Capítulo 2.
Conceptos básicos

2.1 INTRODUCCIÓN

En el presente capítulo se plantean una serie de conceptos básicos que serán de importancia crucial para llevar a cabo el estudio de la eficiencia volumétrica. La definición de los modelos de referencia OSI (*Open System Interconection*) y TCP/IP (*Transport Control Protocol/Internet Protocol)* mismos que plantean una descripción simplificada de redes al dividirlas en capas con funciones especificas permitirá entender la descripción que plantean los estándares de redes inalámbricas [1] y [2].

En base a estos modelos se define una arquitectura de protocolos que serán los que se tomen en cuenta para el estudio de la eficiencia volumétrica. Así mismo se describe de forma detallada la relación entre protocolos y servicios de tal forma que se comprenda el concepto de encapsulamiento de datos en PDU's (*Packet data Units*), las cuales actúan como bloques de información transparente para las capas adyacentes.

El encapsulamiento de datos es fundamental para entender el estudio de la eficiencia volumétrica, pues es mediante este proceso por el cual se agrega información de control en cada capa de acuerdo con el protocolo usado, lo cual da la pauta para el cálculo del rendimiento de la red.

Por último, se describen de forma simplificada las redes WLAN (*Wireless Area Network*) y las WMAN (*Metropolitan Area Networks*) y de la mano de éstas últimas se plantean de forma breve las redes BWA (*Broadband Wireless Access*); sus semejanzas y diferencias así como la arquitectura de cada una de ellas. La razón por la que es necesario presentar ésta clasificación reside en el hecho de que las redes WiFi son el término comercial para las WLAN, y WiMAX lo es para las redes BWA con extensión a redes WMAN.

2.2 DISEÑO DE REDES

Al implementar una red, es necesario definir además de las características técnicas que esta tendrá, su arquitectura lógica, es decir, los modelos en los que se basará su diseño y los protocolos de comunicación que se usarán para implementarla.

Se presentan de forma general una descripción de dos modelos muy usados en la actualidad para conceptualizar y diseñar redes, así como el proceso por el cual la información del usuario se traslada a través de la red.

2.2.1 Jerarquía de protocolos

Una forma de simplificar el diseño de redes complejas es organizarlas como una serie de **capas o niveles,** cada uno de los cuales se apoya en el nivel inmediato inferior a él.

Cada sistema está organizado de forma particular y muchos de los existentes no tienen delimitadas de forma precisa las funciones que ejecutan en cada capa, o bien difieren en el número que de ellas definen. De forma general se puede decir que el propósito de cada capa es ofrecer una serie de servicios a las capas superiores de forma simplificada, es decir, sin mostrar los detalles de la forma en la que se llevan a cabo dichas acciones (por ejemplo detalles del estado interno o algoritmos). El proceso anterior se conoce como encapsulamiento de datos.

En la Figura 2.1 [5] se observa un ejemplo de red de cinco capas; en ella se puede ver que las capas se interconectan entre si las superiores con las inferiores y los hosts convergen de forma común en el medio físico por medio del que se envía la información. La forma en la que se comunican las capas del mismo nivel o *peers* se denomina ***protocolo,*** lo cual es una serie de convenciones establecidas para que la capa n se comunique con la capa n de otro host.

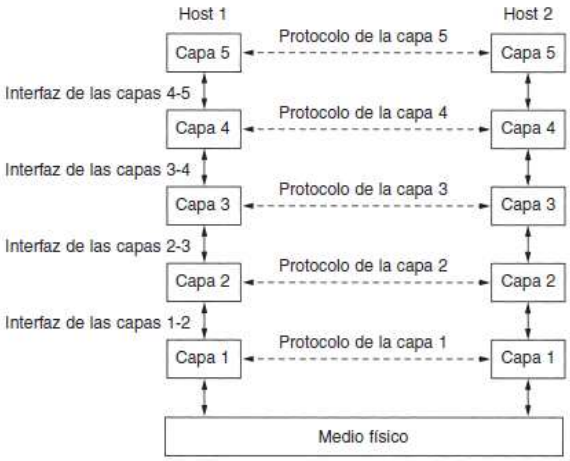

Figura 2.1. Ejemplo de red de cinco capas

La combinación de capas en las que se definirá una red y sus protocolos de comunicación asociados se conoce como ***arquitectura de red,*** la lista de protocolos se conoce como ***pila de protocolos.***

Para que las *capas n* de ambos hosts se logren comunicar, la información debe pasar en el Host 1 a las capas inferiores, atravesar el medio físico que es el medio por el cual se efectúa la comunicación de forma real; y pasar de nuevo por las capas inferiores en el Host 2 hasta llegar a la capa n. El procedimiento se describirá de forma breve en las siguientes secciones.

2.2.2 Protocolos y servicios

Un servicio es un conjunto de operaciones que una capa proporciona a la capa que esta sobre ella, éste define qué operaciones pueden llevarse a cabo pero no cómo se implementan. Se dice que la capa inferior implementa el servicio y la superior lo recibe.

Dado que un ***protocolo*** es un conjunto de reglas las cuales definen el formato de los mensajes que se intercambiarán las entidades iguales en una capa, son estas entidades quienes determinan como se llevaran a cabo los servicios; los protocolos pueden cambiar siempre que los cambios sean transparentes a los usuarios, por tanto no son dependientes uno de otro. La Figura 2.2 [5] muestra de forma gráfica dicha relación.

Figura 2.2. Relación protocolo y servicio

2.3 MODELO DE REFERENCIA OSI

2.3.1 Definición

El modelo de Interconexión de sistemas abiertos (*OSI Open System Interconnection)* es un modelo creado en 1984 por la ISO (*International Standard Organization*) cuyo propósito es establecer un marco de referencia descriptivo/teórico que definiera la arquitectura básica en la que debe estar basado un sistema de comunicaciones, de tal forma que le sea posible interactuar los demás sistemas existentes. Lo anterior quiere decir que busca que los sistemas sean compatibles usando un conjunto de reglas aplicables a ellos y basados en una serie de protocolos.

Se integra por una serie de 7 capas, cada una de las cuales describe una serie de funciones que permitirá una interacción con las capas adyacentes y que permite simplificar y clasificar las funciones en particular que ejecutaran los dispositivos.

La Figura 2.3 ilustra de forma simple el modelo OSI y las relaciones de protocolos y servicios definidos. Se puede ver en medio de ambos Hosts un dispositivo de red de capa 3 como un ruteados que permite la interconexión de ambos.

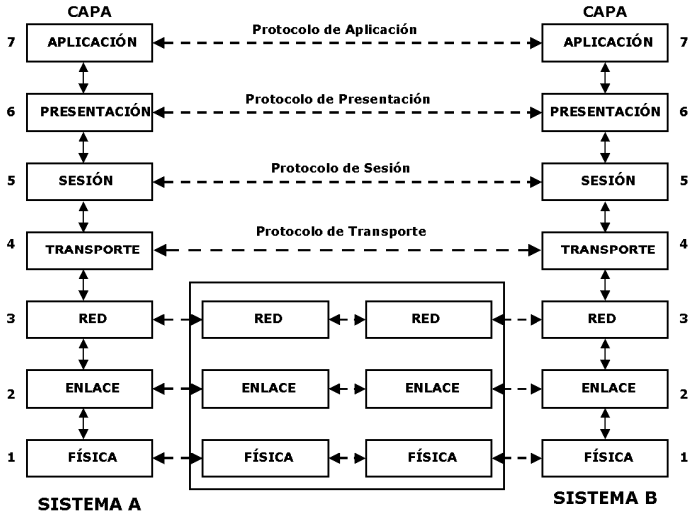

Figura. 2.3 Modelo OSI

2.3.2 Capas del modelo OSI

La Tabla 1 resume de forma breve las funciones de cada una de las capas presentes en el modelo OSI:

Tabla 1. Funciones de la capa del modelo OSI [5] pp. 20

Capa	Descripción	Funciones
1. Física	Es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico como a la forma en la que se transmite la información.	▪ Definir el medio o medios físicos por los que va a viajar la comunicación. ▪ Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de voltaje) a utilizar. ▪ Transmitir el **flujo de bits** a través del medio. ▪ Definir la forma en la que se inicia o termina la conexión.
2. Enlace de datos	Esta capa se ocupa del direccionamiento físico[2], del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo	▪ Transforma una transmisión de datos binarios en una secuencia libre de errores. ▪ Divide los datos de entrada en **tramas** y los transmite en forma secuencial. ▪ Procesa las tramas de estado (confirmación) que envía el nodo destino.

[2] Se refiere al direccionamiento único en relación con el hardware de red y el fabricante, no cambia (dirección MAC) que es un identificador de 48 bits.

3. Red	En este nivel se realiza el direccionamiento lógico[3] y la determinación de la ruta de los datos hasta su receptor final.	▪ Determinar la forma en la que los **paquetes** se enrutarán a su destino mediante tablas estáticas o dinámicas. ▪ Llevar a cabo el control de congestión. ▪ Determinar la calidad de servicio QoS.
4. Transporte	Efectúa el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino; independiente al tipo de red física que se esté utilizando.	• Lleva a cabo fragmentación de los datos recibidos si es necesario y los encapsula en **segmentos.** ▪ Proporciona seguridad a la información. ▪ Efectúa el control de flujo e los datos y de recuperación de errores.
5. Sesión	Se encarga de establecer una sesión entre los usuarios de dos hosts distintos.	▪ Controla la comunicación entre las aplicaciones de los usuarios finales. ▪ Establece, gestiona y cierra las conexiones o sesiones entre las aplicaciones involucradas.
6. Presentación	Proporciona a las aplicaciones independencia en la representación de datos (en caso de existir) de *hosts* distintos.	▪ Se encarga de la sintaxis y semántica de la información transmitida[4]. ▪ Maneja las representaciones abstractas de datos (que se aplicaron para el transporte de información a nivel de bits) para su intercambio a un nivel más alto.
7. Aplicación	Se compone de los protocolos que permiten a los hosts comunicarse con el usuario, es decir, las aplicaciones de interfaz humana.	▪ Proporciona a los usuarios el acceso al entorno de modelos de referencia de forma tranparente.

2.3.3 Encapsulamiento de datos

Para que los datos de capas iguales (capas n) en el transmisor y receptor de la información puedan ser interpretados, es necesario que éstos datos pasen a través de las capas inferiores en el transmisor, pasen por el medio físico y de forma inversa al transmisor, vayan de la capa más baja en el receptor hasta la capa n.

Para que este procedimiento se lleve a cabo, a la información en la capa n debe agregársele información de señalización como son las direcciones físicas y lógicas para identificar el origen y destino de dicha información, así como otro tipo de identificadores que permitan sincronizar y aportar información diversa acerca del contenido de los mensajes.

Cada capa agrega su propia información (encabezados y suma de control de errores FCS o *tail*) a los datos que llegan desde la capa superior, formando un PDU (*Packet Data*

[3] Direccionamiento IP, identificador de 32 bits que permite enrutar la información a su destino. Consulte el glosario para referencia rápida.

[4] Se refiere a la representación particular que tienen los datos provenientes de capas inferiores.

Unit) de capa n, es decir, la forma que toman estos datos una vez que han sido encapsulados [8].

Dicho conjunto de datos se transmitirá de forma integra a la capa inferior, es decir, su contenido será oculto a dicha capa y ésta considerará que la PDU capa n recibida son los datos útiles a transmitir y agregara su propia información, volverá a empaquetar en una nueva PDU capa n-1, y así sucesivamente a través de las diversas capas hasta llegar al medio físico.

En cada etapa se asigna entonces un nuevo nombre a cada PDU para reflejar el cambio que ha sufrido al atravesar cada una de las capas, de forma genérica se les denomina [8]:

1. Datos: el término general para las PDU en las capas de aplicación.
2. Segmento: PDU en la capa de transporte.
3. Paquete o Datagrama: PDU en la de Internet.
4. Trama: PDU de la capa de acceso a la red.
5. Bits: una PDU que se utiliza cuando se transmiten físicamente datos a través de un medio.

Se observa de forma grafica en la e Figura 2.4:

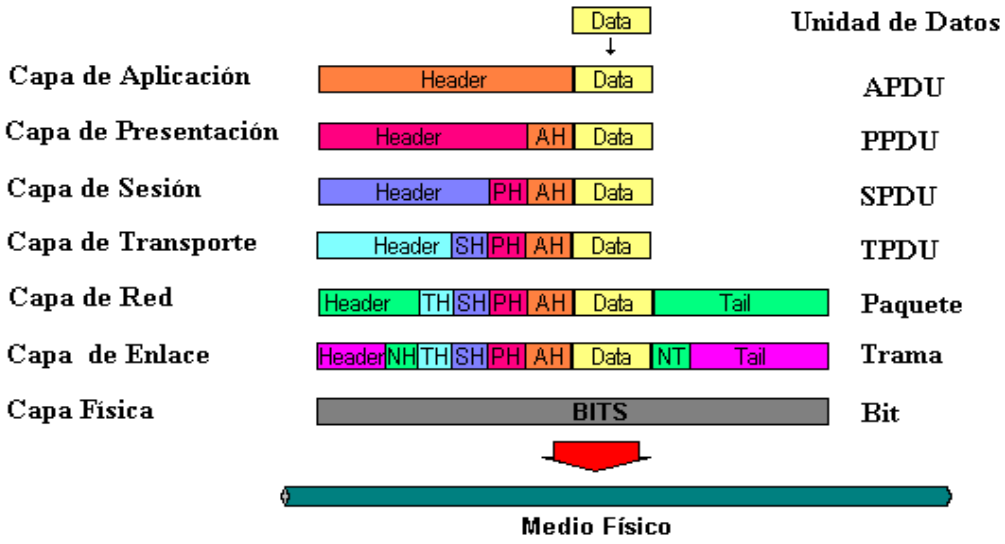

Figura 2.4. Encapsulamiento de datos en modelo OSI

En el receptor se efectúa el proceso inverso, es decir, para extraer la información que corresponde a cada capa es necesario quitar los encabezados y FCS que han sido agregados en las etapas previas para leer la información correspondiente. Este proceso se conoce como desencapsulamiento de la información.

2.4 MODELO TCP/IP

2.4.1 Definición

Es un modelo que se creó en la década de 1970, por DARPA la cual es una agencia del departamento gubernamental del Departamento de Defensa de los Estados Unidos y que evoluciono en ARPNET que fue la primera red de área amplia que precedió a Internet [5].

Este modelo describe un conjunto de guías para la implementación y diseño de protocolos de red parta permitir la interconexión de dispositivos en una red. Provee una conectividad *end-to-end* especificando el formato de los datos y su forma de transmisión, direccionamiento y ruteo. Define protocolos con diverso propósito de acuerdo a los servicios que se pretenda implementar dentro de la red.

Se integra por cuatro capas y su forma de comunicarse es muy similar a la descrita para el modelo OSI pues también están jerarquizadas y cada una lleva a cabo diversas funciones específicas. La Figura 2.5 muestra una analogía entre el modelo TCP/IP y el modelo OSI:

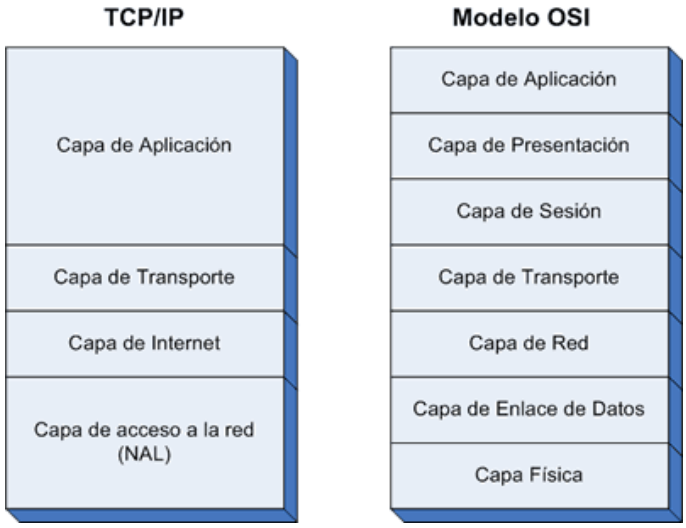

Figura 2.5. Comparación modelo TCP/IP y OSI

2.4.2 Descripción de las capas y protocolos asociados

La Figura 2.6 ilustra los protocolos que se asociaron originalmente al modelo TCP/IP en cada una de las capas que lo conforman:

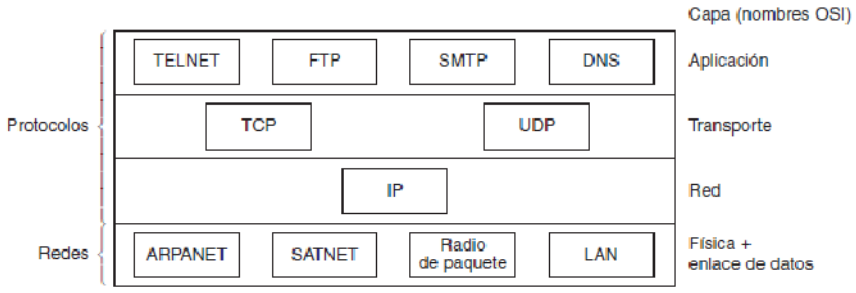

Figura 2.6. Protocolos en modelo TCP/IP

A continuación se describe de forma general la función de cada una de estas capas, de acuerdo con [5], [6] y [8] :

- ***Capa de aplicación***

  Esta capa engloba de forma teórica a las capas de aplicación, transporte y sesión definidas en el modelo OSI. No se describen las últimas dos en éste modelo pues se ha probado que son de poca utilidad para muchas de las aplicaciones. Contiene los protocolos de nivel más alto, es decir, aquellos que definen la interacción con el usuario final, entre ellos están: la terminal virtual (TELNET), transferencia de archivos (FTP) y correo electrónico (SMTP), DNS (*Domain Name Server*) para la resolución de nombres de host en sus direcciones de red; NNTP, para transportar los artículos de noticias de USENET; HTTP, para las páginas de *World Wide Web*, entre otros.

- ***Capa de transporte***

Está diseñada para permitir que los hosts de origen y destino puedan comunicarse (conversar) en sus entidades iguales; define dos protocolos de extremo a extremo.

  - ***TCP[5] (Transport Control Protocol):*** es un protocolo confiable, orientado a conexión que garantiza que la información originada en un punto de la red se entregue sin errores en otro punto de la misma. Todas las conexiones que se efectúan a través de él deben ser full dúplex y punto a punto. Para ello, divide el flujo de bytes entrantes en segmentos pequeños denominados mensajes discretos (fragmentación), y los entrega a la capa de Internet. En el destino, el protocolo TCP re-ensambla los mensajes recibidos, además de proveer un control de flujo para evitar saturación en el receptor y cuellos de botella. Se define a detalle en la RFC 793, y se publican correcciones en la RFC 1122 [3].

[5] Dado que este protocolo es importante para el presente trabajo se describirá de forma más detallada en la sección siguiente.

- ***UDP (User Datagram Protocol):*** protocolo no confiable y no orientado a conexión para aplicaciones para las que no se requiere estricto control de flujo y secuenciación, o para aquellas que la entrega a tiempo es prioritaria sobre la entrega precisa; como son aplicaciones en tiempo real (por ejemplo voz y video *streaming*) y otras aplicaciones como consultas cliente-servidor en una sola entrega. Se define en detalle en la RFC 768.

El presente trabajo se enfoca en considerar al **protocolo TCP** como el protocolo de capa de transporte usado para los estudios de la eficiencia volumétrica.

- ***Capa de Internet***

Permite que los hosts inyecten paquetes en la red y que estos viajen de forma independiente hacia su destino, sin importar que lo hagan de forma desordenada, pues las capas superiores se encargan de ordenarlos, es decir, permiten la conmutación de paquetes. De acuerdo con [3], define como el protocolo oficial a:

- ***IP (RFC-791 Internet Protocol)***[6]: que es el protocolo que permite el correcto enrutamiento de los paquetes a través de la red mediante las direcciones IP, Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de la red, sin embargo, o no fue diseñado para rastrear ni administrar el flujo de paquetes. En el presente trabajo se tratara únicamente con la versión 4 de dicho protocolo (IPv4). Sus características son:
  - Sin conexión: No establece conexión antes de enviar los paquetes de datos.
  - Máximo esfuerzo (no confiable): No se usan encabezados para garantizar la entrega de paquetes.
  - Medios independientes: Operan independientemente del medio que lleva los datos.

- ***Capa de acceso a la red***

Describe las funciones en conjunto de la capa física y de enlace de datos. De forma general se establece que el host debe conectarse a la red usando el mismo protocolo en ambos lados de la comunicación para poder enviarse mensajes IP en la capa de Internet.

No se especifica en este modelo de referencia la forma en que se procesa la información a éste nivel, pues depende del tipo de red a implementar el formato que tomarán los datos.

[6] Se ampliara su descripción en una sección posterior.

Para el desarrollo del presente trabajo, esta capa está definida por los estándares [1] y [2], los cuales se expondrán de forma más amplia en los capítulos 3 y 4 respectivamente. Como ilustración del proceso de encapsulación y des encapsulación de los datos en este modelo, el cual es análogo al descrito para el modelo OSI, la Figura 2.7 [6] resulta muy útil para observar de forma gráfica el procedimiento.

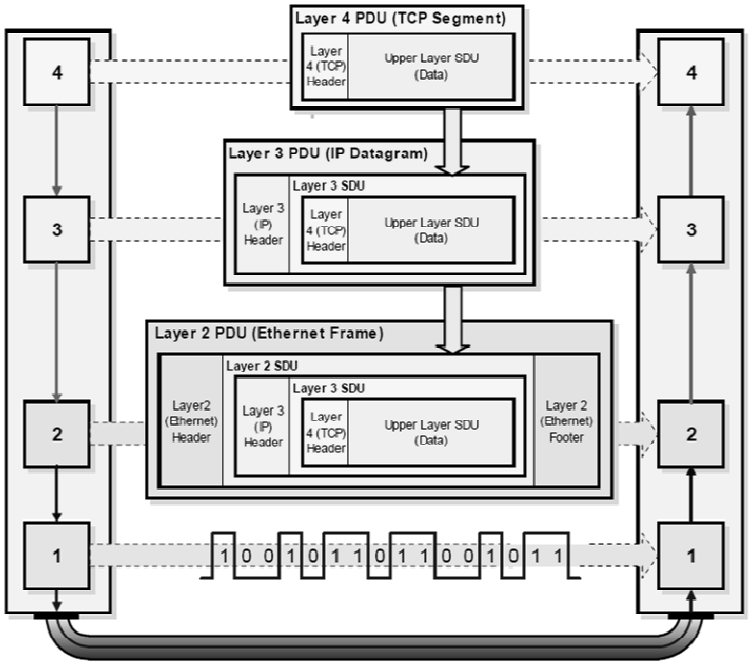

Figura 2.7. Encapsulación de datos en modelo TCP/IP.

2.5 PROTOCOLO TCP

Se describieron con anterioridad de forma general las características de éste protocolo. En esta sección se hace énfasis en describir el formato de los segmentos TCP haciendo énfasis en el tamaño de éstos y en la fragmentación que se presenta en esta capa. Ambos parámetros son los más útiles y fundamentales para llevar a cabo el estudio de la eficiencia volumétrica en este tema.

2.5.1 Formato de los segmentos TCP

La Figura 2.8, tomada de [5] ilustra la distribución de un segmento TCP:

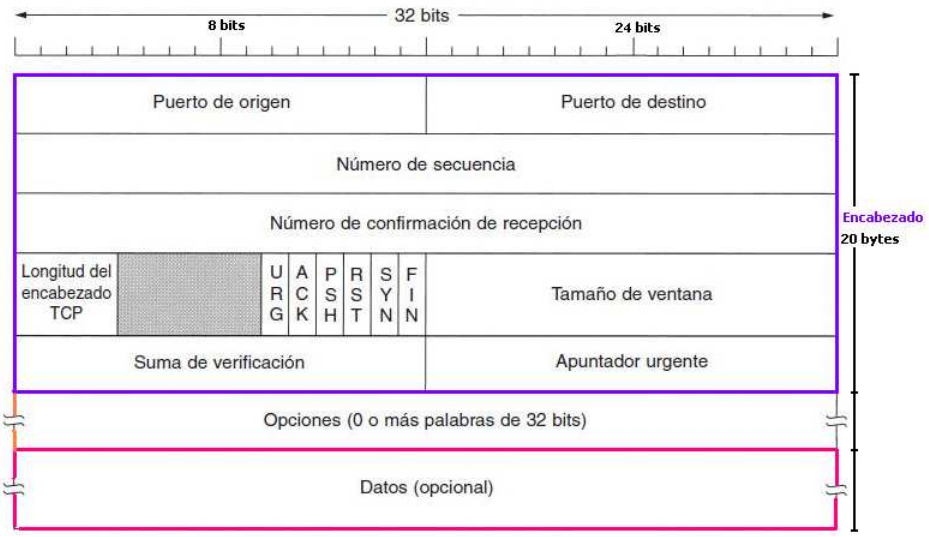

Figura 2.8. Segmento TCP

Sus campos de acuerdo con [5] son los siguientes:

- ***Encabezado (20 a 60 bytes):*** cada segmento comienza con éste campo; su formato tiene una tamaño fijo de *20 bytes (160 bits*) pero puede estar seguido de opciones, que de estar presentes, pudieran ocupar hasta 60 bytes en total (20 bytes + 40 bytes = 160 bits + 320 bits = 480 bits).

  A continuación se desglosaran de forma breve cada uno de los campos que componen el encabezado.

  Puerto de origen y destino (2 bytes cada uno= 16 bits cada uno): su función es identificar los puntos locales terminales de la conexión. Pueden ser *puertos*[7] bien conocidos o los que el host en cuestión asigne. En conjunto con la dirección IP (32 bits) forman un punto terminal único de 48 bits.

  Número de secuencia (4 bytes =32 bits): se usa en caso de fragmentación para designar el orden e los fragmentos.

  Número de confirmación de recepción (4 bytes =32 bits): especifica el siguiente byte esperado y no el último que se haya recibido de forma correcta.

[7] Para mayor información consultar el glosario.

Longitud del encabezado (4bits): indica la cantidad den palabras de 32 bits contenidas en el encabezado TCP. Es necesaria pues el campo de opciones es de longitud variable. Indica también comienzo de los datos en el segmento.

Reservado (6 bits): campo reservado para uso futuro.

Indicadores de 1 bit cada uno (6 bits):

- ***URG:*** indica si se usa el ***Apuntador Urgente (16 bits = 2 bytes),*** el cual sirve para indicar un desplazamiento en bytes a partir del número de secuencia si hay datos urgentes.
- ***ACK:*** indica si el número de confirmación de recepción es válido o no.
- ***PSH:*** indica la presencia de datos que deben transmitirse de inmediato.
- ***RTS:*** se usa para indica el restablecimiento de una conexión que haya fallado o rechazar el intento de iniciar una.
- ***SYN:*** denota *Connection Request* o *Connection Accept*, es decir, sirve para establecer el estado de la conexión en conjunto con ACK.
- ***FIN:*** se usa para liberar una conexión, especifica que el emisor no tiene más datos que transmitir.

Tamaño de ventana (2 bytes=16 bits): indica la cantidad de bytes que pueden enviarse, iniciando con el byte del que se ha confirmado recepción.

Suma de verificación (2 bytes=16 bits): sirve para verificar la integridad del encabezado, agrega confiabilidad.

Apuntador Urgente (2 bytes=16 bits): se describió brevemente en el indicador URG.

Opciones (variable máximo 40 bytes=320 bits en palabras de 32 bits): agrega características a las funcionalidades estándar del segmento, puede por ejemplo, indicar un número máximo de carga útil TCP que cada host está dispuesto a recibir, enviar opciones de sincronización, y otras.

Una vez que se han descrito los campos del encabezado, la cantidad que agrega a la información de usuario el protocolo TCP es un máximo de 60 bytes, sin embargo, la cantidad más usual es de 20 bytes, por lo cual se considerará para el presente trabajo que:

$$\boldsymbol{EncTCP = 20\ [bytes]} \qquad \boldsymbol{(1)}$$

2.5.2 Fragmentación en TCP

Es importante considerar el hecho de que el tamaño de los segmentos que se intercambian a través de la red los decide el software TCP, de acuerdo con [5], es por ello que puede agrupar fragmentos de un segmento para crear uno solo o bien, dividir uno que sobrepase el tamaño máximo en varios segmentos más pequeños.

Hay dos límites que restringen éste tamaño (encabezado TCP+ carga útil):

1. El tamaño de la carga útil del protocolo de capa de red, pues el segmento TCP debe ser encapsulado en este campo. Como se considerará al protocolo IP como el protocolo de capa de red, este tamaño es de 65 515 bytes.

2. El tamaño de la ***Máxima Unidad de Transferencia (MTU),*** que es propio de cada red y en el que debe caber cada segmento TCP. En la práctica se usa una MTU de 1500 bytes.

En el presente trabajo se tomara en cuenta la fragmentación llevada a cabo por el protocolo TCP considerando los parámetros mencionados para la **fragmentación por MTU**

2.6 PROTOCOLO IP

Análogo al protocolo TCP, se ha presentado ya una descripción general del propósito y características del protocolo IP, que opera en la capa de red. A continuación se describirá de forma breve la estructura de un datagrama IP.

2.6.1 Formato de los paquetes IP

Un paquete IP está integrado por un encabezado y una sección de datos útiles (también conocido como *payload*). El encabezado, al igual que en el protocolo TCP tiene una longitud fija de 20 bytes más el campo opciones.

De acuerdo con [5], la estructura de un paquete IP está establecida como se muestra en la Figura 2.9.

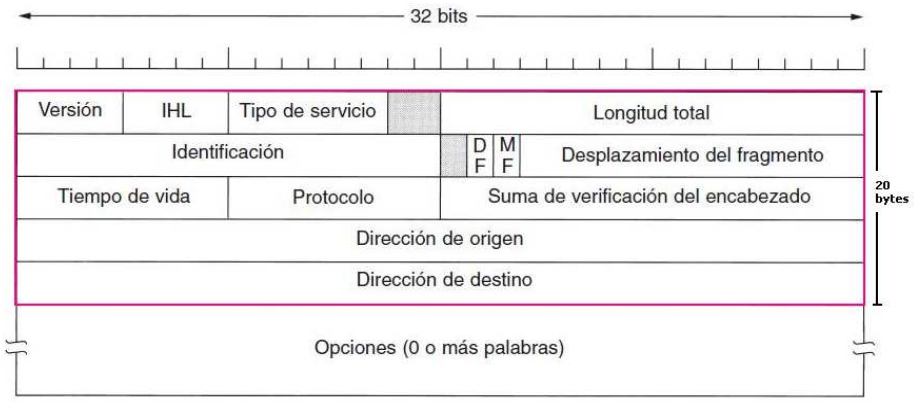

Figura 2.9. Encabezado IP

A continuación, se hará una breve descripción de los campos que integran el encabezado, de acuerdo con [5] y [6]:

Versión (4 bits): indica el número de la versión del protocolo IP que se esté usando; por ejemplo IP versión 4 o versión 6.

Longitud de la cabecera de Internet (HIL, Internet Header Length) (4 bits): longitud de la cabecera medida en palabras de 32 bits. Su valor mínimo es cinco (20 bytes) y el máximo 15 (60 bytes).

Tipo de servicio (1 byte= 8bits): indica parámetros de seguridad prioridad, retardo y rendimiento; es decir, distingue clases de servicio relacionados al QoS.

Identificación (2 bytes= 16 bits): es un número que sirve para identificar a los fragmentos de un mismo datagrama. Junto a la dirección origen y destino caracterizan de forma única a cada uno de ellos, por tanto todos los fragmentos del mismo datagrama tiene el mismo identificador.

Indicadores (3bits= 1 bit cada uno):

- ***Primero:*** es un campo no definido.
- DF ***(Do not Fragment o no fragmentar):*** es una indicación para los ruteadores que le indica que no deben fragmentar el paquete pues el destino no los re-ensambla.
- ***MF (Más Fragmentos o More Fragments***): está establecido en todos los paquetes excepto el último, para indicar que aun hay (todos los fragmentos antes del último) o que ya no hay más fragmentos.

Desplazamiento del fragmento (13 bits): indica el lugar del datagrama actual en el que se debe colocar el fragmento en cuestión. Todos los fragmentos deben tener un múltiplo de 8 bytes, y como son 13 bits puede haber un máximo de 8192 fragmentos en un paquete.

Tiempo de vida (1 byte= 8 bits): especifica en segundos el tiempo que puede permanecer un paquete en la red antes de ser descartado.

Suma de comprobación de cabecera (2 bytes =16 bits): verifica la integridad del encabezado. Es cero cuando el paquete llega sin errores.

Dirección origen y destino (4 bytes=32 bits cada una): contienen la dirección IP del host de origen o destino respectivamente. Indican la red a la que pertenecen y el identificador del host.

Si se realiza la suma de los valores en bytes de los campos ya mencionados, se podrá verificar que la longitud mínima para éste encabezado es de 20 bytes.

Opciones (máximo 40 bytes): indica opciones para seguridad, enrutamiento libre o estricto, registra ruta y mide tiempos.

De igual forma que con TCP, para el presente trabajo se considerara que la longitud del encabezado IP es:

$$\boldsymbol{EncIP = 20\ [byes]} \quad (2)$$

2.7 Redes Inalámbricas de Área Local (WLAN)

2.7.1 Definición

Una red inalámbrica de área local WLAN *(Wireless Local Area Network*) es un sistema de comunicación que se utiliza para comunicar dispositivos que se encuentren dentro de un entorno físico relativamente pequeño y limitado, como son hogares, oficinas, escuelas, pisos dentro de un edificio, entre otros con la ventaja de que no existe cableado entre dichos dispositivos.

La Figura 2.10 muestra una configuración común para las WLAN, en esta se aprecia que la red tiene diversos dispositivos comunicados con estaciones centralizadas llamadas Access Points (AP's) los cuales se comunican con él de forma inalámbrica (su área de cobertura se señala con un ovalo) y una parte de la red se comunica con redes cableadas. A continuación se describirán de forma más detallada su arquitectura.

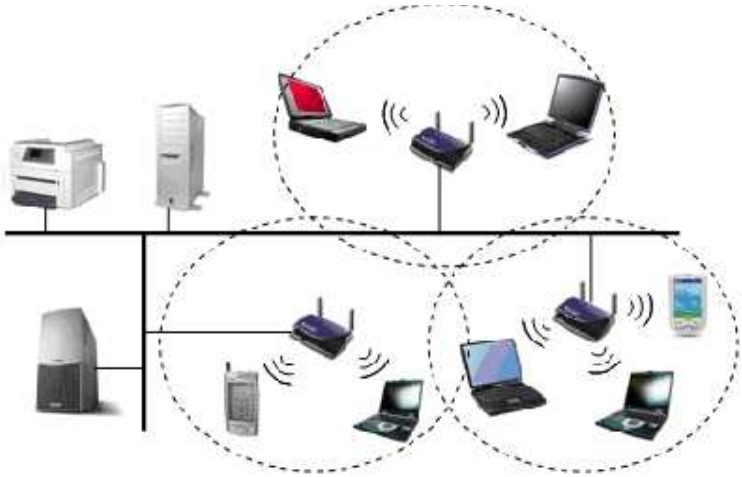

Figura 2.10. Ejemplo de una red WLAN

2.7.2 Características

- *Movilidad*: permite transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario. Esto supone mayor productividad y posibilidades de servicio.

- *Facilidad de instalación*: al no usar cables, se evitan obras cablear a través de muros y techos, mejorando así el aspecto y la habitabilidad de los locales, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red.

- *Flexibilidad:* puede llegar donde el cable no puede, superando mayor número de obstáculos, de esta forma es útil en zonas donde el cableado no es posible o es muy costoso: parques naturales, reservas o zonas escarpadas.

2.7.3 Arquitectura

Una red WLAN está constituida por diversos elementos que hacen posible la interconexión de los dispositivos inalámbricos, los cuales son:

- **Estaciones:** todos los componentes que pueden ser conectados a un medio inalámbrico están referidos a una estación, la cual está equipada con tarjetas de interfaz de red inalámbrica (WNICs); las estaciones pueden ser de dos categorías:
- ***Puntos de acceso (APs Access Points):*** son ruteadores que transmiten y reciben el tráfico mediante enlaces de radiofrecuencia para establecer la comunicación. Tienen un alcance finito, del orden de 150 m en lugares u zonas abiertas.

Figura 2.11 Imagen de un AP

Clientes: son los dispositivos inalámbricos que se conectan al punto de acceso, pueden ser móviles como un teléfono celular o laptop, incuso estaciones de trabajo. Están equipados con una interfaz de red inalámbrica, como son: tarjetas PCMCIA[8] que no permiten acedar a conexión de alta velocidad y las tarjetas USB, el tipo de tarjeta más común que existe y más sencillo de conectar a una PC.

Conjunto de servicio básico (Basic Service Set BSS): conjunto de estaciones que pueden intercomunicarse, cada una de ellas tiene un identificador que es la dirección MAC del punto de acceso. Hay dos tipos:

- Independientes: no contienen puntos de acceso, es decir, no pueden conectarse con otro dispositivo fuera de su rango de acceso.

- De infraestructura: pueden comunicarse con otra estación fuera de su propio conjunto de servicio básico través de puntos de acceso.

Conjunto de servicio extendido (Extended Service Set ESS): es un conjunto de dos o más conjuntos de servicio básicos (BSS), cuyos puntos de acceso están conectados a un sistema de distribución; tiene un identificador de 32 bits denominado SSID.

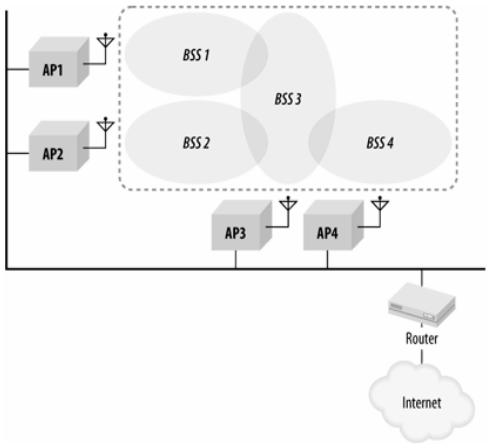

Figura 2.12.Conjunto de BSS interconectados.

[8] PCMCIA: *Personal Computer Memory Card International Association*

Sistema de distribución: conecta puntos de acceso de Conjuntos de servicio entendido. El concepto de un DS (*Distribution System*) puede ser usado para incrementar la cobertura de la red cambiando entre diversas celdas.

2.7.4 Tipos de redes WLAN

Punto a punto (Peer-to-Peer) o "Ad Hoc": es una red inalámbrica en la que las estaciones se comunican únicamente entre ellas de forma directa (sin intervención de una estación de puntos de acceso) mediante el Conjunto Básico de Servicio Independiente (IBSS). Usan el espacio de cobertura para descubrirse e iniciar comunicaciones

Figura. 2.13 Red Ad-Hoc

Puente: puede usarse para conectar redes de diferente tipo; actúa como un punto de acceso para ambos dispositivos, por ejemplo, al conectar una red inalámbrica Ethernet con una alambica, el puente es un punto de acceso para la red WLAN.

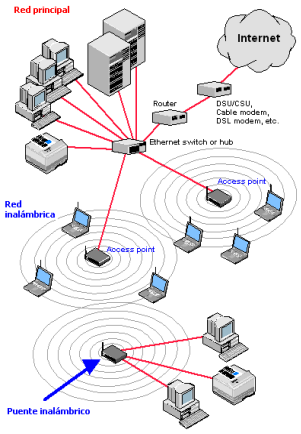

Figura 2.14. Red inalámbrica interconectada a redes cableadas

Sistema de distribución inalámbrico (Wireless Distribution System): sistema que permite la interconexión de puntos de acceso, permite a la red inalámbrica ampliar la zona de cobertura sin la necesidad de un enlace cableado al *Backbone* (red troncal) para interconectarse, es decir, preserva las direcciones MAC de los clientes a través de diversos puntos de acceso, las conexiones entre clientes se realizan usando direcciones MAC en lugar de direcciones IP. Se deben configurar los diversos puntos de acceso a un mismo canal de radio.

2.8 REDES DE ÁREA METROPOLITANA WMAN Y ACCESO INALÁMBRICO DE BANDA ANCHA BWA

2.8.1 Definición

Una ***red inalámbrica de área metropolitana WMAN*** es una red de datos que ofrece una cobertura en un área geográfica amplia de algunos kilómetros, como puede ser un campus amplio en una universidad o incluso una ciudad.

Se basan en el estándar desarrollado por la IEEE 802.16 el cual se inicio en 1979, y en Febrero de 1980 se creó el comité o grupo de trabajo para definir el estándar de las redes MAN. Sus protocolos y servicios se enfocan en las dos capas más bajas del modelo OSI[9] (enlace de datos y física). Algunos ejemplos son las redes de telefonía celular.

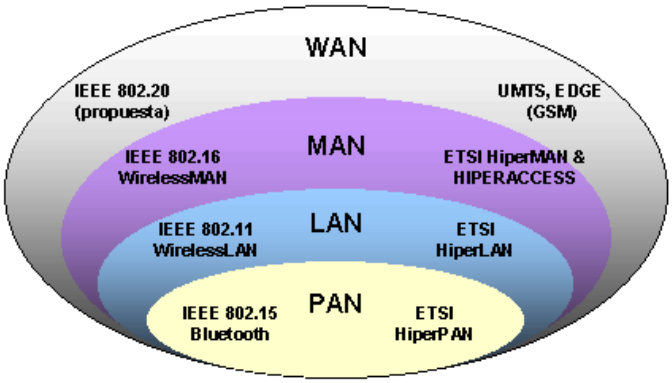

Figura 2.15. Estándares de redes inalámbricas según su cobertura geográfica

BWA (*Broadband Wireless Access*)

Las **redes BWA** tiene una rango de alcance mucho mayor que la redes WLAN (en el orden de los 50 km), además de ofrecer tasa de transmisión mucho mayores y son más económicas que otras tecnologías como la fibra óptica.

Han emergido de forma muy rápida pues el consumo cada vez mayor de las aplicaciones multimedia han generado una demanda extra en el ancho banda que llega a los usuarios finales; es por esta razón que se hace necesario adicionalmente, implementar técnicas de calidad de servicio (QoS) las cuales permiten ofrecer a los usuarios diferentes tipos de servicios de acuerdo con el tipo de tráfico que manejen.

[9] Se describirá en la sección 2.3 del presente trabajo.

2.8.2 Arquitectura de redes BWA

Un sistema fijo BWA incluye al menos una ***estación base (BS)*** y una o más ***estaciones suscriptoras (SS).*** La ***estación base*** es un nodo central y las estaciones suscriptoras son nodos remotos colocados a diferentes distancias de la estación base.

- ***Estación base (BS):*** se encarga de controlar y manejar la conexión. Envía datos a través del canal de bajada o Downlink el cual ha sido asignado a varios suscriptores. Una estación base puede cubrir varios celdas (sectores) con la ayuda de patenas sectoriales. En una configuración *PMP (Point to Multipoint o Punto a Multipunto*) el canal *Downlink* es multipunto. Cada estación base es configurada con una dirección MAC de 48 bits, en la cual los primeros 24 bits identifican al operador.

- ***Estación suscriptora (SS):*** es una terminal que se comunica con la BS. Envía datos a través del canal de subida *Uplink* el cual es punto a punto en una configuración PMP o punto multipunto en una configuración *Mesh*. Todos los suscriptores en la misma área y canal de frecuencia reciben la misma información de *Downlink* (*Broadcasting*). Una dirección MAC de 48 bits identifica de forma única a un suscriptor.

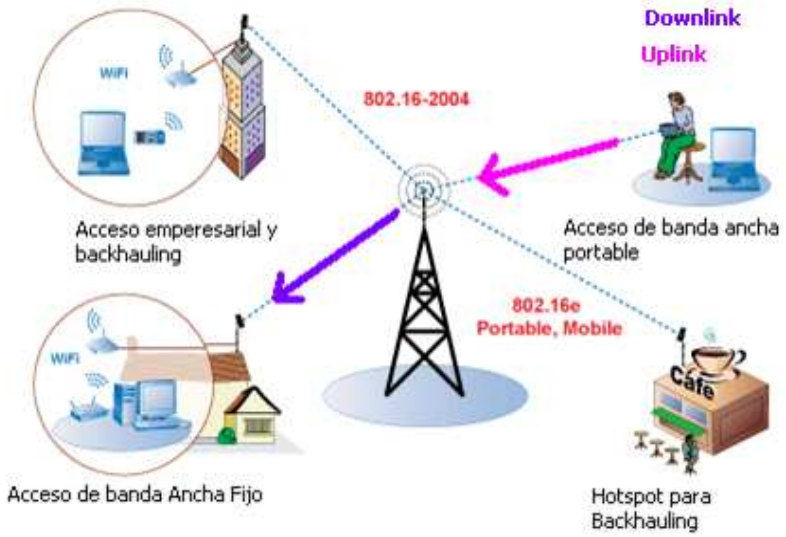

Figura 2.16. Arquitectura BWA

En el canal de subida, el tiempo es dividido en ranuras denominadas *mini-slots*, los cuales proporcionan acceso múltiple por división de tiempo (TDMA)[10]; mientras que el canal de bajada se utiliza un esquema de multiplexión por división de tiempo.

[10] Se describirá con mayor detalle en el Capítulo 4.

Cada SS puede enviar voz y datos utilizando interfaces comunes, como teléfono, Ethernet, video, VoD (*Video on Demand*) y otros servicios con diferentes requerimientos en cuanto a calidad de servicio.

2.8.3 Aplicaciones y tipos de acceso

Esta tecnología está representada por el estándar IEEE 802.16, algunas de sus aplicaciones son el ***acceso fijo*** con una alta tasa de datos, la cual puede ser utilizada para el acceso a Internet, TV y otras aplicaciones que requieran dicho volumen de datos como Video en demanda; sin embargo, no en todos los casos resulta útil aplicarlo pues tecnologías como DSL que están fuertemente implantadas hacen que sea económicamente poco viable.

Otra aplicación es la denominada ***WiFi Backhauling*** (red de retorno), es decir, la interconexión con las redes WiFi. Dicha conexión consiste en enlazar los puntos de acceso (AP) al *Backbone* de Internet a través de estaciones base (BS) en línea de vista con otras estaciones base; sin embargo no la hay con las estaciones suscriptoras, es por ello que éstas deben contar un con un Equipo de Permisos de Consumidor CPE *(Consumer Permises Equipment*) que es un canal de radio que lleva a cabo el enlace entre la estación base y el equipo terminal. Después del CPE el usuario instala su equipo terminal conectado a un AP WiFi. Entonces la BWA lleva a cabo el retorno de la información hacia la red WiFi.

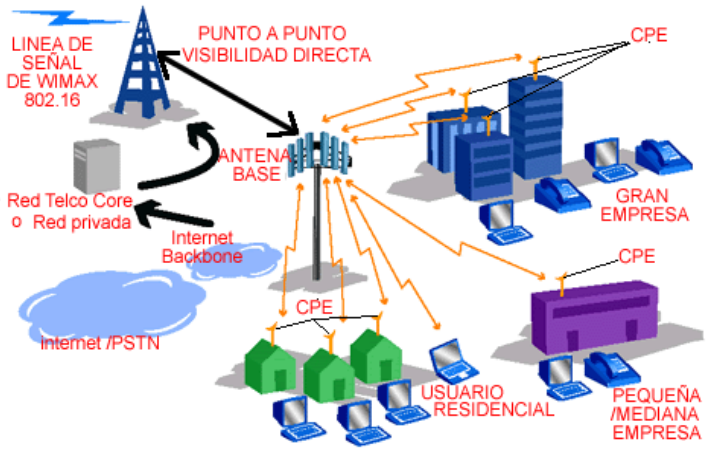

Figura 2.17. Aplicación *WiFi Backhauling*

Las aplicaciones ***nómadas o wireless*** permitirían conservar activas las conexiones o sesiones ya establecidas cuando el se mueva dentro del área de cobertura de una BS. Esto es muy útil, sin embargo, la BS y SS no tendrían línea de vista en muchas ocasiones debido al movimiento de la SS.

Por último, está el caso en el que existe ***movilidad,*** en este escenario, la estación suscriptora se mueve tanto que puede salir del área de cobertura de una BS y cambiarse a

otra BS para que continúe recibiendo el servicio (*Handover*), conservando activas las conexiones realizadas en la primera BS.

Incluye también el hecho de que, en igual forma, la sesión continua activa cuando la estación suscriptora se mueva con una velocidad considerable, mayor a los 350 Km/h, en otros casos, donde la velocidad está limitada al orden de los 120 Km/h, se habla de portabilidad más que de movilidad.

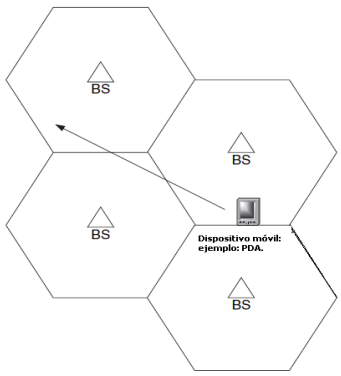

Figura 2.18. El dispositivo móvil cambia de una BS a otra sin reiniciar la sesión

2.9 CONCLUSIONES

En el presente Capítulo se retomaron conceptos básicos de redes como son el protocolo, su jerarquía, la relación entre esto y los servicios. Se describieron de forma puntual algunos protocolos de capa de aplicación y de transporte, aso como el protocolo de red IP, lo cual resultara útil paras secciones posteriores. Además se estableció a TCP como el protocolo de capa de aplicación a utilizar por su amplio uso y por ser orientado a conexión.

De igual forma se presentaron las definiciones de redes de área local WLAN y redes de banda ancha inalámbrica BWA, las cuales tiene ámbitos de aplicación totalmente distinto, aso como arquitecturas análogas, pero a su vez muy distintas que les permiten tener tal diversidad de características.