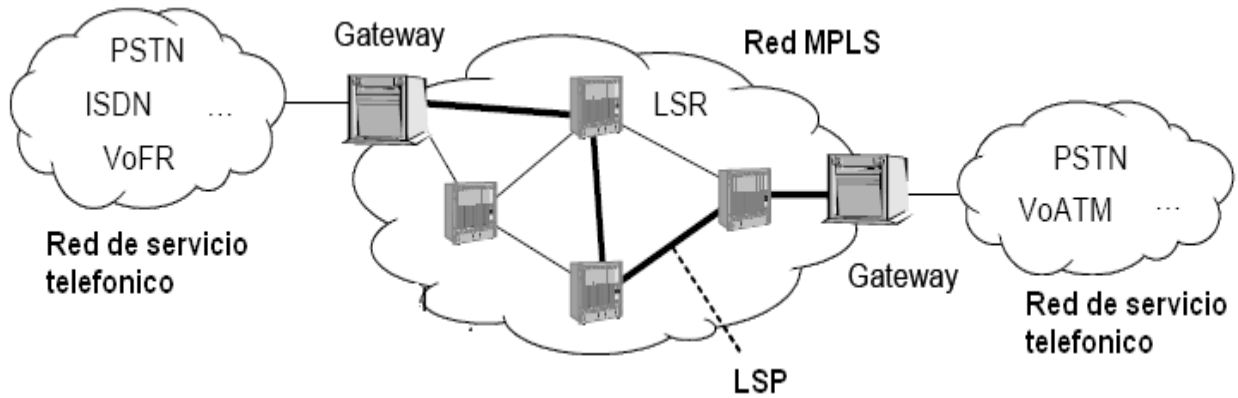


Figura. 4-16 Arquitectura de referencia de Voz sobre red MPLS.

Al implementar el servicio de voz sobre una red MPLS, 2 grandes soluciones pueden ser propuestas para concatenar. La primera se define en un escenario en donde se ha realizado una alianza entre MPLS y Frame Relay. Este tipo de red soporta el transporte de canales de voz multiplexados, varios algoritmos de compresión de voz, retiro de silencios y descriptores de inserción de silencios, transferencia de los dígitos marcados, y señalización asociada a los canales. Cada paquete de voz concatenado es precedido por un encabezado de 4 octetos que incluye un canal de identificación, un campo de tipo, un contador, y un campo de longitud. (Ver Figura. 4-17).

Si la longitud no es múltiplo de 4 octetos, 32 bits son incluidos para completar la dirección. Hasta 248 llamadas pueden ser multiplexadas dentro de un LSP identificado por la etiqueta de salida MPLS. Como una opción de implementación, LSPs interiores adicionales pueden ser creados utilizando pilas de etiqueta.

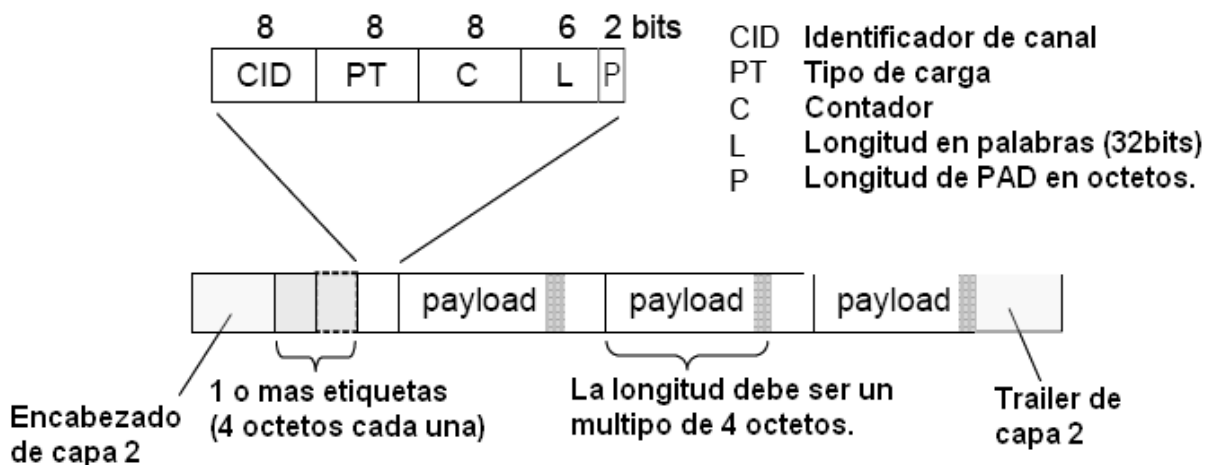


Figura. 4-17 Voz sobre red MPLS (Alianza MPLS-Frame Relay)

La segunda solución es a través de direcciones con funciones similares, este nuevo formato de encapsulamiento utiliza componentes de una adaptación de capa ATM tipo 2 (AAL2), definida para el transporte de diferentes y variables tasa de transmisión de bits de

voz y flujo de datos multiplexados sobre una conexión ATM. El concepto de AAL2 sobre MPLS es muy similar al concepto de AAL2 sobre ATM pero reemplaza las conexiones con los LSPs de MPLS, de tal forma que el encabezado de las celdas ATM es eliminado.

4.13 Preguntas de control.

1. ¿Qué es MPLS?
2. ¿Cuáles son los campos del encabezado MPLS? Explique brevemente cada uno.
3. ¿Cuáles son los componentes de MPLS? Describa sus funciones brevemente.
4. ¿Cómo opera una red MPLS? Ejemplifique.
5. ¿Cómo se crean las etiquetas MPLS?
6. ¿Qué es un Espacio de Etiquetas?
7. ¿Qué es un LSR?
8. ¿Cuándo un LSR es de egreso?
9. Explique el proceso de distribución de etiquetas.
10. Describa las funciones de:
 - Mensaje Hello
 - Mensaje de Inicialización
 - Mensaje de Notificación
 - Mensaje de dirección
11. ¿Qué son mensajes de distribución de etiquetas?
12. ¿Cuáles son los mensajes de distribución de etiqueta?
13. Explique brevemente las funciones de los mensajes:
 - Mensajes de dirección
 - Mensaje de asignación de etiqueta
 - Mensaje de solicitud de etiqueta
 - Mensaje de liberación de etiqueta
 - Mensaje de retiro de etiqueta
14. ¿Qué parámetros se utilizan para crear la clasificación de etiquetas?
15. ¿Cómo se lleva a cabo el intercambio de etiquetas?
16. ¿Cuáles son las ventajas del etiquetado?
17. ¿Cómo se establecen los parámetros de calidad de servicio en redes MPLS?

Abreviaturas

ID	Acrónimo	Descripción
i.	LAN	Local Area Network – Red de área local
ii.	WAN	Wide Area Network – Red de Área Amplia
iii.	MAN	Metropolitan Area Network – Red de Área Metropolitana
iv.	FTP	File Transfer Protocol – Protocolo de transferencia de archivo.
v.	ISP	Internet Service Provider – Proveedor de servicios de Internet
vi.	VPN	Private Virtual Network – Red Privada Virtual
vii.	IrDa	Infrared Data Association – Asociación de datos Infrarrojos
viii.	RTP	Real Time Transfer Protocol = Protocolo de Transferencia en Tiempo real
ix.	RTCP	Real Time Control Protocol = Protocolo de Control de Transferencia en Tiempo real.
x.	IP	Internet Protocol – Protocolo de Internet
xi.	UDP	User Datagram Protocol – Protocolo de unidad de datagrama
xii.	SIP	Session Initiation Protocol – Protocolo de Inicio de Sesión.
xiii.	PBX	Private Branch Exchange - Central Privada de Conmutación.
xiv.	OSI	Open System Interconnection – Sistema Abierto de Interconexión
xv.	NSAP	Network Service Access Point – Punto de Acceso de Servicio de Red.
xvi.	CSMA/ CD	Carrier Sense Multiple Access/ Colission Deteccion – Acceso múltiple por detección de portadora/ Detección de Colisión
xvii.	CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance - Acceso múltiple por detección de portadora/ Anticolisión
xviii.	RTS	Request To Send – Pregunta para enviar.
xix.	CTS	Clear To Send – Despeja para enviar.
xx.	DSL	Digital Subscriber Line – Línea Digital de suscriptor.
xxi.	DHCP	Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Hosts.
xxii.	MTA	Mail Transport Agent – Agente de Transporte de Correo
xxiii.	MDA	Mail Delivery Agent – Agente de entrega de correo.
xxiv.	PPP	Point to Point Protocol - Protocolo Punto a Punto
xxv.	HTTP	Hypertext Transfer Protocol – Protocolo de Transferencia de HyperTexto.
xxvi.	DNS	Domain Name Server – Servidor de Nombre de Dominio
xxvii.	SMTP	Simple Mail Transfer Protocol – Protocolo Simple de Transferencia de Correo
xxviii.	SNMP	Simple Network Management Protocol – Protocolo Simple de Administración de Red.
xxix.	Telnet	Telecommunication Network – Red de Telecomunicación
xxx.	NFS	Network File System - Sistema de archivos Via Red
xxxi.	POP	Post Office Protocol – Protocolo de la Oficina de Correo
xxxii.	WWW	World Wide Web - Red Mundial Amplia.
xxxiii.	MPLS	Multi-Protocol Label Switching – Conmutación de etiquetas multi-protocolos.
xxiv.	LSP	Label switched path – rutas de conmutación de etiqueta.
xxxv.	IGP	Interior Gateway Protocol – Protocolo de Pasarela Interior
xxvi.	FEC	Forwarding Equivalence Class
xxvii.	LDP	Label Distribution Protocol. – Protocolo de Distribución de Etiquetas

Bibliografía

- ALEGSA. (27 de Agosto de 2010). *Alegsa.com.ar*. Recuperado el 10 de Abril de 2011, de <http://www.alegsa.com.ar/Dic/protocolo%20punto%20a%20punto.php>
- Alvarez, M. A. (1998). *DesarrolloWeb*. Recuperado el 14 de Octubre de 2010, de <http://www.desarrolloweb.com/faq/que-es-proxy.html>
- CISCO. (2008). Aspectos basicos de networking. En CISCO, *CCNA Exploration 4.0* (pág. 241).
- CISCO. (2008). *Aspectos basicos de Networking*. United States: CISCO academy.
- CISCO. (2008). Ejemplos de herramientas de comunicacion mas populares. En JoseMaria36, *Conceptos Basicos de Networking* (pág. 7).
- CISCO. (2008). Redes de are amplia. En JoseMaria36, *Aspectos basicos de networking* (pág. 42).
- ckp. (24 de Febrero de 2006). *Conectivity Knowledge Platform*. Recuperado el 1 de Noviembre de 2010, de <http://ckp.made-it.com/ieee8022.html>
- Company, T. N. (2010). *About.com*. Recuperado el 12 de 10 de 2010, de <http://compnetworking.about.com/od/basicnetworkingconcepts/1/aa021403a.htm>
- dns.bdat.net. (s.f.). *dns.bdat.net*. Recuperado el 6 de Junio de 2011, de http://dns.bdat.net/seguridad_en_redes_inalambricas/x59.html
- Fábrega, P. P. (Abril de 2003). *dns.bdat.net*. Recuperado el 6 de Junio de 2011, de <http://dns.bdat.net/dhcp/x84.html>
- FarSite Communications. (20 de Enero de 2010). *FarSite Communications*. Recuperado el 19 de Noviembre de 2010, de http://www.farsite.com/cable_standards/v.24_rs232c.shtml
- GoldenInk. (s.f.). *Golden Ink*. Recuperado el 12 de 10 de 2010, de <http://goldenink.com/computersandnetworks2.shtml>
- GS Comunicaciones. (1999). *Telecomunicaciones: Redes de Datos*. D.F Mexico: Mc Graw Hill.
- Kevin Vergara. (6 de Mayo de 2007). *Blog informatico*. Recuperado el 1 de Noviembre de 2010, de <http://www.bloginformatico.com/topologia-de-red.php>
- Kioskea.net. (16 de Octubre de 2008). *Kioskea.net*. Recuperado el 6 de Junio de 2011, de <http://es.kioskea.net/contents/courrier-electronique/regles-bon-usage-messagerie.php3>

- Masadelante. (1999). *Masadelante*. Recuperado el 14 de Octubre de 2010, de <http://www.masadelante.com/faqs/host>
- Masadelante. (1999). *Masadelante*. Recuperado el 14 de Octubre de 2010, de <http://www.masadelante.com/faqs/modem>
- Masadelante. (2011). *Masadelante*. Recuperado el 6 de Junio de 2011, de <http://www.masadelante.com/faqs/servidores-ftp>
- Microsoft. (2011). *Technet*. Recuperado el 7 de Junio de 2011, de [http://technet.microsoft.com/es-es/library/cc787434\(WS.10\).aspx](http://technet.microsoft.com/es-es/library/cc787434(WS.10).aspx)
- Microsoft. (2011). *Technet*. Recuperado el 7 de Junio de 2011, de [http://technet.microsoft.com/es-es/library/cc776674\(WS.10\).aspx](http://technet.microsoft.com/es-es/library/cc776674(WS.10).aspx)
- Mitchell, B. (2010). *About.com*. Recuperado el 3 de Noviembre de 2010, de http://compnetworking.about.com/od/hardwarenetworkgear/g/bldef_switch.htm
- Mitchell, B. (2010). *About.com*. Recuperado el 3 de Noviembre de 2010, de http://compnetworking.about.com/cs/internetworking/g/bldef_hub.htm
- Palet, J. (Mayo de 1997). *consulintel*. Recuperado el 10 de Abril de 2010, de http://www.consulintel.es/html/Tutoriales/Articulos/tutorial_fr.html
- Ronces, F. R., & Reyes Santos, A. R. (12 de Marzo de 2009). *SlideShare Inc.* . Recuperado el 21 de Abril de 2011, de <http://www.slideshare.net/almars/capa-de-aplicacion-tcpip>
- Stallings, W. (2004). *Comunicaciones y redes de Computadores*. Madrid: Pearson Educacion S.A.
- Tanenbaum, A. S. (2003). *Redes de Computadoras*. Amsterdam: Prentice Hall.
- TECH - FAQ. (4 de Junio de 2011). *TECH - FAQ*. Recuperado el 11 de Junio de 2011, de <http://www.tech-faq.com/jitter.html>
- Universidad de Valencia. (2009). *Seguridad en Redes Inalambricas*. Valencia.
- Universidad Nacional Autonoma de Mexico. (s.f.). *Multimania*. Recuperado el 5 de Octubre de 2010, de <http://usuarios.multimania.es/aledomiisa/historia.php>
- Universidad Politecnica SALESIANA. (2004). *Repositorio Digital*. Recuperado el 24 de Abril de 2011, de <http://dspace.ups.edu.ec/bitstream/123456789/209/3/Capitulo%202.pdf>
- University of South Florida. (s.f.). *fcit*. Recuperado el 12 de 10 de 2010, de <http://fcit.usf.edu/network/chap1/chap1.htm>
- Ureña Poirier, H., & Rodriguez, J. F. (2005). *Gobierno de Canarias*. Recuperado el 2 de Noviembre de 2010, de

http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/topolog.htm

- Wetcom Group. (2011). *Wetcom*. Recuperado el 6 de Junio de 2011, de <http://www.wetcom.com.ar/content/cisco-lanza-nuevo-router-crs-con-escalabilidad-hasta-los-322tbps/>
- Whatls.com. (8 de Octubre de 2009). *SearchSecurity.com*. Recuperado el 4 de Noviembre de 2010, de http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212125,00.html
- Wikipedia - CSMA. (5 de Octubre de 2010). *La enciclopedia libre*. Recuperado el 20 de Noviembre de 2010, de http://en.wikipedia.org/wiki/Carrier_sense_multiple_access
- Wikipedia - Enlace de datos. (18 de Junio de 2010). *La enciclopedia libre*. Recuperado el 20 de Noviembre de 2010, de http://en.wikipedia.org/wiki/Data_Link_Layer
- Wikipedia - Ethernet. (15 de Octubre de 2010). *La enciclopedia libre*. Recuperado el 20 de Noviembre de 2010, de http://en.wikipedia.org/wiki/Ethernet_physical_layer
- Wikipedia. (12 de Diciembre de 2009). *La enciclopedia libre*. Recuperado el 10 de Octubre de 2010, de http://es.wikipedia.org/wiki/Computaci%C3%B3n_distribuida
- Wikipedia. (31 de Octubre de 2010). *La Enciclopedia libre*. Recuperado el 19 de Noviembre de 2010, de www.wikipedia.com
- Wikipedia. (11 de Mayo de 2011). *La enciclopedia libre*. Recuperado el 6 de Junio de 2011, de http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet#Retardo_o_latencia
- Wikipedia. (10 de Abril de 2011). *La enciclopedia Libre*. Recuperado el 10 de Abril de 2011, de http://es.wikipedia.org/wiki/Asynchronous_Transfer_Mode
- Wikipedia, L. e. (6 de Junio de 2011). *La enciclopedia Libre*. Recuperado el 13 de Junio de 2011, de http://es.wikipedia.org/wiki/Open_Shortest_Path_First

-
- ⁱ LAN = Local Area Network – Red de área local
 - ⁱⁱ WAN = Wide Area Network – Red de Área Amplia
 - ⁱⁱⁱ MAN = Metropolitan Area Network – Red de Área Metropolitana
 - ^{iv} CSMA/ CD = Carrier Sense Multiple Access/ Colission Deteccion – Acceso múltiple por detección de portadora/
Detección de Colisión
 - ^v CSMA/CA =Carrier Sense Multiple Access/ Collision Avoidance - Acceso múltiple por detección de portadora/
Anticolisión
 - ^{vi} RTS = Request To Send – Pregunta para enviar.
 - ^{vii} CTS = Clear To Send – Despeja para enviar.
 - ^{viii} IrDa = Infrared Data Association – Asociación de datos Infrarrojos
 - ^{ix} FTP = File Transfer Protocol – Protocolo de transferencia de archivo.
 - ^x ISP = Internet Service Provider – Proveedor de servicios de Internet
 - ^{xi} VPN = Private Virtual Network – Red Privada Virtual
 - ^{xii} RTP = Real Time Transfer Protocol = Protocolo de Transferencia en Tiempo real
 - ^{xiii} ^{xiii} RTCP = Real Time Control Protocol = Protocolo de Control de Transferencia en Tiempo real.
 - ^{xiv} IP = Internet Protocol – Protocolo de Internet
 - ^{xv} UDP = User Datagram Protocol – Protocolo de unidad de datagrama
 - ^{xvi} SIP= Session Initiation Protocol – Protocolo de Inicio de Sesión.
 - ^{xvii} PBX = Private Branch Exchange - Central Privada de Conmutación.
 - ^{xviii} NSAP = Network Service Access Point – Punto de Acceso de Servicio de Red.
 - ^{xix} PPP= Point to Point Protocol - Protocolo Punto a Punto
 - ^{xx} DSL = Digital Subscriber Line – Línea Digital de suscriptor.
 - ^{xxi} DHCP = Dynamic Host Configuration Protocol – Protocolo de Configuración Dinámica de Hosts.
 - ^{xxii} HTTP = Hypertext Transfer Protocol – Protocolo de Transferencia de HyperTexto.
 - ^{xxiii} DNS = Domain Name Server – Servidor de Nombre de Dominio
 - ^{xxiv} SMTP = Simple Mail Transfer Protocol – Protocolo Simple de Transferencia de Correo
 - ^{xxv} SNMP = Simple Network Management Protocol – Protocolo Simple de Administración de Red.
 - ^{xxvi} Telnet = Telecommunication Network – Red de Telecomunicación
 - ^{xxvii} NFS = Network File System - Sistema de archivos Via Red
 - ^{xxviii} POP = Post Office Protocol – Protocolo de la Oficina de Correo
 - ^{xxix} WWW = World Wide Web - Red Mundial Amplia.
 - ^{xxx} MTA = Mail Transport Agent – Agente de Transporte de Correo
 - ^{xxxi} MDA = Mail Delivery Agent – Agente de entrega de correo.
 - ^{xxxii} MPLS = Multi-Protocol Label Switching – Conmutación de etiquetas multi-protocolos.
 - ^{xxxiii} LSP = Label switched path – rutas de conmutación de etiqueta.
 - ^{xxxiv} IGP = Interior Gateway Protocol – Protocolo de Pasarela Interior
 - ^{xxv} FEC = Forwarding Equivalence Class
 - ^{xxvi} LDP = Label Distribution Protocol. – Protocolo de Distribución de Etiquetas