Tres reglas en seguridad.

- **No existen sistemas absolutamente seguros.**
- **Para reducir su vulnerabilidad a la mitad se tiene que doblar el gasto en seguridad.**
- **Típicamente, los intrusos *brincan* la criptografía, no la rompen.**

[Francisco Rodríguez Enríquez]

CAPÍTULO 1
Conceptos Básicos

La seguridad es un aspecto primordial que no sólo se considera en el ámbito del cómputo, actualmente las organizaciones y sus sistemas de información se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes por medios tecnológicos, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o denegación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La seguridad significa que el costo para romperla excede al costo del bien de cómputo asegurado, esto es, el tiempo requerido para romper la seguridad excede el tiempo de vida útil del bien de cómputo, siendo éste último hardware, software o información.

1.1. Redes de datos

El concepto red actualmente es mencionado prácticamente en cualquier lugar, la razón es simple y sencilla, se vive en un mundo rodeado de redes y no se hace referencia sólo en el ámbito de la computación, pues el concepto se amplía más allá, como lo es en el hogar, la educación, el transporte, comunicaciones, banca, transacciones y servicios. Por ejemplo, una red carretera que permite conectar ciudades, redes telefónicas, redes eléctricas entre otras más.

Desde el punto de vista de la computación, una red de datos es un conjunto de computadoras autónomas interconectadas física y lógicamente para facilitar el intercambio y procesamiento de la información.

La importancia radica en el hecho de que se han convertido desde hace algunas décadas en una necesidad en cualquier ámbito, por ejemplo, el crecimiento económico de una empresa mucho se debe al adecuado uso de la mercadotecnia haciendo uso de la redes para alcanzar nuevos mercados, por lo que han permitido un impacto económico en las distintas áreas. Actualmente las redes de datos son una indiscutible necesidad en cualquier sector, por lo que cada día seguirán evolucionando y alcanzando nuevas fronteras.

Actualmente las redes de datos brindan comunicación inmediata casi en cualquier parte de la tierra, esto gracias a la versatilidad de la misma, emplean diferentes medios que se utilizan para su transmisión por medios físicos e inalámbricos, siendo estos últimos empleados día a día en mayor volumen. En el caso de los medios físicos, éstos tienen características especiales que los diferencian de los inalámbricos, como mayor velocidad de transferencia, disponibilidad y área de cobertura.

Las redes de datos se clasifican con base en su forma de transmisión en redes cableadas e inalámbricas, dentro de éstas existen clasificaciones tomando en cuenta su topología, alcance, medio de transmisión y velocidad.

Las características más importantes de las redes cableadas son:

- Se utilizan cables como medios para la transmisión (fibra óptica y cables de cobre como UTP [Unshielded Twisted Pair - Cable de par trenzado] y coaxial).
- Existen distintos estándares como son IEEE 802.3 (Ethernet), IEEE 802.4 (Token Bus), IEEE 802.5 (Token Ring), del estándar 802.3 se derivan otros estándares de acuerdo con la velocidad de transferencia de datos y tipo de medio utilizado como son Fast Ethernet IEEE 802.3, Gigabit Ethernet IEEE 802.3z.
- Por su alcance se clasifican en redes LAN (Local Area Network –Redes de Área local), WAN (Wide Area Network- Redes de Área Amplia), MAN (Metropolitan Area Network-Redes de Área Metropolitana) entre algunas otras.
- Las topologías comunes son: Bus, estrella, anillo, árbol, malla, etcétera.
- Permiten grandes velocidades de transmisión hasta 1 Gbps, actualmente existe equipos que permiten enlaces 10Gps.

Las características más importantes de las redes inalámbricas son:

- Utiliza el aire como medio de transmisión.
- Diferentes velocidades de transmisión, desde 2 hasta 300 Mbps.
- Movilidad.
- Flexibilidad en la instalación.
- Escalabilidad.
- Bajo costo de implementación.

En la figura 1.1 se observa un diagrama en el cual se muestra la clasificación de las redes.

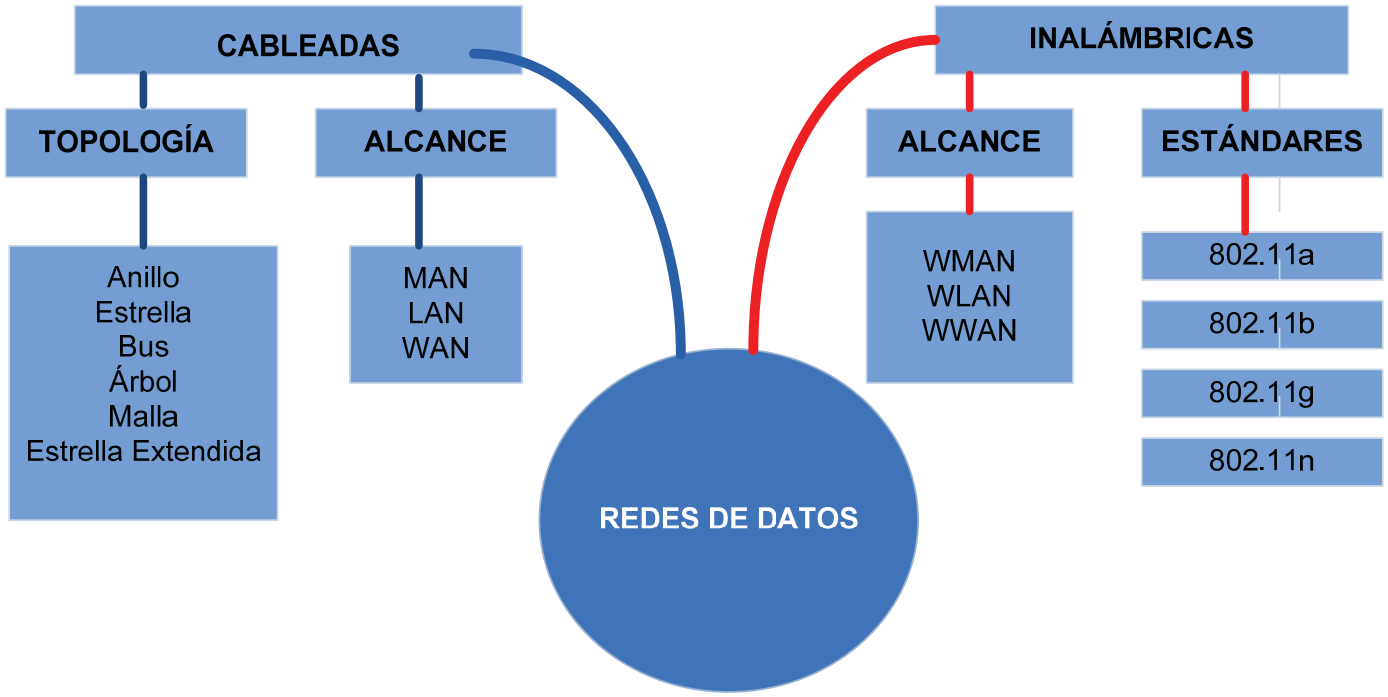

Figura 1. 1 Clasificación de las redes por alcance, topología y estándar.

1.1.1. Conceptos básicos

Dentro del mundo de las redes se manejan conceptos que permiten comprender el proceso de interacción entre los distintos dispositivos que comprenden una red.

Enseguida se describen algunos conceptos que frecuentemente se encuentran relacionados con las redes datos.

a) Dirección física

La dirección física es un término de uso común en las redes de datos, de acuerdo con la definición de redes de datos, para formar una red, los equipos de cómputo deben estar interconectados a través de una interfaz que les permite comunicarse, esta interfaz se conoce como tarjeta de red o también denominada NIC (Network Interface Controller – Controlador de interfaz para red).

Cada tarjeta de red NIC tiene asignado un identificador único llamado MAC (Media Access Control – control de acceso al medio), o dirección física, dicha dirección está formada por 48 bits y para mayor facilidad de su representación se utiliza el sistema hexadecimal, por lo que se utilizan 12 dígitos.

Los seis primeros dígitos hexadecimales, que son administrados por el IEEE (Institute of Electrical and Electronics Engineers - Instituto de ingenieros eléctricos y electrónicos), identifican al fabricante o proveedor y, de ese modo, abarcan el *Identificador Exclusivo de Organización* (*OUI*). Los seis dígitos hexadecimales restantes abarcan el *número de serie de interfaz*, u otro valor administrado por el proveedor específico. Las direcciones MAC, como identificador, son grabadas en una memoria de sólo lectura en la tarjeta de red. Un ejemplo de dicha dirección se presenta en la figura 1.2.

Figura 1. 2 Dirección física (MAC Address).

No existen direcciones físicas iguales, sin estos identificadores únicos sería complicado determinar a quién le será entregado un paquete, por lo que cuando un equipo envía información, ésta es encapsulada agregando las direcciones MAC Address origen y destino. La información no se puede enviar o entregar de forma adecuada en una red si no tiene esas direcciones.
Si se desea obtener el nombre de algún fabricante a partir de la dirección MAC Address, se puede realizar la búsqueda desde el sitio http://standards.ieee.org/regauth/oui/index.shtml, es importante este dato en auditorías y seguimiento de incidentes.

b) Dirección IP

Cuando un equipo de cómputo desea enviar un paquete a otro equipo, dicho paquete deberá contener la dirección destino y origen, ya que sin esto no sería posible que el paquete llegue a su destino. La dirección IP (Internet Protocol – Protocolo de internet) contiene la información necesaria para enrutar un paquete a través de la red TCP/IP (Transmission Control Protocol/Internet Protocol – Protocolo de control de transmisión/ Protocolo de Internet).

La dirección IPv4 es representada por 32 bits, dicha dirección comúnmente es representada utilizando notación decimal, se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal máximo de cada octeto es 255, reservando este número para envió broadcast.

Los campos que componen a una dirección IP son identificador de red (Network ID) e identificador de host (host ID), el número de red de una dirección IP identifica la red a la cual pertenece dicho dispositivo. El host ID de una dirección IP identifica el dispositivo específico de una red.

Existen tres clases de direcciones IP A, B, C, que una organización puede recibir de parte del Registro Americano de Números de Internet (ARIN) o ISP de la organización (Ver tabla 1.1).

Tabla 1. 1 Direcciones IP.

Tipo	Dirección menor	Dirección más alta	Máscara de Red	Numero de host por red
A	0.0.0.0	126.0.0.0	255.0.0.0	16,777,214
B	128.0.0.0	191.255.0.0	255.255.0.0	65,534
C	192.0.0.0	223.255.255.0	255.255.255.0	254
D	224.0.0.0	239.255.255.255	No aplica	No aplica
E	240.0.0.0	247.255.255.255	No aplica	No aplica

Adicional a estas direcciones IP, existe otra clasificación, utilizada en la asignación de IP mediante NAT, para generar intranet en las organizaciones, las direcciones privadas son:

Tabla 1. 2 Direcciones IP privadas.

Tipo	Dirección menor	Dirección más alta	Máscara de Red
A	10.0.0.0	10.255.255.255	255.0.0.0
B	172.16.0.0	172.31.255.255	255.255.0.0
C	192.168.0.0	192.168.255.255	255.255.255.0

c) Resolución de direcciones

Cada equipo conectado a la red tiene una dirección física única, además de tener una dirección IP, por lo que cuando un equipo desea transmitir un paquete de información a otro debe existir un mecanismo que relacione ambas direcciones mencionadas, la dirección física con la dirección IP para que la información llegue al destino correcto (Figura 1.3).

Este proceso se realiza en la capa de red (modelo OSI) o en la capa de enlace de red (modelo TCP/IP) mediante el protocolo ARP (Address Resolution Protocol – Protocolo de resolución de dirección), el cual se encarga de asociar la dirección física a una determinada dirección IP, si el equipo destino está ubicado dentro de la red local, el equipo origen envía un mensaje a todos los equipos preguntando a quién le corresponde dicha dirección IP, el equipo destino responde a dicho mensaje agregando su dirección MAC.

Sin embargo, cuando la dirección destino no pertenece al mismo segmento de red, para que un dispositivo envíe datos a la dirección MAC de un dispositivo que está ubicado en otro segmento de la red, el dispositivo origen envía los datos a un gateway por defecto. El gateway por defecto es la dirección IP de la interfaz del router conectada al mismo segmento de red física que el host origen. El host origen compara la dirección IP destino con su propia dirección IP para determinar si las dos direcciones IP se encuentran ubicadas en el mismo segmento. Si el dispositivo receptor no está ubicado en el mismo segmento, el dispositivo origen envía los datos al gateway por defecto.

Si la dirección de subred es distinta, el router responderá con su propia dirección MAC a la interfaz que se encuentra directamente conectada al segmento en el cual está ubicado el host origen. Dado

que la dirección MAC no está disponible para el host destino, el router suministra su dirección MAC para obtener el paquete. Luego el router puede enviar la petición ARP (basándose en la dirección IP destino) a la subred adecuada para que se realice la entrega.

Existe otro protocolo RARP (Reverse Address Resolution Protocol –Protocolo de resolución de dirección de retorno) que funciona de manera inversa, para este caso debe existir un servidor que mantiene una base de datos de correspondencia de direcciones MAC a direcciones IP.

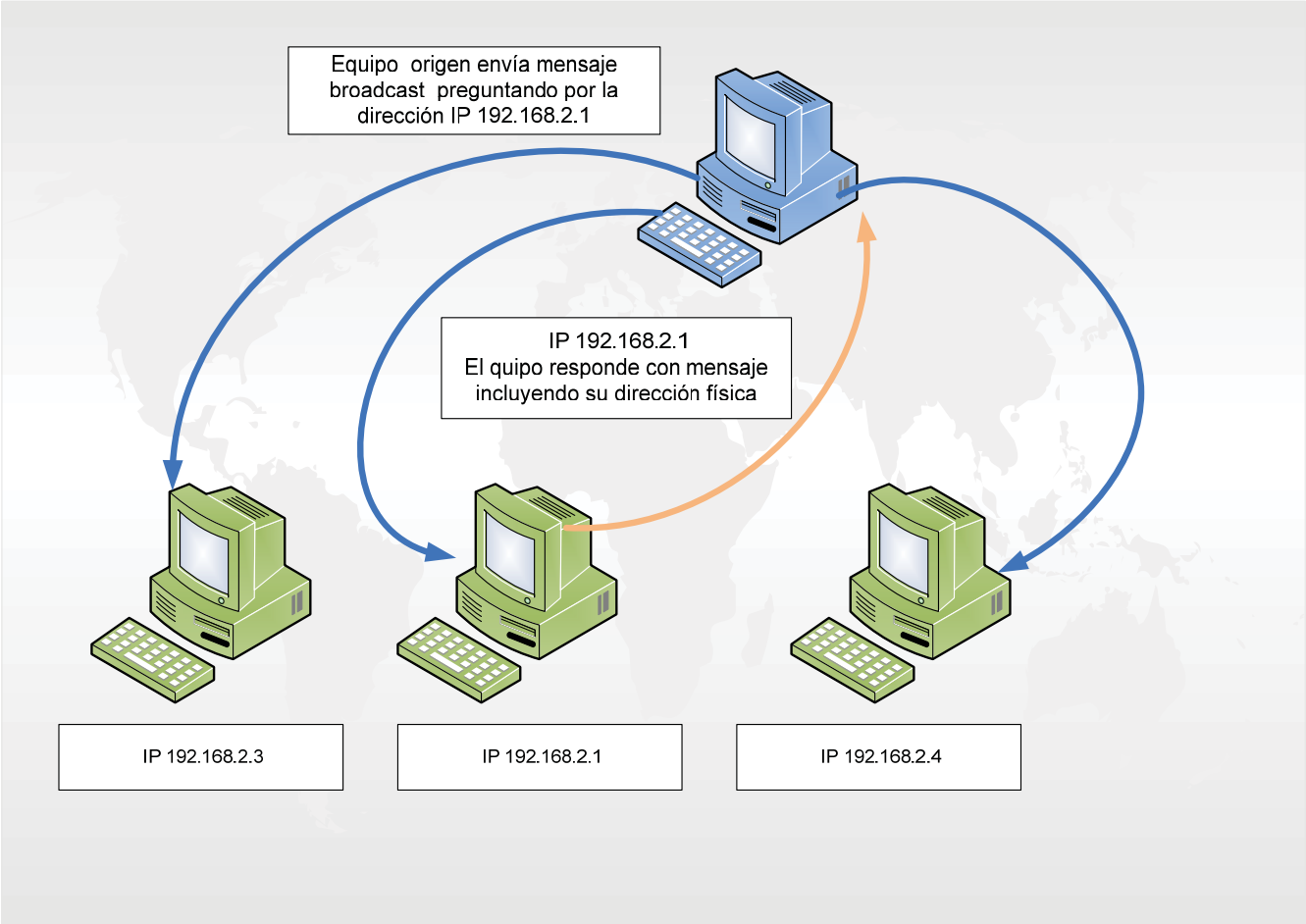

Figura 1. 3 Resolución de direcciones.

d) Definición de protocolo

En todo proceso de comunicación es necesario seguir reglas para poder comprender el intercambio de información, por ejemplo para poder entablar una conversación es necesario que los interlocutores hablen el mismo idioma , ya que si no fuese así no podrían comunicarse entre ellos.

Se presenta la misma situación en las redes de datos, en el momento en que dos equipos intenten comunicarse deberán seguir ciertas reglas para establecer el proceso de intercambio de información, a este proceso se le conoce como protocolo.

Un protocolo, en el contexto de las telecomunicaciones, es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente. Una definición técnica de un protocolo de

comunicaciones de datos es: un conjunto de normas, o un acuerdo, que determina el formato y la transmisión de datos.[1]

Cabe mencionar que existen distintos protocolos y cada uno de ellos tiene una tarea en específico.

e) Definición de puertos

Cuando un programa cliente necesita de un servicio particular de un servidor, además del tipo de servicio y localización del servidor, debe indicar el puerto por el que se establecerá la conexión. En este sentido, un puerto es un canal lógico de comunicación que permite a dos equipos intercambiar información.

Los puertos son representados con un valor numérico y se representan mediante una palabra de 2 bytes, por lo que existen 2^{16}, es decir 65535 puertos, existe una organización que se encarga de regular dichos puertos conocida como IANA (Internet Assigned Numbers Authority -Agencia de asignación de números de internet), dicha organización realiza una clasificación de los puertos en:

- Puertos bien conocidos, definidos del puerto 1 al 1023, utilizados para servicios bien conocidos como web, correo electrónico, etcétera.
- Puertos registrados, definidos del puerto 1024 al 49151, utilizados por aplicaciones conocidas y registrados en IANA, como es el caso de DB (Database – Base de datos), escritorio remoto, RADIUS, etcétera.
- Puertos dinámicos y/o privados del puerto 49152 al 65535.

f) Definición de puerta de enlace

El gateway o puerta de enlace es el encargado de interconectar distintas redes utilizando distintos protocolos, es el punto de la red que permite la entrada a otra red, el gateway se asocia al router (dispositivo de capa tres) sin embargo, el gateway es capaz de enlazar redes con diferentes protocolos, además de que este dispositivo puede trabajar en los siete niveles del modelo OSI.

Los gateways pueden ser personalizados para realizar una función específica, por ejemplo para una conversión de protocolos, aplicación de conversión de datos etcétera.

1.2. Modelo OSI y TCP/IP

En redes de datos existen modelos que determinan la manera en la cual es interpretada la información, como es el caso de los modelos OSI (Open System Interconnection –Sistema de interconexión abierta) y TCP/IP, el modelo OSI es la base de un conjunto de protocolos además de

[1] Programa de la academia Cisco Networking, material multimedia, 2006.

ser la plataforma de un programa internacional para el desarrollo de protocolos de red y otros estándares que faciliten la intercomunicación de los dispositivos ofrecidos por diferentes vendedores.

1.2.1 Modelo OSI

Durante las últimas décadas ha habido un enorme crecimiento en la cantidad y tamaño de las redes, muchas de ellas se desarrollaron utilizando implementaciones de hardware y software diferentes, como resultado, muchas de las redes eran incompatibles y se volvió muy difícil la comunicación entre ellas, debido a que utilizaban especificaciones distintas. Para solucionar este problema, la Organización Internacional para la Normalización (ISO) realizó varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) y por lo tanto, elaboraron el modelo de referencia OSI en 1984.

El modelo de referencia OSI es el modelo utilizado para las redes de datos. Sin embargo, no es el único modelo que existe, ya que existen otros modelos de referencia como lo es el modelo TCP/IP.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red.

1.2.1.1 Esquema del modelo OSI

En el modelo de referencia OSI, existen siete capas como se muestra en la figura 1.4.

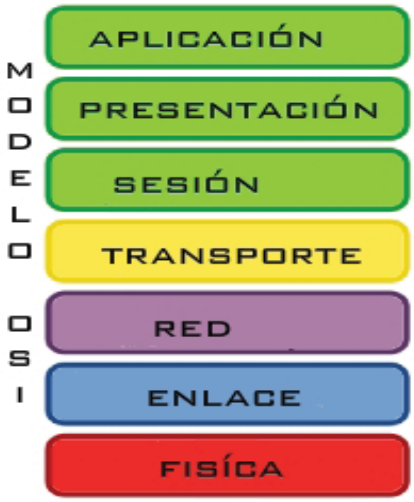

Figura 1. 4 Capas del modelo OSI.

El modelo de capas permite comprender de manera sencilla el proceso de comunicación entre equipos, además de que esto implica identificar y solucionar problemas de comunicación de manera más eficiente, permite la interoperabilidad de las tecnologías, estandariza las interfaces y permite un desarrollo mucho más rápido. Las capas que conforman al modelo OSI son:

1) Presentación.
2) Aplicación.
3) Sesión.
4) Transporte.
5) Red.
6) Datos.
7) Física.

a) Capa física

Enumerando el modelo OSI de forma ascendente, la capa física ocupa el lugar número uno, recordando que una computadora o cualquier dispositivo electrónico funciona a base de voltaje, por lo que en esta capa se consideran los dispositivos encargados de transportar la señal de un dispositivo a otro y que a su vez son convertidos en ceros y unos para que el dispositivito pueda interpretarlos.

La capa física es la capa que define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre los sistemas finales.

A lo largo de la historia de las redes se han utilizado distintos medios para interconectar los equipos que conforman la red, esto debido a que se encuentran mejoras en los medios de transmisión, lo cual permite tener un mejor desempeño, desde luego el medio no es el único factor que interviene en el tiempo de retardo para trasmitir datos ya que existen otros factores.

Dentro de los elementos que componen a la capa física se encuentran los distintos medios de transmisión como son fibra óptica, cable UTP (Unshielded Twisted Pair – Cable de par trenzado) en sus distintas categorías, atmósfera que es un medio para transmitir ondas de radio además del cable coaxial que prácticamente desaparece. También ha cambiado la topología, por lo que los medios de enlace físico han evolucionado, ofreciendo nuevas ventajas como mayor alcance, mayor velocidad de transmisión, fácil instalación, etcétera, incluyendo estándares que se han desarrollado en función del tipo de red.

Enseguida se enumeran los componentes pertenecientes a la capa física:

- Medios de transmisión (coaxial, UTP, fibra óptica, ondas magnéticas en general, DSL, ADSL, etcétera).
- Repetidores.
- Concentradores (router, switch, hub).
- Tarjeta de Red.

b) Capa de enlace

Los bits que son transportados independientemente del medio que se utilice, no serían de utilidad si no fuese posible identificar quién los genera y cuál es su destino, he aquí la importancia de la capa de enlace de datos.

La capa de enlace de datos se divide en dos partes:

- Estándar LLC (Logical Link Control- Control de enlace lógico), se define en la especificación IEEE 802.2. independiente de la tecnología.
- Las partes específicas, que dependen de la tecnología e incorporan la conectividad de la capa uno.

El *IEEE* divide la capa de enlace OSI en dos subcapas separadas, las subcapas IEEE reconocidas son:

- Control de acceso al medio (MAC) (realiza transiciones hacia los medios).
- Control de enlace lógico (LLC) (realiza transiciones hasta la capa de red).

Estas capas son de vital importancia ya que garantizan que las tecnologías sean compatibles y que las computadoras puedan establecer la comunicación.

En la tarjeta NIC se encuentra la dirección MAC o dirección física, aunque la tarjeta de red es un dispositivo de capa uno, este dispositivo funciona en las dos capas ya que se conecta directamente con el medio físico.

La capa de enlace lógico permite que la capa de enlace de datos funcione independientemente de las tecnologías existentes, por lo que esta capa proporciona versatilidad en los servicios de los protocolos de la capa de red que está sobre ella, mientras se comunica de forma efectiva con las diversas tecnologías que están por debajo. El LLC, como subcapa, participa en el proceso de encapsulamiento. La PDU (Protocol Data Unit- Unidad de datos de protocolo) del LLC a veces se denomina paquete LLC.

LLC define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.

El LLC transporta los datos del protocolo de la red, un paquete IP, y agrega más información de control para ayudar a entregar ese paquete IP en el destino. Agrega dos componentes de direccionamiento de la especificación IEEE 802.2: el punto de acceso al servicio destino (DSAP) y el punto de acceso al servicio fuente (SSAP). Luego este paquete IP re empaquetado viaja hacia la subcapa MAC para que la tecnología específica requerida le adicione datos y lo encapsule. Un ejemplo de esta tecnología específica puede ser una de las variedades de Ethernet, Token Ring o FDDI (Fibber Distributed Data Interface – Interfaz de Datos Distribuida por Fibra).

La subcapa LLC de la capa de enlace de datos administra la comunicación entre los dispositivos a través de un solo enlace a una red. LLC se define en la especificación IEEE 802.2 y soporta tanto servicios orientados a conexión como servicios no orientados a conexión, los cuales son utilizados por los protocolos superiores. IEEE 802.2 define una serie de campos en las tramas de la capa de enlace de datos que permiten que múltiples protocolos de las capas superiores compartan un solo enlace de datos físico.

De manera general la capa dos realiza las siguientes funciones:

- Suministra un tránsito confiable de datos a través de un enlace físico.
- Usa un sistema denominado Control de acceso al medio (MAC).
- Usa la dirección MAC, que es la dirección física que se ubica en una NIC.
- Usa el entramado para organizar o agrupar los bits.

c) Capa de red

La tercera capa del modelo OSI es la capa de red, ésta es la encargada de la navegación de los datos a través de la red, se encarga de encontrar la mejor ruta a través de la misma.

A medida que las redes crecen surge la necesidad de interconectarlas entre sí para formar nuevas redes creando el ya conocido Internet, para poder lograr esta comunicación entre las distintas redes, surge la necesidad de nuevos dispositivos encargados de realizar esta operación como los routers.

Los routers son dispositivos de interconexión que operan en la capa tres del modelo OSI. Estos dispositivos unen o interconectan segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de enlace.

Los routers cuentan con algoritmos capaces de tomar decisiones como calcular la mejor ruta de envío de datos, luego dirigen los paquetes hacia el segmento y el puerto de salida adecuados. Los routers toman paquetes de dispositivos LAN, basándose en información de la capa tres la información es enviada a través de la red, además de que estos dispositivos pueden calcular la menor ruta basándose en la densidad del tráfico y la velocidad del enlace.

Para que un router pueda encontrar la mejor ruta, lo puede realizar de dos maneras, empleando direccionamiento plano o direccionamiento jerárquico. Un esquema de direccionamiento plano asigna a un dispositivo la siguiente dirección disponible mientras que un direccionamiento jerárquico se asigna a través de la ubicación, el protocolo Internet (IP) es la implementación más popular de un esquema de direccionamiento de red jerárquico.

Los routers requieren direcciones de red para garantizar el envío correcto de los paquetes, por lo que la dirección IP contiene la información necesaria para enrutar un paquete a través de la red. Cada dirección origen y destino que contiene está compuesta por 32 bits.

d) Capa de transporte

Una vez que el router ha elegido la mejor ruta para el envío de datos a través de la red, pasan a la capa de transporte, la cual es la encargada de regular el flujo de información desde el origen hasta el destino de manera confiable y precisa, para llevar a cabo este proceso entran en juego dos protocolos TCP (Transmission Control Protocol – Protocolo de control de transmisión) y UDP (User Datagram Protocol – Protocolo de datagrama de usuario).

Una característica tajante que diferencia TCP de UDP es que el primero es un protocolo orientado a conexión.

a) Las características de TCP

- Orientado a conexión.
- Confiable.
- Divide los mensajes salientes en segmentos.
- Re ensambla los mensajes en la estación destino.
- Vuelve a enviar lo que no se ha recibido.
- Re ensambla los mensajes a partir de segmentos entrantes.
- Forma parte de la pila de protocolos TCP/IP.

b) Las características de UDP:

- No orientado a conexión.
- Poco confiable.
- Transmite mensajes (llamados datagramas del usuario).
- No utiliza acuses de recibo.

Tanto TCP como UDP utilizan diferentes puertos que les permiten dar seguimiento a la comunicación y pasar información a capas superiores.

e) Capa de sesión

La capa de sesión establece, administra y termina las sesiones entre las aplicaciones. Esto incluye el inicio, la terminación y la re sincronización de dos computadoras que están manteniendo una "sesión". La capa de sesión coordina las aplicaciones mientras interactúan en dos hosts que se comunican entre sí. Las comunicaciones de datos se transportan a través de redes conmutadas por paquetes, al contrario de lo que ocurre con las llamadas telefónicas que se transportan a través de redes conmutadas por circuitos. La comunicación entre dos equipos involucra una gran cantidad de pequeñas conversaciones, permitiendo de esta manera que las dos computadoras participen de forma efectiva. Un requisito de estas conversaciones es que cada host tenga que jugar un doble papel: el de solicitar el servicio, como si fuera un cliente y el de contestar como servicio, como lo hace un servidor. La determinación del papel que están desempeñando en un preciso momento se denomina *control de diálogo*.

Las peticiones y respuestas de los equipos que han establecido una sesión son coordinadas por protocolos implementados en la capa cinco.

f) Capa de presentación

Esta capa permite la comunicación entre aplicaciones en diversos sistemas informáticos, de tal forma que sean transparentes para las aplicaciones.

Se ocupa del formato y de la representación de datos, entre las principales funciones de esta capa se encuentran:

- Formateo de datos
- Compresión de datos
- Cifrado de datos

Después de recibir los datos de la capa de aplicación, la capa de presentación ejecuta algunas funciones, o todas ellas, con los datos antes de mandarlos a la capa de sesión.

Por otro lado, en la estación receptora, la capa de presentación toma los datos de la capa de sesión y ejecuta las funciones requeridas antes de pasarlos a la capa de aplicación.

La capa de presentación también se ocupa de la compresión de los archivos.

g) Capa de aplicación

La capa número siete del modelo OSI es llamada capa de aplicación, los usuarios finales interactúan directamente con esta capa, en ella se encuentran todos los programas con los que puede interactuar el usuario que hacen uso de la red.

Por lo que esta capa es la encargada de identificar la disponibilidad de los participantes de la comunicación, sincronizar aplicaciones y controlar la integridad de los datos. La capa de aplicación no brinda servicios a ninguna otra capa OSI. Sin embargo, brinda servicios a los procesos de aplicación que se encuentran fuera del alcance del modelo OSI.

1.2.2 Modelo TCP/IP

Todos quienes utilizan un equipo de cómputo e Internet, ingenieros, académicos, profesionistas, gente de negocios, estudiantes y muchos más, emplean de manera invisible el uso de los protocolos TCP/IP para realizar cualquiera de sus actividades que impliquen comunicación con otros equipos de cómputo.

El nombre de TCP/IP se refiere a una suite completa de protocolos de comunicación, esta suite obtiene su nombre de los protocolos que le pertenecen; el protocolo de control de transmisión (TCP) y el protocolo de Internet (IP), TCP/IP es el nombre tradicional para este conjunto de protocolos, éste en ocasiones es llamado Internet Protocol Suite (IPS), ambos nombres son aceptables aunque en este caso se hará referencia al protocolo como TCP/IP.

1.2.2.1 Introducción al modelo TCP/IP

El origen de los protocolos TCP/IP se remonta al año de 1969, por medio de un proyecto de desarrollo e investigación fundado en la Agencia de Proyectos de Investigación Avanzada (ARPA) por sus siglas en inglés, el proyecto consistía en crear un red de intercambio de paquetes la cual fue llama ARPANET, fue construida para estudiar técnicas para brindar comunicaciones de datos robusta, confiable e independientes de los vendedores.

Estas redes experimentales fueron tan exitosas que muchas de las organizaciones comenzaron a utilizarlas en sus comunicaciones de datos diariamente. En 1975 el ARPANET fue convertido de una red experimental a una red operacional y la responsabilidad para administrar esta red fue asignada a DCA (Defense Communications Agency-Agencia de defensa para las comunicaciones) ahora

conocida como DISA (Defense Information Systems Agency- Agencia para la defensa de sistemas de información), división que pertenece al Departamento de Defensa de los Estados Unidos.

Los protocolos TCP/IP fueron desarrollados después de que la red se volviera operacional, estos protocolos fueron adoptados como estándares militares en 1983 y todos los nodos conectados a la red se convirtieron al nuevo protocolo. Al mismo tiempo de que TCP/IP fue adoptado como un estándar, el término Internet comenzó a ser utilizado de manera común. En 1983 el viejo ARPANET fue dividido en MILNET, la parte no clasificada de la red de datos de defensa y en un nuevo y más pequeño ARPANET, Internet fue utilizado para referirse a la red entera, actualmente internet es el término genérico utilizado para referirse a toda la red.

La popularidad de TCP/IP creció rápidamente ya que este modelo fue la base para la conexión a Internet, además de ser un protocolo estándar abierto, ser independiente de la conexión física de red (Ethernet, DSL, dial-up, fibra óptica, inalámbrica y cualquier otro medio de transmisión), además de su compatibilidad con diferentes sistemas operativos y hardware, un esquema de direccionamiento común que permite a cualquier dispositivo una dirección única que cualquier otro dispositivo en la red entera, inclusive al ser empleado en redes que no tienen conexión a Internet y una estandarización en los protocolos de capa superior.

1.2.2.2 Arquitectura del protocolo TCP/IP

La arquitectura del protocolo TCP/IP está compuesta de menos capas que las siete utilizadas en el modelo OSI, las 4 capas del modelo TCP/IP se ilustran en la figura 1.5.

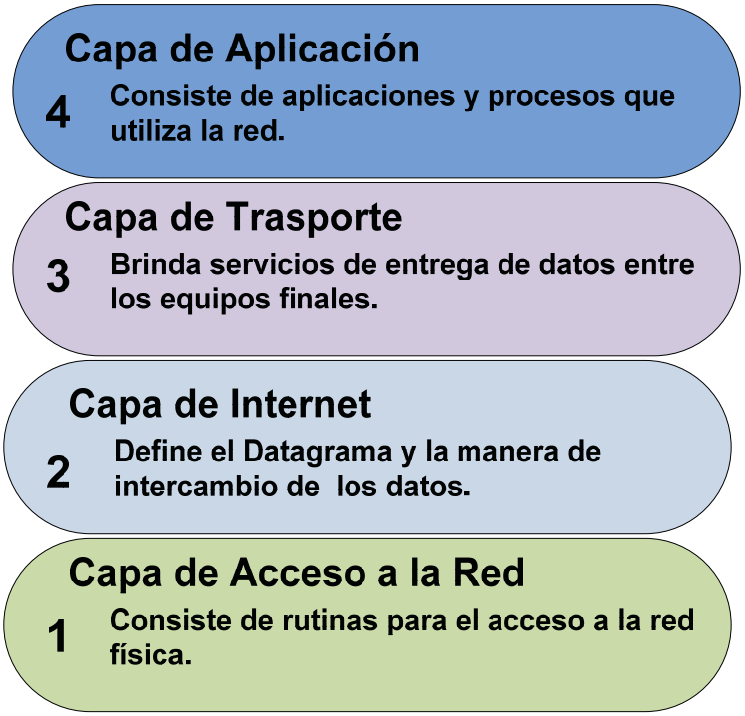

Figura 1. 5 Arquitectura TCP/IP.

Como en el modelo OSI, los datos pasan de la capa inferior hacia la superior, es decir, de la capa de *acceso a red* hasta llegar a la *capa de aplicación*, cada capa de la pila agrega controles a la información para garantizar la apropiada entrega, este control de información es llamado encabezado, porque éste es colocado frente a los datos que serán trasmitidos, cada capa trata toda la información que ésta recibe como datos y le agrega su propia cabecera al principio de la información, esto también es conocido como encapsulado, cuando los datos se reciben, cada capa quita su encabezado de los datos hasta llegar a la capa de aplicación, la cual interpreta los datos(figura 1.6).

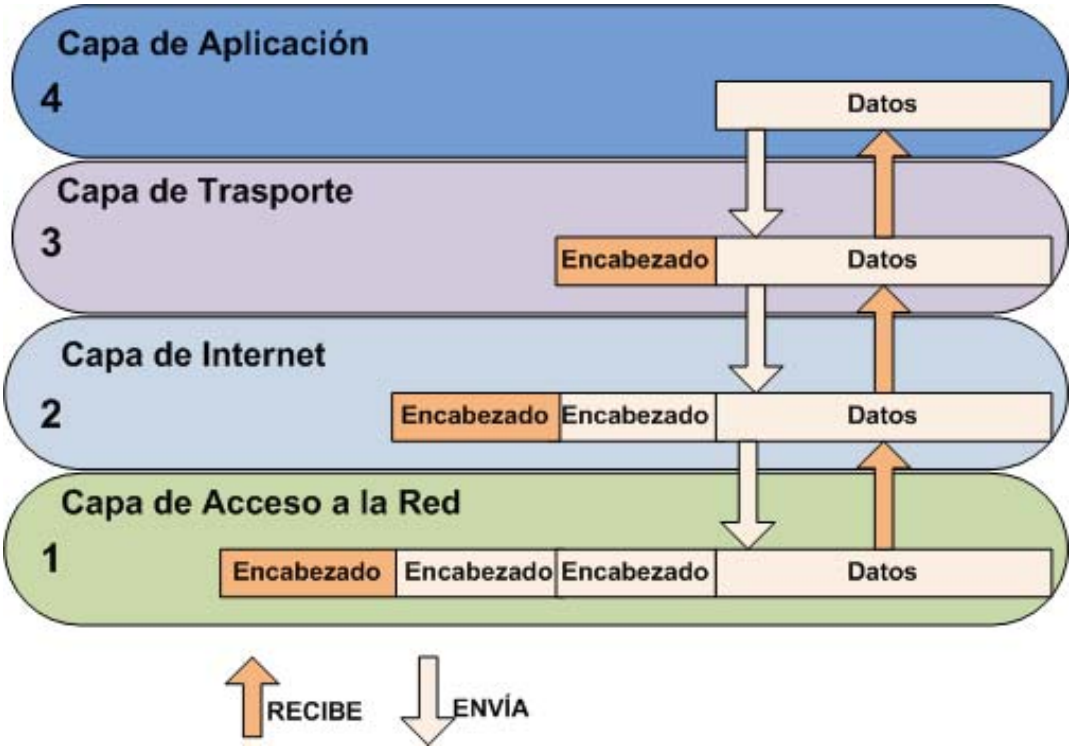

Figura 1. 6 Encapsulado de los datos.

Cada capa tiene su propia estructura de datos, la cual está diseñada para ser compatible con las capas que la rodean. Mostrando los términos utilizados por las diferentes capas para definir que los datos sean enviados, las aplicaciones utilizan TCP (Transmission Control Protocol – Protocolo de control de transmisión) para referirse a datos como un flujo (stream), mientras que las aplicaciones que utilizan UDP (User Datagram Protocol Protocolo de datagrama de usuario) llaman a estos datos paquete como mensaje (message), dentro de la capa de transporte para TCP la estructura se conoce como segmento (segment) y para UDP paquete (packet). En la capa de internet se conocen todos los bloques como datagrama tanto para TCP y UDP, y la capa de acceso a la red la estructura de datos se conoce como frame- marco (figura1.7).

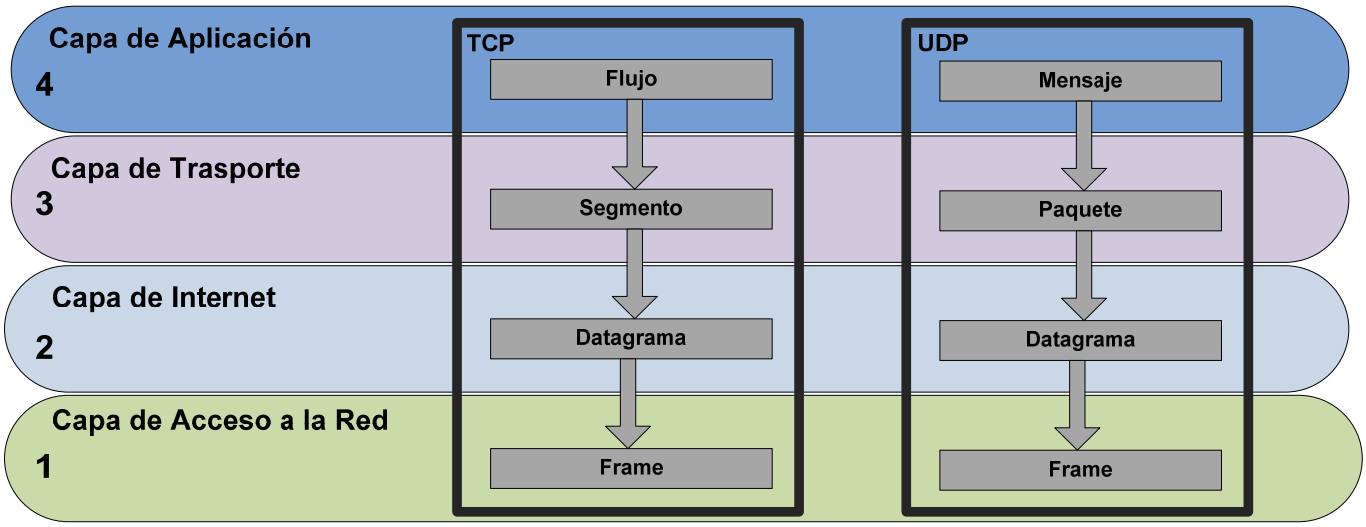

Figura 1. 7 Estructura de datos.

a) Capa de acceso a red

Es la capa más inferior del modelo TCP/IP, los protocolos en esta capa brindan el significado para que el sistema entregue datos a otros dispositivos, esta capa define cómo utilizar la red para trasmitir un datagrama IP, a diferencia de los protocolos de nivel superior, el protocolo de acceso a red deberá conocer los detalles de todo el paquete (estructura del paquete, dirección IP, MAC Address, etcétera) para que el dato pueda ser transmitido correctamente. Esta capa es equivalente a las 3 capas inferiores del modelo OSI (Red, Enlace de datos y Física) (figura 1.8).

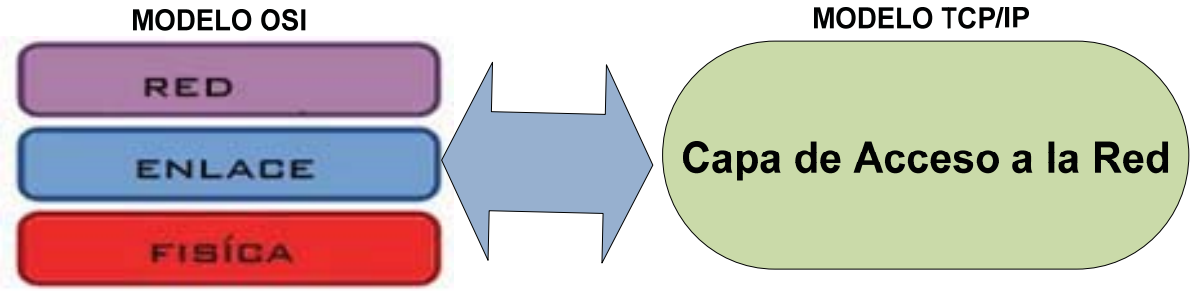

Figura 1. 8 Equivalencia de la capa de acceso a red del modelo TCP/IP con las tres primeras capas del modelo OSI.

Las funciones ejecutadas en este nivel incluyen encapsulamiento de datagramas IP dentro de los frames transmitidos, mapeo de direcciones IP a direcciones físicas *MAC Address*, dos RFC (Request For Comment – Petición de comentario) que definen protocolos en la capa de *acceso a la red* son:

- RFC 826, Address Resolution Protocol –Protocolo de resolución de direcciones (ARP).

- RFC 894, Un estándar para la transmisión de datagramas IP sobre redes Ethernet, que especifica cómo los datagramas IP son encapsulados para trasmitirse sobre redes Ethernet.

1. Protocolo ARP

Mientras TCP/IP encuentra otros equipos de cómputo en la red con base en la dirección IP única de cada equipo, la transmisión de datos tuvo que ocurrir sobre algún tipo de enlace de datos, el cual debe ser debidamente identificado y relacionado con la dirección IP, la identificación de este medio se realiza por medio del protocolo ARP definido en el RFC 826, comúnmente ubicado en la capa dos del modelo OSI o en la capa uno del modelo TCP/IP.

Las direcciones utilizadas por este protocolo se conocen como MAC Address (Media Access Control Address –Dirección de control de acceso al medio), todas las tarjetas de red para redes Ethernet tiene este identificador, constituido por 48 bits o seis números en formato hexadecimal, los primeros seis números se refieren al fabricante del dispositivo y los últimos seis representan al identificador del dispositivo, también son utilizadas por algunos routers, switches, firewalls, este número es único a nivel mundial para cada dispositivo.

Cuando una máquina envía un paquete, éste es encapsulado por el protocolo IP, el cual contiene la MAC Address de la máquina que se encuentra enviando, para obtener la MAC Address del destino del paquete, se envía un paquete ARP a todo el segmento de red preguntando por algún host con base en su dirección IP, una vez que el host destino es encontrado, éste contesta enviando la relación de su IP con la MAC Address(figura 1.9).

Source	Destination	Protocol	Info
AsustekC_3c:de:50	Broadcast	ARP	Who has 192.168.16.10? Tell 192.168.16.15
00:23:8b:19:f8:c8	AsustekC_3c:de:50	ARP	192.168.16.10 is at 00:23:8b:19:f8:c8

Figura 1. 9 Protocolo ARP.

Es importante mencionar que debido a la manera en la que trabaja el protocolo ARP, permite la ejecución de ataques de hombre en el medio, es permitido debido a la vulnerabilidad en el diseño del protocolo.

b) Capa de internet

La capa que sigue en jerarquía después del acceso a red es la capa de internet, en esta capa el protocolo IP (Internet Protocol) es el más importante, la versión de IP utilizada actualmente es la versión 4 (IPv4) definida en el RFC 791, actualmente se busca migrar IPv4 a una versión más reciente llamada IPv6 que se encuentra en crecimiento, ya que brinda mayores beneficios como lo es una gama más grande de direcciones, calidad en el servicio y seguridad desde el diseño, en este tema sólo se considera al protocolo IPv4 ya que es el estándar utilizado actualmente en la mayoría de las redes mundiales.

1. Protocolo IP

El protocolo IP (Internet Protocol – Protocolo de Internet), definido en el RFC 791 dentro de sus funciones incluye:

- Define el datagrama, que es la unidad básica de transmisión en Internet definida por el protocolo de internet (Internet Protocol).
- Define el esquema de direccionamiento de Internet.
- Mueve datos entre la capa de enlace a red (Network Access Layer) y la capa de transporte (Transport Layer).
- Determina la ruta a seguir para equipos en otro segmento.
- Ejecuta fragmentación de paquetes y re ensambla los mismos (cada tipo de red define su unidad de transmisión máxima).

Para realizar el intercambio de paquetes o datagramas, se hace uso de la dirección física (MAC Address) y la dirección IP determinada en esta capa, cada paquete viaja en la red independientemente de cualquier otro paquete. El datagrama es el paquete formado definido por el protocolo de internet el cual contiene una cabecera y los datos, esto implica que mensajes grandes como una enciclopedia sean fragmentados en mensajes más pequeños para su transporte, en la cabecera se tienen los datos necesarios para que el paquete pueda ser entregado, con base en la dirección IP destino, el datagrama está formado por 6 palabras de 32 bits cada una, como se muestra en la figura 1.10.

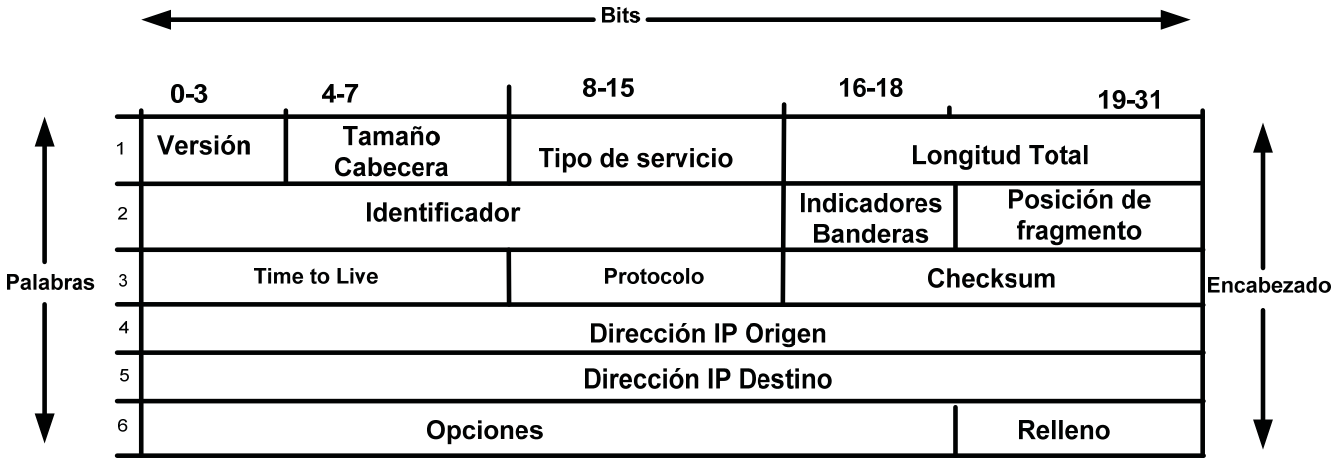

Figura 1. 10 Datagrama IP.

La cabecera IP está formada por los campos que se ilustran en la imagen anterior, cada uno tiene usos específicos que ayudan a encaminar la tarea del protocolo. En caso de que el paquete se envíe a un equipo del mismo segmento, el paquete es enviado directamente al host, si el paquete va dirigido a un equipo que no es de la red local, éste es enviado al gateway para que procese su entrega.

2. Protocolo ICMP

Una parte integral de la capa de Internet es el protocolo ICMP (Internet Control Message Protocol – Protocolo de mensaje de control de Internet) definido en el RFC 792, este tipo de protocolos realizan un seguimiento de control que determinan errores y funciones informativas de TCP/IP, además de ser un protocolo no orientado a conexión, es decir, no realiza un seguimiento de los paquetes que han sido enviados.

ICMP es un protocolo no orientado a conexión, una de sus utilidades primordiales es solucionar problemas en la red por medio de la aplicación ping, ping generalmente utiliza un paquete ICMP especial *petición – echo tipo (8)* (echo-request type (8)) en sus banderas, el cual pregunta si está activo el equipo, en caso de que el host solicitado esté disponible envía una *repetición – echo tipo (0)* (echo-replay type (0)) en sus banderas, el seguimiento de este tipo de prueba se observa en la figura 1.11.

Figura 1. 11 Protocolo ICMP.

Existen en total 11 tipos de mensajes ICMP, cada que hay comunicación en la capa de internet, los cuales tienen utilidades específicas, los usos principales que se le dan a este protocolo se muestran en la tabla 1.3.

Tabla 1. 3 Mensajes ICMP.

Nombre	Descripción
Flow Control (Control de flujo).	Cuando el datagrama llega demasiado rápido para ser procesado.
Detecting unreachable destinations, (Detectando destinos inalcanzables).	Cuando un destino no es encontrado.
Redireting routes (redireccionando rutas).	Es enviado para avisar a un host que utilice otro gateway, posiblemente por mejor elección.
Checking remote host (checando host remoto).	Para verificar si un host remoto se encuentra en operación.

c) Capa de transporte

Después de la capa de Internet, está definida la capa de transporte equipo a equipo - Host to Host Transport Layer, usualmente conocida como capa de transporte, los protocolos más importantes en esta capa son protocolo de control de transmisión *TCP* y protocolo de datagrama de usuario *UDP*. *TCP* brinda servicio de entrega de datos confiable en cada punto final con detección y corrección de errores, a diferencia de *UDP* que brinda un servicio de entrega de datos sin conexión, ambos protocolos entregan datos entre la capa de aplicación y la capa de Internet.

1. Protocolo TCP

El protocolo *TCP* es utilizado en aplicaciones que requieren la garantía de entrega en sus paquetes, verificando que los datos sean entregados, por lo tanto *TCP* es un protocolo orientado a conexión, la unidad de datos intercambiada entre cada módulo de datos *TCP* es llamada segmento, cada segmento contiene un *checksum* (suma de verificación) para verificar que los datos no tengan daño, si el segmento enviado contiene daños, éste es rechazado hasta recibir un segmento en buen estado, el encabezado de este protocolo es de 32 bits formado por 6 palabras (figura 1.12).

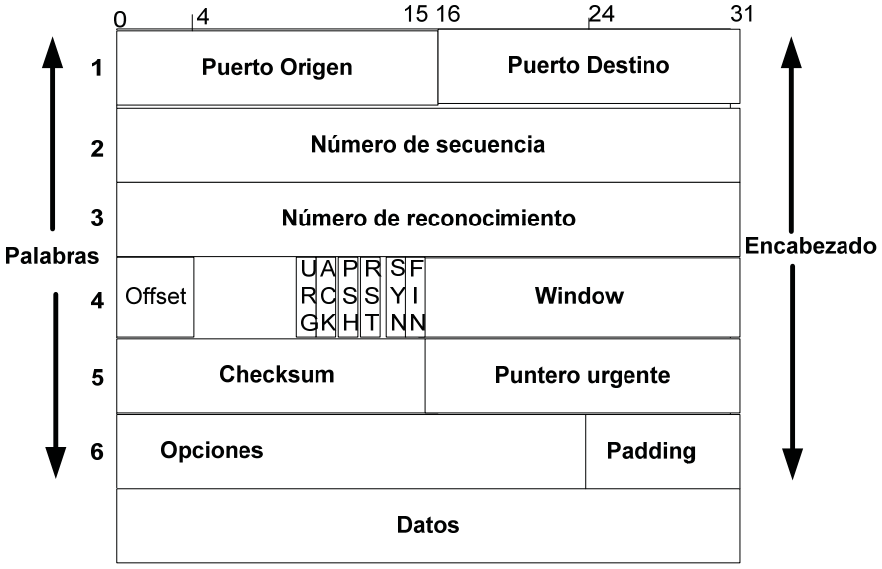

Figura 1. 12 Cabecera TCP.

El protocolo TCP establece una conexión punto final a punto final, entre dos equipos, la información de control de esta conexión recibe el nombre de handshake (saludo de mano) es un intercambio entre los 2 puntos finales para establecer un diálogo. El tipo de handshake utilizado por *TCP* recibe el nombre de Three-way handshake o (Saludo de *3* vías), porque tres segmentos son intercambiados.

TCP ve los datos que envía como un flujo continuo de bytes, no como paquetes independientes, por lo tanto *TCP* tiene cuidado en mantener la secuencia en que los datos son enviados y recibidos. El estándar *TCP* no requiere que cada sistema comience numerando los bytes con un número específico, cada sistema elige el número que éste utilizará como punto de comienzo, para mantener el flujo de datos correctamente, cada punto final debe conocer el *ISN* (Initial Sequence Number - número inicial de secuencia) del otro punto final, por razones de seguridad este número es elegido aleatoriamente.

2. Protocolo UDP

El protocolo *UDP* definido en el *RFC 768*, permite la entrega de datagramas con un mínimo de carga, es un protocolo sin garantía de entrega y no orientado a conexión, es decir, no tiene mecanismos para verificar que la información ha sido entregada al punto final, utiliza un encabezado de 32 bits donde define el puerto origen y destino en una palabra, cada uno utilizando 16 bits, el formato de mensajes *UDP* es el siguiente (figura 1.13).

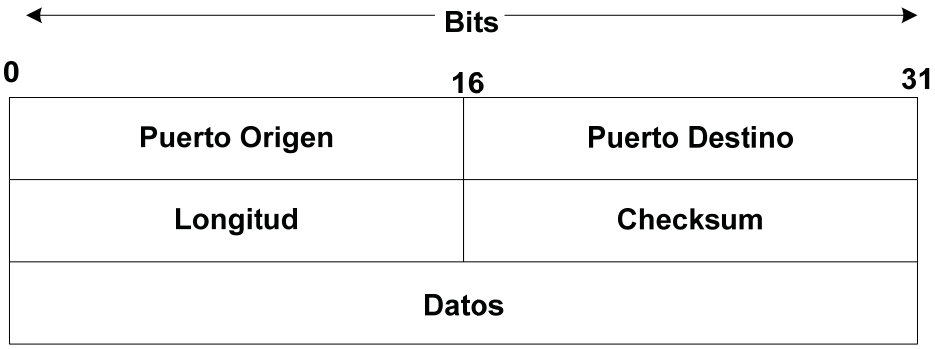

Figura 1. 13 Cabecera UDP.

Uno de los protocolos más conocidos el cual emplea como transporte *UDP* es el protocolo *DNS*, debido a las ventajas de transporte que éste brinda para su finalidad.

3. Three-Way Handshake

El Three-way handshake – saludo de tres vías, es el proceso mediante el cual el protocolo *TCP* inicializa una conexión, el *host A* comienza la conexión al enviar un segmento al *host B* con el bit *SYN* (Sychronize sequence number – Número de secuencia de sincronización) activado, este bit indica a *B* que *A* desea comenzar una comunicación con él, enviándole un número de secuencia el cual indica a *B* el número de secuencia utilizado para mantener los datos en orden apropiado. El host *B* responde al host *A* con un segmento que tiene el bit *ACK* (Acknowledgment -Reconocimiento) y *SYN* (Sychronize sequence number – Número de secuencia de sincronización) activado, el segmento *B* reconoce la recepción del segmento *A* e informa a *A* qué número de secuencia comenzará con *B*, finalmente el *host A* envía al *host B* un segmento que reconoce la recepción del segmento *B*, al término de estos tres envíos se concreta el inicio de la comunicación (figura 1.14).

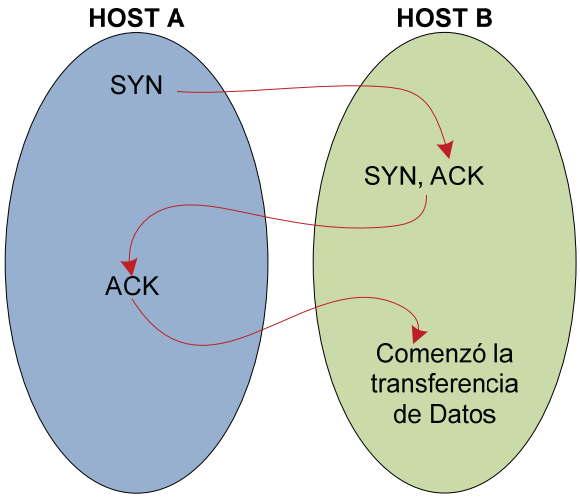

Figura 1. 14 Three-way handshake.

Después de este intercambio el *host A* tiene evidencia suficiente de que el *host B* está listo para recibir datos, tan pronto como la conexión es establecida, esta conexión se mantendrá hasta que alguno de los dos hosts envíe un segmento con la bandera de FIN (Finalize – finalizar, bandera para dar por terminada una conexión) activada, esto es el final del intercambio que brinda la conexión

lógica entre los 2 sistemas de una manera formal, aunque existe la posibilidad de concluir la comunicación con la bandera de reset.

d) Capa de aplicación

En la parte superior de la arquitectura *TCP/IP* se encuentra la capa de aplicación, esta capa incluye todos los procesos que utilizan los protocolos de la capa de transporte para la entrega de datos, aquí existen muchos protocolos de aplicación, muchos de éstos brindan servicios a los usuarios, suelen generarse nuevos servicios que se agregan continuamente a esta capa.

Los protocolos más conocidos e implementados son TELNET*, FTP, HTTP, SMTP, SMTP, POP3, DNS, SSH DHCP, NFS*, entre muchos otros que se generan con el paso del tiempo y las necesidades que surgen en el mismo.

1. Protocolo TELNET

Este protocolo está definido en el RFC 854 desde el año de 1983, conocido como *The Network Terminal Protocol – Protocolo de terminal para la red,* protocolo orientado a conexión utilizando por lo tanto transporte TCP, brinda autenticación remota sobre la red, es un protocolo inseguro ya que toda la información que viaja por este protocolo está en claro, es decir se puede interpretar todos los datos que fluyen, por lo tanto es punto fácil de ataque, actualmente ya es un protocolo muy poco utilizado pero algunos dispositivos y sistemas lo siguen utilizando como mecanismo de acceso remoto.

El protocolo TELNET le asigna al servidor el puerto 23 *TCP*, el cliente puede elegir el que desee, mayor a 1024, es muy útil cuando se desea ver alguna información que brinda un servicio por algún otro puerto conocido.

2. Protocolo FTP

Conocido como File Transport Protocol -Protocolo de transferencia de archivos, definido en el RFC 959 la primera propuesta de este protocolo data de 1971, es un protocolo simple cliente / servidor, que permite al servidor publicar un directorio para compartir sus archivos utilizado para realizar transferencia de archivos de manera interactiva, entre sus objetivos principales esta el permitir compartir archivos o datos, transferir datos confiable y eficazmente además de brindar autenticación.

El proceso de conexión es mediante el protocolo *TCP*, el servidor utiliza el puerto 21 TCP para la autenticación y la ejecución de comandos especificados en el protocolo, conocido como *control port*- puerto de control, además emplea el puerto 20 TCP para la transferencia de datos conocido como data port- puerto de datos.

El protocolo FTP tiene 3 principales debilidades, la comunicación viaja en claro, es decir, se puede interpretar a su paso por la red la información transmitida, los servidores FTP permiten conexiones anónimas en ocasiones, dicho con otras palabras, cualquier persona u equipo puede acceder a los

recursos si se tiene dicha configuración habilitada, y las vulnerabilidades propias ya conocidas de las versiones de servidores FTP que tienen que ver con errores en su programación.
Existe una versión similar conocida como *TFTP*, definida en el RFC 1350, The *TFTP* Protocol – Protocolo de transporte de archivo trivial, el cual no brinda autenticación y acceso al listado de directorios, además de emplear UDP en el puerto 69 para su transporte.

3. Protocolo HTTP

Hypertext Transfer Protocol – Protocolo de transferencia de hipertexto, definido en el RFC 2616, este protocolo es el encargado de traducir el código de los documentos *HTML* en páginas web, fue utilizado por World Wide Web – Red global mundial, desde 1990, especificado como *HTTP* /1.1, está diseñado para el acceso público, considera que la seguridad no es importante (figura 1.15).

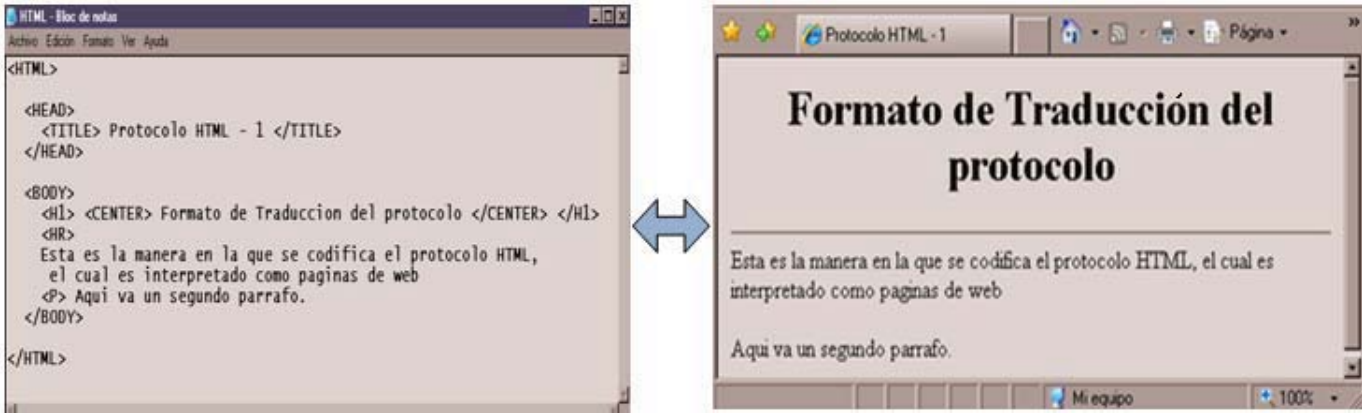

Figura 1. 15 Protocolo HTTP.

Es un protocolo orientado a conexión, utiliza el protocolo *TCP* y su servicio se brinda en el puerto 80, actualmente este protocolo combina el protocolo *HTML* con otros lenguajes de programación como aspx, php, jsp, entre otros, razón por la cual, el protocolo se vuelve más vulnerable al añadirle las vulnerabilidades propias de cada uno de los lenguajes de programación.

4. Protocolo SMTP

El protocolo Simple Message Transport Protocol – Protocolo de transporte de mensajes simple, es uno de los protocolos más utilizados ya que es el encargado del envío y recepción de correos electrónicos, actividad primordial hoy en día, está definido en el RFC 821, es utilizado para intercambiar mensajes entre servidores, su uso data de 1982, es una conexión TCP que emplea el puerto 25 para el servidor.
Además de *SMTP* existen otros protocolos de correo electrónico, como es el caso de POP (Post Office Protocol) utilizando el puerto 110 en el servidor, *IMAP* (Internet Message Access Protocol – Protocolo de acceso a mensajes de internet) utilizando el puerto 143, los tres tienen debilidades en común ya que todos envían sus mensajes y datos en claro, es decir se puede obtener fácilmente contraseñas y el contenido de los mensajes.
A la fecha muchos proveedores brindan el servicio a través de webmail, empleado los puertos 80 y 443 TCP.

5. Protocolo DNS

Todas las máquinas que trabaja sobre *TCP/IP* deben tener una dirección *IP* única para comunicarse con los otros hosts, las computadoras operan fácilmente con direcciones *IP,* a diferencia de las personas que les es más sencillo aprender un nombre, por esta razón los usuarios deberán identificar las direcciones *IP* por un nombre. En los inicios cercanos a *ARPANET* y comienzo de internet, el número de nombres de equipos conectados a la red fue pequeño, por lo tanto la traducción de nombres se realizaba por medio de un archivo llamado *HOST.TXT* que contenía el nombre y direcciones de cada host, este archivo fue alojado en un servidor a cargo de The Network Information Center –Centro de información sobre la red (*NIC*) del Instituto de Investigaciones de Stanford, como la red *ARPANET* siguió creciendo, se creó la necesidad de generar el concepto de servicio de distribución de nombres y dio origen al protocolo *DNS* (Domain Name Server –Servidor de nombres de dominio), el cual fue una manera más eficiente de distribuir los nombres de dominio, esta arquitectura fue liberada en el RFC 882 y 883. (figuras 1.16 y 1.17).

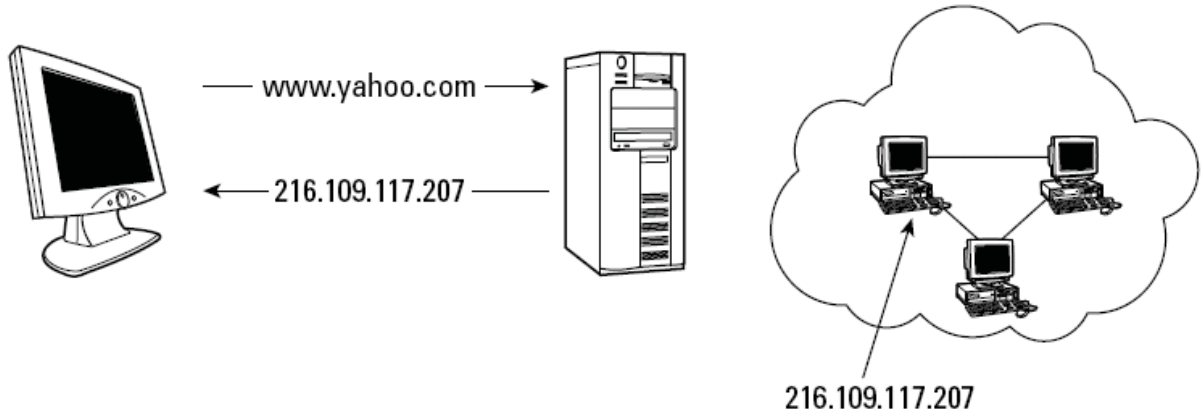

Figura 1. 16 Traducción DNS.

Este protocolo es un protocolo de traducción de nombres de dominio a direcciones *IP* y viceversa, aplicado a todos los servicios que hagan uso de los nombres de dominio como es *FTP*, *HTTP*, *SMTP*, *NetBIOS* y muchos más, está definido en los *RFC's* 1034 y 1035 actualmente, es un protocolo no orientado a conexión UDP el cual utiliza el puerto 53 del lado del servidor para atender las consultas, hoy en día a nivel mundial se cuenta con 13 servidores *DNS* raíz registrados en http://www.root-servers.org/.

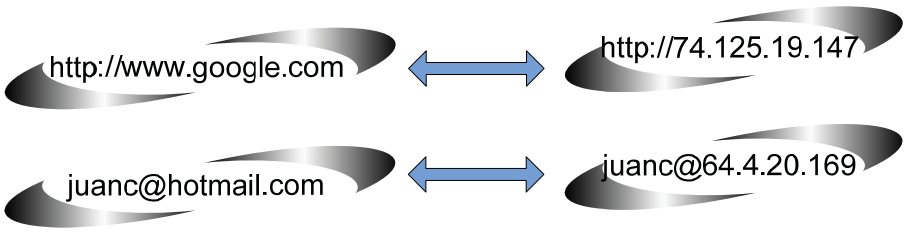

Figura 1. 17 DNS.

Dentro de los ataques a este protocolo se tiene la modificación de la base de datos del servidor, suplantación y denegación de servicio principalmente, ataques que se explicarán en capítulos posteriores.

6. Protocolo DHCP

El protocolo *DHCP* (Dynamic Host Configuration Protocol –Protocolo de configuración dinámica de host) es utilizado para asignar un conjunto de configuraciones de red, de manera centralizada y dinámica, evitando al usuario o administrador configurar los datos de cada equipo de manera manual, es un protocolo definido en el RFC 2131, no orientado a conexión UDP hace uso del protocolo *BOOTP* (Bootstrap Protocol – Protocolo Bootstrap) que es un protocolo de configuración de host anterior a *DHCP* resolviendo las limitaciones propias de *BOOTP*, ambos protocolos utilizan el puerto 67 para atender peticiones, los clientes normalmente reservan el puerto 68 dentro de los parámetros que determina este protocolo se encuentran dirección *IP*, servidor *DNS*, gateway, máscara de red.

Este protocolo fue pensado para equipos de red que cambian continuamente de ubicación, dentro de sus vulnerabilidades se tiene el seguimiento de actividades por parte de un cliente, denegación de servicio así como la posible suplantación de un servidor *DHCP* para varios propósitos (figura 1.18).

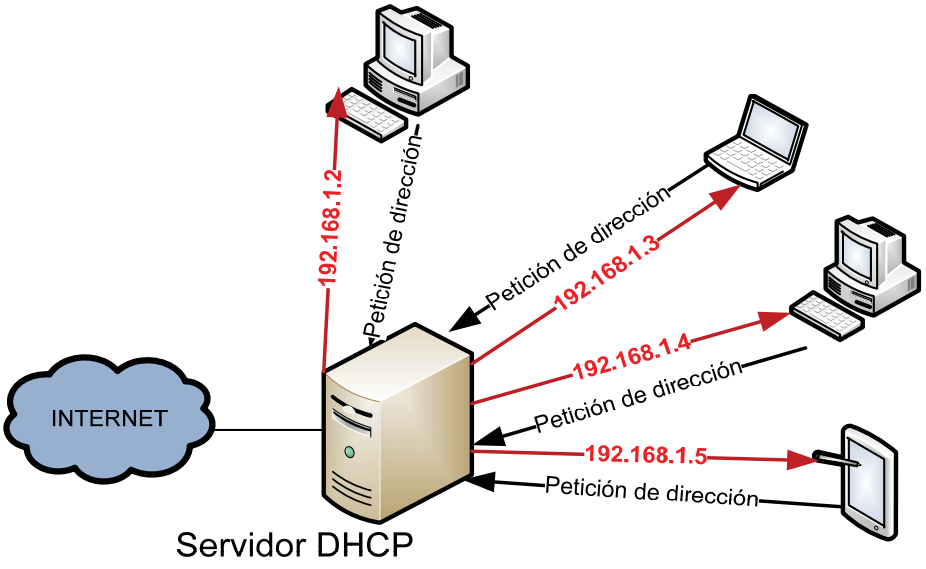

Figura 1. 18 DHCP.

1.3 Protocolo de administración SNMP

Un punto importante que debe ser considerado dentro de los protocolos tiene que ver con aquellos que pueden simplificar la administración de la red, como es el caso de los protocolos SNMP y RMON protocolos empleados para tratar de tener una mejor control.

El protocolo SNMP (Simple Network Management Protocol- Protocolo simple de administración de red) es un estándar de administración de redes ampliamente utilizado, brinda de manera centralizada la administración de hosts, servidores, switches, router, sistemas de respaldo de energía, además de sistemas operativos que tengan instalado el protocolo de administración como

es el caso de los sistemas operativos de Windows y Unix desde un equipo que tenga el software para la administración del protocolo (figura 1.19).

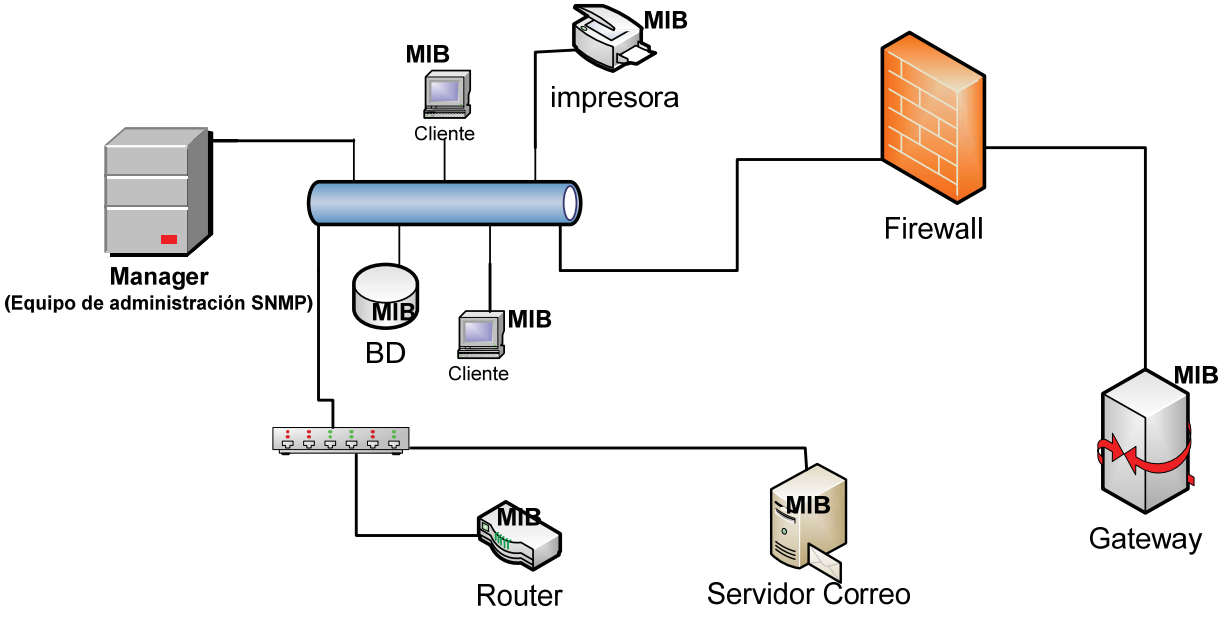

Figura 1. 19 Protocolo SNMP.

SNMP puede ser utilizado para configuración remota de dispositivos, rendimiento de la red, detectar fallas en la red o acceso inapropiado, auditoría de la red, pero una de las más importantes es el monitoreo de la red. Este protocolo consta de tres versiones hasta la fecha, la primera versión de este protocolo definida en el RFC 1157, sólo se definían comunidades, las cuales son el nombre con el cual se establece el intercambio de información entre los *agentes* que son los equipos que envían información relevante de su estado y los *managers*, equipos que se encuentran ejecutando alguna aplicación para interpretar la información enviada por los clientes y administrar la misma.

A partir de la versión uno de SNMP se determinaban tres tipos de acceso, escritura, lectura y trap *(alertas que informan algún cambio en el sistema)*, éstos dependen de la comunidad a la que se pertenezca, la mayoría de los fabricantes que brindan este servicio tienen configurado por defecto la comunidad *public* para sólo lectura y *private* para lectura y escritura, en el caso de los *traps* son alertas que emiten los equipos de comunicación para informar entre algunas cosas lo siguiente:

- Deja de funcionar una interfaz.
- Se estropea el ventilador de un router.
- Inventario y estado actual de los nodos en el segmento.
- El ancho de banda consumido en cierto intervalo de tiempo.
- La carga de procesos excede un límite.
- Se llena una partición de disco.
- Un UPS (Uninterrumtible Power Supply–Entrega de alimentación ininterrumpida) cambia de estado.

Existe más información que es entregada, pero es importante contar con un mecanismo que sólo entregue la información indispensable.

La versión 2 de este protocolo le agregó seguridad, es definida en el RFC 1905, 1906, 1907 y la versión 3, brinda las mayores opciones de seguridad que incluyen cifrado en la comunicación y autenticación segura, se recomienda la utilización de SNMP versión 3 por las opciones de seguridad que ofrece.

Este protocolo consta de tres componentes básicos llamados *manager* y *agente*, además de una base de información MIB (Management Information Base – Base Información gestionada) utiliza los puertos UDP 162 para el envío de alertas o eventos denominadas *trap* y 161 para enviar y recibir peticiones, conocidas como *query*. La MIB está definida en el RFC 1156, la cual fue actualizada en el RFC 1213, ésta contiene la estructura de la información que entrega el protocolo.

Algunas aplicaciones que son utilizadas como administradores o *managers* para el protocolo son los siguientes:

- Nagios (UNIX).
- PRTG (Windows).
- Cacti (UNIX).
- MIB Browser SolarWinds (Windows).
- Net-SNMP (UNIX).
- Netscan Tools (Windows).
- AdRem SNMP Manager (UNIX).

1.4 Protocolo de administración RMON

Entre los protocolos de administración de red además de SNMP existe el protocolo RMON (Remote Monitoring – Monitoreo remoto), la especificación de este protocolo se encuentra en el RFC 2819, sin embargo, existe una versión mejorada de dicho protocolo llamado RMON2 y sus especificaciones se localizan en el RFC 2021.

El protocolo RMON se convirtió en un estándar en 1992 y cinco años más tarde se terminó la versión RMON2, el protocolo RMON1 o simplemente RMON trabaja en la capa de enlace de acuerdo con el modelo OSI, sin embargo, RMON2 agrega nuevas capacidades ya que opera a nivel de aplicación proporcionando mayores ventajas para la administración de la red, permitiendo con ello resolver problemas de red de manera más eficiente.

Este protocolo también es capaz de recolectar datos con mayor detalle, puede ser configurado para que éste proporcione información, como utilización de la red, obtener información de los datos intercambiados entre dos equipos etcétera.

Las diferencias entre RMON y SNMP son:

- RMON es utilizado para operar en hardware.
- RMON es un protocolo proactivo capaz de enviar datos en lugar de esperar a ser analizados, permitiendo que el ancho de banda sea más eficiente.

- Es capaz de recolectar datos con mayor detalle.
- RMON puede ser implementado de distintas maneras y esto depende del tamaño o tipo de dispositivo a ser monitoreado, además de que éste reemplaza las costosas unidades analizadoras de red.

Las formas en las que puede ser implementado son:

- RMON MIB utilizada para monitorear dispositivos de hardware llamados también agentes embebidos.
- Como un módulo adicional de un dispositivo de monitoreo.

Es importante mencionar que existen otros protocolos de administración de redes adicionales a NMTP y RMON, como es el caso de Netflow (Cisco) y sflow (RFC 3176).

1.5 Protocolos utilizados en menor volumen

Existe una infinidad de protocolos y servicios que se utilizan y que se siguen utilizando, generados con base en las necesidades que van surgiendo, como todos los protocolos anteriores que tienen una finalidad específica estos también son protocolos comúnmente utilizados en un volumen menor, los cuales dependen en esencia de las actividades propias de cada institución. algunos servicios utilizados en menor volumen son escritorio remoto que utiliza el puerto 3389 TCP, secure shell utilizando el puerto 22 TCP, HTTPS utilizando el puerto 443 TCP, NetBIOS para los sistemas operativos de Microsoft utilizando los puertos TCP/135, TCP/139, TCP/445, TCP/1025-1030, UDP/137,UDP/138, UDP/445 y UDP/1025-1030, en el caso de los sistemas operativos Unix se tienen TCP/21,TCP/22, TCP/23, TCP/25, TCP/80, TCP/111, UDP/53, UDP/67-69, UDP/111, en el caso de impresoras de red 515 TCP/UDP, BD ms-SQL 1433 TCP, citrix 1494 TCP, tinbuktu 407 TCP, MySQL 3306 TCP, NTP puerto 123 UDP, IRC puerto 6667 TCP, LDAP puerto 389 TCP, RTSP entre muchos otros.

Sería una tarea muy complicada conocer todos los protocolos de comunicación que existen, pero es muy importante por lo menos saber los protocolos que comúnmente se utilizan en el segmento de red que se administra, esto con la finalidad de tener más control sobre el tráfico que se genera en el segmento de red.