UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

"DIPLOMADO INTEGRAL EN TELECOMUNICACIONES APLICADO A LA OPTIMIZACIÓN DE APPLICATIONS SERVERS"

T R A B A J O E S C R I T O

EN LA MODALIDAD DE SEMINARIOS Y CURSOS DE ACTUALIZACIÓN Y CAPACITACIÓN PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

JOSÉ MARÍA OROPEZA RANGEL

ASESOR: ENRIQUE GARCÍA GUZMÁN

MEXICO, 2010.

ÍNDICE

AGRADECIMIENTOS

- A mis padres, por todo el apoyo y confianza que siempre han tenido en mí.
- Al Ing. Enrique García Guzmán, por sus enseñanzas y apoyo.
- Al Ing. Eleazar Margarito Pineda Díaz, por sus enseñanzas y apoyo.
- Al Ing. Alfredo Montaño Serrano, por sus enseñanzas y apoyo.
- A la Lic. Norma Reyes Tecontero, por sus enseñanzas y apoyo.
- Al Ing. Efrén Jesús Guerrero Santamaría, por sus enseñanzas y apoyo.

OBJETIVO GENERAL

Explicar diversas tecnologías acerca del ámbito de las telecomunicaciones permitiendo tener una idea general acerca de estas.

Mostrar el avance y la funcionalidad de cada tecnología y como es que se puede aplicar en el ambiente laboral, así como presentar nuevas y diversas opciones de cómo se podría resolver cierto caso de negocio.

Justificar la importancia de estos componentes, mecanismos y tecnologías haciendo notar el gran aporte profesional y como es que el presente trabajo permite tener una visión más amplia a la hora de resolver un problema relacionado en la empresa.

JUSTIFICACIÓN

Hoy día el área de ingeniería ha tenido gran evolución y las empresas han tenido que migrar constantemente el tipo de tecnología que utilizan, existen diferentes opciones para resolver cualquier tipo de problema, ya sea en el tipo de red, topología, protocolo, u otro tipo de componente. Es por eso que en el siguiente trabajo se muestran diversos caminos para llegar a la mejor respuesta.

En los capítulos de esta tesina se muestran temas de tecnologías de la información y telecomunicaciones así como las diferentes características de estas, además de las diferentes formas de aplicación, el tipo de protocolos que pueden soportar y cuando pueden ser utilizados. Por otra parte se da idea de cómo pueden ser aplicados todos estos conceptos y metodologías, para su mejor aprovechamiento.

Con estas justificaciones se puede decir que el diplomado en telecomunicaciones genera y amplía la perspectiva del egresado.

MODULO 1

INTRODUCCIÓN

MODULO 1: INTRODUCCIÓN

La intención de este trabajo de titulación es proporcionar las bases fundamentales en el área de las telecomunicaciones, con objeto de conocer algunas de sus ventajas, su infraestructura y la forma en que estas tecnologías funcionan.

Este trabajo esta basado en el diplomado Integral de telecomunicaciones, en el cual se impartieron diversos módulos donde se vieron distintos enfoques y diferentes perspectivas acerca del mundo de las telecomunicaciones.

La telecomunicación (comunicación a distancia) es una técnica que consiste en transmitir un mensaje desde un punto a otro, normalmente con el atributo típico adicional de ser bidireccional. El término telecomunicación cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de ordenadores.

Telecomunicaciones, es toda transmisión, emisión o recepción de signos, señales, datos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de cables, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos.

A lo largo de esta tesina se dará una explicación de estos conceptos, así como una descripción de las tecnologías que estos requieren.

1.1 Telecomunicación

El concepto de telecomunicación abarca todas las formas de comunicación a distancia. Es una técnica que consiste en la transmisión de un mensaje desde un punto hacia otro, usualmente con la característica de poder transmitir y recibir información.

El físico ingles James Clerk Maxwell fue el responsable de sentar las bases para el desarrollo de la telecomunicación, al introducir el concepto de onda electromagnética para describir mediante las matemáticas la interacción entre la electricidad y

magnetismo. De esta forma Maxwell anuncio que era posible propagar ondas por el espacio libre al utilizar descargas eléctricas.

La historia de las telecomunicaciones comenzó a desarrollarse en la primera mitad del siglo XIX, con el telégrafo eléctrico (que permitía enviar mensajes con letras y números). Más adelante apareció el teléfono, que agrego la posibilidad de comunicarse utilizando la voz. Con las ondas de radio, la comunicación inalámbrica llegó para completar una verdadera revolución en los hábitos de la humanidad.

Por supuesto, las innovaciones tecnológicas en el campo de las telecomunicaciones nunca se detuvieron. El MODEM posibilito la transmisión de datos entre computadoras y otros dispositivos, en lo que constituyo el punto de inicio para el desarrollo de Internet y otras redes informáticas.

1.2 Modelo de comunicación

La comunicación constituye una de las formas en que las personas interactúan entre sí, estableciendo lazos. Según el modelo de Shannon y Weaver, los elementos que deben darse para que se considere el acto de la comunicación son:

Emisor: Es quien emite el mensaje, puede ser o no una persona.

Receptor: Es quien recibe la información. Dentro de una concepción primigenia de la comunicación es conocido como Receptor, pero dicho término pertenece más al ámbito de la teoría de la información.

Canal: Es el medio físico por el que se transmite el mensaje.

Código: Es la forma que toma la información que se intercambia entre la Fuente (el emisor) y el Destino (el receptor) de un lazo informático. Implica la comprensión o decodificación del paquete de información que se transfiere.

Mensaje: Es lo que se quiere transmitir.

Situación o contexto: Es la situación o entorno extralingüístico en el que se desarrolla el acto comunicativo.

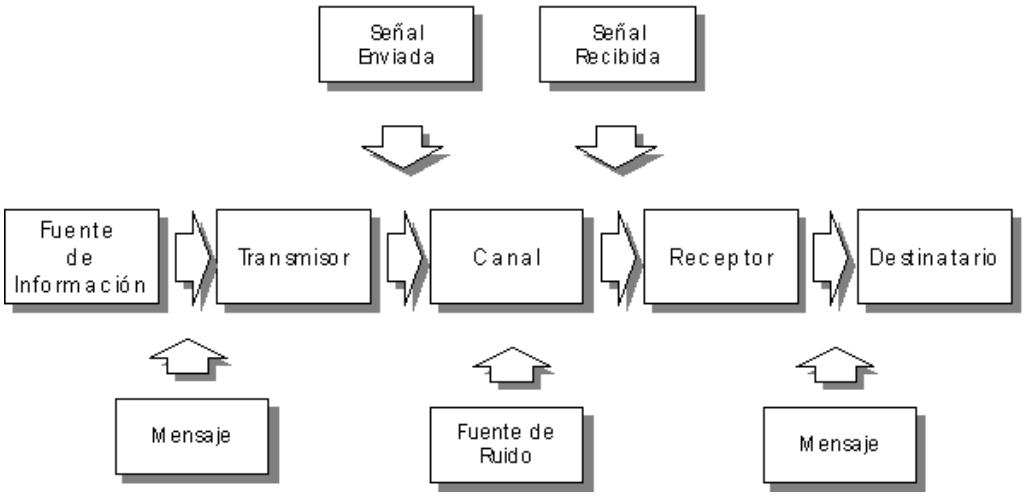


Figura 1.1 Modelo de Comunicación.

MODULO 2

MEDIOS DE TRANSMISIÓN ALÁMBRICOS

MODULO 2: MEDIOS DE TRANSMISIÓN ALÁMBRICOS

El medio de transmisión constituye el soporte físico a través del cual emisor y receptor pueden comunicarse en un sistema de transmisión de datos.

Los medios de transmisión conducen (guían) las ondas electromagnéticas a través de un camino físico, ejemplos de estos medios son el cable coaxial, la fibra óptica y el par trenzado.

La naturaleza del medio junto con la de la señal que se transmite a través de él, constituyen los factores determinantes de las características y la calidad de la transmisión. En el caso de estos medios es el propio medio el que determina principalmente las limitaciones de la transmisión: velocidad de transmisión de los datos, ancho de banda que puede soportar y espaciado entre repetidores.

Su uso depende del tipo de aplicación particular ya que cada medio tiene sus propias características de costo, facilidad de instalación, ancho de banda soportado y velocidades de transmisión máxima permitidas.

2.1 Líneas de par trenzado

El cable de par trenzado es una forma de conexión en la que dos aisladores son entrelazados para tener menores interferencias y aumentar la potencia y la diafonía de los cables adyacentes.

El entrelazado de los cables disminuye la interferencia. En la operación de balanceado de pares, los dos cables suelen llevar señales paralelas y adyacentes (modo diferencial), las cuales son combinadas mediante sustracción en el destino. El ruido de los dos cables se aumenta mutuamente en esta sustracción debido a que ambos cables están expuestos a interferencias electromagnéticas similares.[1]

1 Bruce A. Hallberg *Fundamentos De Redes* Mcgraw-Hill Interamericana, p. 43

La tasa de trenzado, usualmente es definida en vueltas por metro, forma parte de las especificaciones de un tipo concreto de cable. Cuanto menor es el número de vueltas, menor es la atenuación de la diafonía. Donde los pares no están trenzados, como en la mayoría de conexiones telefónicas residenciales, un miembro del par puede estar más cercano a la fuente que el otro y, por tanto, expuesto a niveles ligeramente distintos de interferencias electromagnéticas.

2.1.1 AWG

El AWG (American Wire Gauge), calibre de alambre estadounidense, es un organismo de normalización sobre el cableado, también es una referencia de clasificación de diámetros.

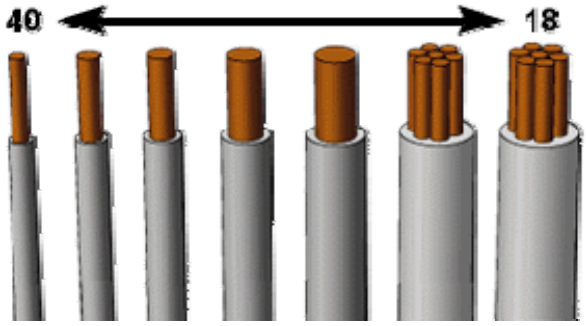


Figura 2.1 Diferencias entre calibres

Entre mas grande sea el valor AWG menor será el grosor o diámetro del conductor. El conductor 18 es más grueso que el cable 40, por ejemplo. Los primeros 5 cables (de izquierda a derecha) son sólidos y los últimos dos son hilados o trenzados (stranded). El hilo telefónico se utiliza como punto de referencia; tiene un grosor de 22 AWG.

2.1.2 Presentación del Cable UTP

El diseño del cable esta constituido por 4 pares trenzados. Los colores del aislante están estandarizados y son los siguientes:

- Par 1 Blanco/Azul Azul
- Par 2 Blanco/Naranja Naranja
- Par 3 Blanco/Verde Verde

- Par 4 Blanco/Marrón Marrón

Cada par de cables es un conjunto de dos conductores aislados con un recubrimiento plástico. Este par se trenza para que las señales transportadas por ambos conductores (de la misma magnitud y sentido contrario) no generen interferencias ni resulten sensibles a emisiones.

2.1.3 Categorías

La especificación 568A Commercial Building Wiring Standard de la asociación Industrias Electrónicas e Industrias de la Telecomunicación (EIA/TIA) especifica el tipo de cable UTP que se utilizará en cada situación y construcción. Dependiendo de la velocidad de transmisión ha sido dividida en diferentes categorías:

Categoría 1: Hilo telefónico trenzado de calidad de voz no adecuado para las transmisiones de datos. Las características de transmisión del medio están especificadas hasta una frecuencia superior a 1MHz.

Categoría 2: Cable par trenzado sin apantallar. Las características de transmisión del medio están especificadas hasta una frecuencia superior de 4 MHz. Este cable consta de 4 pares trenzados de hilo de cobre.

Categoría 3: Velocidad de transmisión típica de 10 Mbps para Ethernet. Con este tipo de cables se implementa las redes Ethernet 10BaseT. Las características de transmisión del medio están especificadas hasta una frecuencia superior de 16 MHz. Este cable consta de cuatro pares trenzados de hilo de cobre con tres entrelazados por pie.

Categoría 4: La velocidad de transmisión llega hasta 20 Mbps. Las características de transmisión del medio están especificadas hasta una frecuencia superior de 20 MHz. Este cable consta de 4 pares trenzados de hilo de cobre.

Categoría 5: Es una mejora de la categoría 4, puede transmitir datos hasta 100Mbps y las características de transmisión del medio están especificadas hasta una frecuencia superior de 100 MHz. Este cable consta de cuatro pares trenzados de hilo de cobre.

Categoría 6: Es una mejora de la categoría anterior, puede transmitir datos hasta 1Gbps y las características de transmisión del medio están especificadas hasta una frecuencia superior a 250 MHz.

Categoría 7. Es una mejora de la categoría 6, puede transmitir datos hasta 10 Gbps y las características de transmisión del medio están especificadas hasta una frecuencia superior a 600 MHz.

2.2 Cable coaxial

El cable coaxial es un cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes. Entre ambos se encuentra una capa aislante llamada dieléctrico, de cuyas características dependerá principalmente la calidad del cable. Todo el conjunto suele estar protegido por una cubierta aislante.

El conductor central puede estar constituido por un alambre sólido o por varios hilos retorcidos de cobre; mientras que el exterior puede ser una malla trenzada, una lámina enrollada o un tubo corrugado de cobre o aluminio. En este último caso resultará un cable semirrígido.

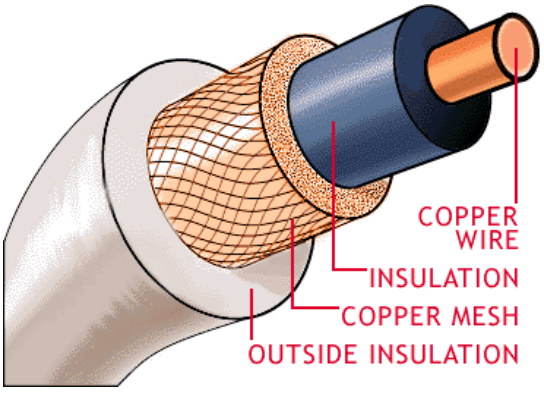


Figura 2.2 Cable Coaxial

2.2.1 Características del cable

El apantallamiento del cable protege los datos que se transmiten, absorbiendo el ruido, de forma que no pasa por el cable y no existe distorsión de datos. Al cable que contiene una lámina aislante y una capa de apantallamiento de metal trenzado se le llama cable apantallado doble. Para grandes interferencias, existe el apantallamiento cuádruple. Este apantallamiento consiste en dos láminas aislantes, y dos capas de apantallamiento de metal trenzado.

El núcleo de un cable coaxial transporta señales electrónicas que forman la información. Este núcleo puede ser sólido (normalmente de cobre) o de hilos.
Rodeando al núcleo existe una capa aislante dieléctrica que la separa de la malla de hilo. La malla de hilo trenzada actúa como masa, y protege al núcleo del ruido eléctrico y de la distorsión que proviene de los hilos adyacentes.

El núcleo y la malla deben estar separados uno del otro. Si llegaran a tocarse, se produciría un cortocircuito, y el ruido o las señales que se encuentren perdidas en la malla, atravesarían el hilo de cobre.

La malla de hilos absorbe las señales electrónicas perdidas, de forma que no afecten a los datos que se envían a través del cable interno. Por esta razón, el cable coaxial es una buena opción para grandes distancias y para soportar de forma fiable grandes cantidades de datos con un sistema sencillo.

Debido a la necesidad de manejar frecuencias cada vez más altas y a la digitalización de las transmisiones, en años recientes se ha sustituido paulatinamente el uso del cable coaxial por el de fibra óptica, en particular para distancias superiores a varios kilómetros, porque el ancho de banda de esta última es muy superior.

2.3 Fibra óptica

Las fibras ópticas son filamentos de vidrio de alta pureza extremadamente compactos: El grosor de una fibra es similar a la de un cabello humano. Fabricadas a alta temperatura con base en silicio, su proceso de elaboración es controlado por medio de computadoras, para permitir que el índice de refracción de su núcleo, que es la guía de la onda luminosa, sea uniforme y evite las desviaciones, entre sus principales

características se puede mencionar que son compactas, ligeras, con bajas pérdidas de señal, amplia capacidad de transmisión y un alto grado de confiabilidad debido a que son inmunes a las interferencias electromagnéticas de radio-frecuencia.

Las fibras no conducen señales eléctricas por lo tanto son ideales para incorporarse en cables sin ningún componente conductivo y pueden usarse en condiciones peligrosas de alta tensión. Tienen la capacidad de tolerar altas diferencias de potencial sin ningún circuito adicional de protección y no hay problemas debido a los cortos circuitos. Tienen un gran ancho de banda, que puede ser utilizado para incrementar la capacidad de transmisión con el fin de reducir el costo por canal; De esta forma es considerable el ahorro en volumen en relación con los cables de cobre.

En cada filamento de fibra óptica podemos apreciar 3 componentes:

- La fuente de luz: LED o láser.
- El medio transmisor: fibra óptica.
- El detector de luz: fotodiodo.

Un cable de fibra óptica está compuesto por: Núcleo, manto, recubrimiento, tensores y chaqueta. Cada filamento consta de un núcleo central de plástico o cristal (óxido de silicio y germanio) con un alto índice de refracción, rodeado de una capa de un material similar con un índice de refracción ligeramente menor. Cuando la luz llega a una superficie que limita con un índice de refracción menor, se refleja en gran parte, cuanto mayor sea la diferencia de índices y mayor el ángulo de incidencia, se habla entonces de reflexión interna total.

En el interior de una fibra óptica, la luz se va reflejando contra las paredes en ángulos muy abiertos, de tal forma que prácticamente avanza por su centro. De este modo, se pueden guiar las señales luminosas sin pérdidas por largas distancias.

2.3.1 Fibra multimodal

En este tipo de fibra viajan varios rayos ópticos reflejándose a diferentes ángulos. Los diferentes rayos ópticos recorren diferentes distancias y se desfasan al viajar dentro de la fibra. Por esta razón, la distancia a la que se puede trasmitir esta limitada.

2.3.2 Fibra multimodal con índice graduado

En este tipo de fibra óptica el núcleo esta hecho de varias capas concéntricas de material óptico con diferentes índices de refracción. La propagación de los rayos en este caso siguen un patrón similar mostrado en la figura.

En estas fibras él numero de rayos ópticos diferentes que viajan es menor y, por lo tanto, sufren menos el severo problema de las multimodales.

2.3.3 Fibra monomodal

Esta fibra óptica es la de menor diámetro y solamente permite viajar al rayo óptico central. No sufre del efecto de las otras dos pero es más difícil de construir y manipular. Es también más costosa pero permite distancias de transmisión mayores.

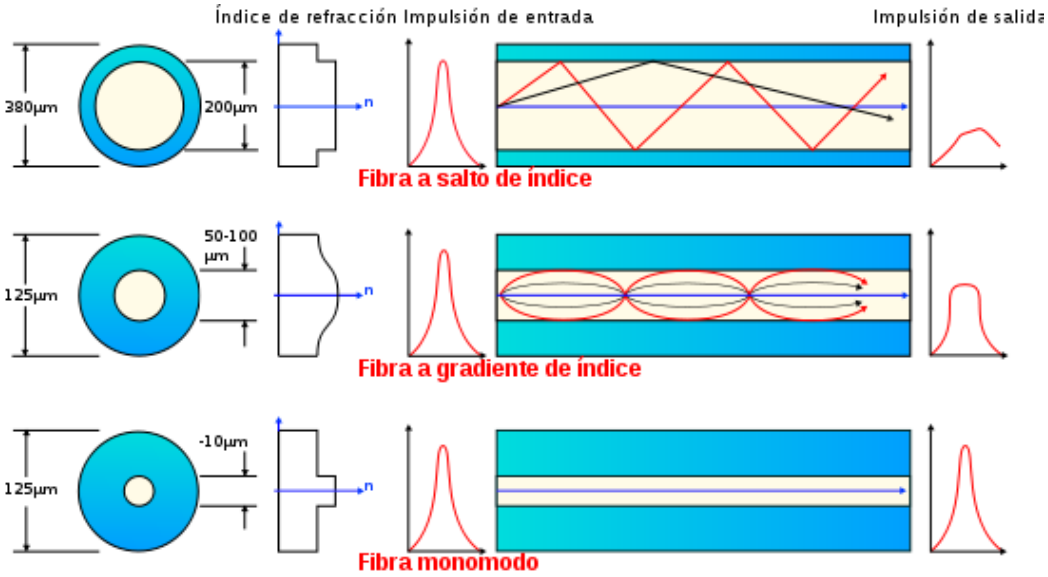


Figura 2.3 Tipos de Fibra

La transmisión de fibra óptica es unidireccional. Actualmente se utilizan velocidades de transmisión de 50, 100 y 200 Mbps, pero experimentalmente se han transmitido hasta Gbps sobre una distancia de 110 Km.

MODULO 3

REDES DE DATOS Y TECNOLOGÍAS DE TRANSPORTE

MODULO 3: REDES DE DATOS Y TECNOLOGÍAS DE TRANSPORTE

El desarrollo de la computación y su integración con las redes de datos han propiciado el surgimiento de nuevas formas de comunicación, que son aceptadas cada vez por más personas. El desarrollo de las redes informáticas posibilito su conexión mtua y, finalmente, la existencia de Internet, una red de redes gracias a la cual una computadora puede intercambiar fácilmente información con otras situadas en regiones lejanas del planeta.

La información a la que se accede a través de Internet combina el texto con la imagen y el sonido, es decir, se trata de una información multimedia, una forma de comunicación que esta teniendo un enorme desarrollo gracias a la generalización de computadores personales dotadas del hardware y software necesarios.

El uso creciente de la tecnología de la información en la actividad económica ha dado lugar a un incremento sustancial en el número de puestos de trabajo informatizados, con una relación de terminales por empleado que aumenta constantemente en todos los sectores industriales.

El crecimiento de las redes locales a mediados de los años ochenta hizo que cambiase nuestra forma de comunicarnos con los ordenadores y la forma en que los ordenadores se comunicaban entre sí.

La importancia de las LAN reside en que en un principio se puede conectar un número pequeño de ordenadores que puede ser ampliado a medida que crecen las necesidades. Son de vital importancia para empresas pequeñas puesto que suponen la solución a un entorno distribuido.

3.1 Concepto de Red

Una red es un conjunto de dispositivos de cómputo interconectados entre sí, que permite a los usuarios comunicarse, compartir información y recursos.

Las redes se componen de los siguientes elementos:

- Servidores
- Estaciones de trabajo o Terminales
- Nodos de Comunicación
- Medios de Transmisión

3.2 Topologías

La topología se refiere a la forma en que están interconectados los distintos equipos (nodos) de una red. Un nodo es un dispositivo activo conectado a la red, como un ordenador o una impresora. Un nodo también puede ser dispositivo o equipo de la red como un concentrador, conmutador o un router.[2]

3.2.1 Anillo

Tipo de LAN en la que los ordenadores o nodos están enlazados formando un círculo a través de un mismo cable. Las señales circulan en un solo sentido por el círculo, regenerándose en cada nodo. En la práctica, la mayoría de las topologías lógicas en anillo son en realidad una topología física en estrella.

3.2.2 Bus

Una topología de bus consiste en que los nodos se unen en serie con cada nodo conectado a un cable largo o bus, formando un único segmento A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo. Una rotura en cualquier parte del cable causará, normalmente, que el segmento entero pase a ser inoperable hasta que la rotura sea reparada. Como ejemplos de topología de bus tenemos 10BASE-2 y 10BASE-5.

3.2.3 Estrella

Lo más usual en ésta topología es que en un extremo del segmento se sitúe un nodo y el otro extremo se termine en una situación central con un concentrador. La principal

2 William Stallings *Comunicaciones Y Redes De Computadoras* Prentice Hall, p. 76

ventaja de este tipo de red es la fiabilidad, dado que si uno de los segmentos tiene una rotura, afectará sólo al nodo conectado en él. Otros usuarios de los ordenadores de la red continuarán operando como si ese segmento no existiera.

3.2.4 Árbol

Topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones y cuenta con un cable principal (backbone) al que hay conectadas redes individuales en bus.

3.2.5 Red en malla

La Red en malla es una topología de red en la que cada nodo está conectado a uno o más de los otros nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos.

Si la red de malla está completamente conectada no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

3.3 Modelo OSI

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) fue el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, fue un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

Proporciona a los fabricantes estándares que aseguran mayor compatibilidad e interoperatibilidad entre distintas tecnologías de red producidas a mundialmente.[3]

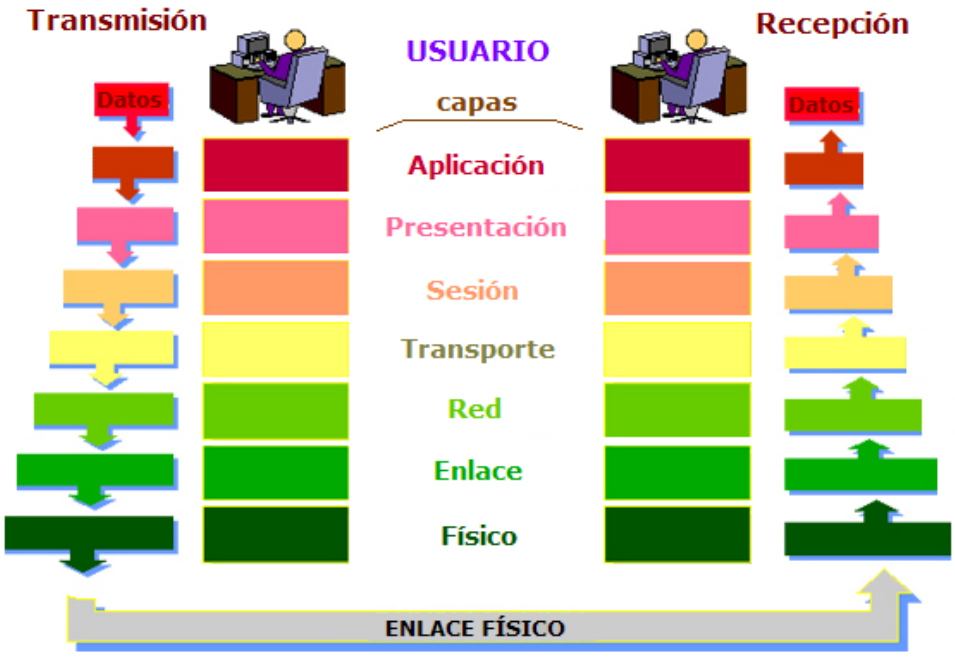


Figura 3.1 Las siete capas del modelo OSI

3.3.1 Físico

Se ocupa de la transmisión del flujo de bits a través del medio. Además se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si ésta es uni o bidireccional (símplex, dúplex o full-dúplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

3.3.2 Enlace

Divide el flujo de bits en unidades con formato (tramas) intercambiando estas unidades mediante el empleo de protocolos. Esta capa se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

3.3.3 Red

Establece las comunicaciones y determina el camino que tomarán los datos en la red. Adicionalmente la capa de red lleva un control de la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red

3 Ariganello, Ernesto / Barrientos Sevilla, *Enrique Redes Cisco Ccnp A* Ra-Ma, p. 52

(similar a un atasco en un cruce importante en una ciudad grande). La PDU (Unidad de Datos del Protocolo, por sus siglas en inglés) de la capa 3 es el paquete.

3.3.4 Transporte

La función de este nivel es asegurar que el receptor reciba exactamente la misma información que ha querido enviar el emisor, y a veces asegura al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente.

3.3.5 Sesión

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre los dos computadores que están transmitiendo datos de cualquier índole. Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado.

3.3.6 Presentación

El objetivo es encargarse de la representación de la información, de manera que los datos lleguen de manera reconocible. Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras es un traductor.

3.3.7 Aplicación

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

3.4 Modelo TCP/IP

El modelo TCP/IP, describe un conjunto de guías de diseño generales e implementaciones de protocolos de red específicos para habilitar computadora a comunicarse sobre una red. TCP/IP provee conectividad de extremo a extremo

especificando como los datos deberían estar formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. Los protocolos existen para una variedad de diferentes tipos de servicios de comunicaciones entre computadoras.[4]

Este modelo solo utiliza niveles para explicar la funcionalidad de red. Las capas son las siguientes:

3.4.1 Acceso a la red

Esta capa combina la capa física y la capa de enlaces de datos del modelo OSI. Se encarga de enrutar los datos entre dispositivos en la misma red. También maneja el intercambio de datos entre la red y otros dispositivos. Asimilable a la capa 1 (física) y 2 (enlace de datos) del modelo OSI.

3.4.2 Internet

Esta capa corresponde a la capa de red. El protocolo de Internet utiliza direcciones IP, las cuales consisten en un identificador de red y un identificador de host, para determinar la dirección del dispositivo con el que se está comunicando.

3.4.3 Transporte

Corresponde directamente a la capa de transporte del modelo OSI, y donde podemos encontrar al protocolo TCP. El protocolo TCP funciona preguntando a otro dispositivo en la red si está deseando aceptar información de un dispositivo local.

3.4.4 Aplicación

La capa 4 combina las capas de sesión, presentación y aplicación del modelo OSI. Protocolos con funciones específicas como correo o transferencia de archivos, residen en este nivel.

3.5 DSL

El DSL es una tecnología de banda ancha que permite que el ordenador reciba datos a una velocidad elevada, todo ello a través de la línea de teléfono convencional mediante la modulación de la señal de datos utilizada por el ordenador.

4 Comer, Douglas *Redes Globales de Información con Internet y TCP/ IP* Prentice Hall, p. 44

La diferencia entre ADSL y otras DSL es que la velocidad de bajada y la de subida no son simétricas, es decir, que normalmente permiten una velocidad de bajada mayor que la de subida.

3.5.1 Comparación de las técnicas xDSL

	ADSL	**HDSL**	**SDSL**	**VDSL**
Bits / segundo	De 1,5 a 9 Mbps en descendente. De 16 a 640 Kbps en ascendente	1,544 a 2,048 Mbps	1,544 a 2,048 Mbps	De 13 a 52 Mbps en descendente. De 1,5 a 2,3 Mbps en ascendente
Modo	Asimétrico	Simétrico	Simétrico	Asimétrico
Pares de cobre	1	2	1	1
Distancia (UTP de calibre 24)	De 3,7 a 5,5 km	3,7 km	3 km	1,4 km
Señalización	Analógica	Digital	Digital	Analógica
Código de Línea	CAP / DMT	2B1Q	2B1Q	DMT
Frecuencia	De 1 a 5 MHz	196 kHz	196 kHz	10 MHz
Bits / ciclo	Variable	4	4	Variable

Tabla 3.1 Comparación de Técnicas DSL

MODULO 4

INTERCONEXIONES DE REDES Y PROTOCOLOS DE ENRUTAMIENTO

MODULO 4: INTERCONEXIONES DE REDES Y PROTOCOLOS DE ENRUTAMIENTO

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean.

El objetivo de la Interconexión de Redes es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías y protocolos de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios.

Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta.

4.1 Ethernet

Ethernet es ahora la tecnología LAN dominante en el mundo. Ethernet no es una tecnología sino una familia de tecnologías LAN que se pueden entender mejor utilizando el modelo de referencia OSI.

Para que varias estaciones accedan a los medios físicos y a otros dispositivos de networking, se han inventado diversas estrategias para el control de acceso a los medios. Comprender la manera en que los dispositivos de red ganan acceso a los medios es esencial para comprender y detectar las fallas en el funcionamiento de toda la red.

La idea original de Ethernet nació del problema de permitir que dos o más host utilizaran el mismo medio y evitar que las señales interfirieran entre sí. El problema de acceso por varios usuarios a un medio compartido se estudió a principios de los 70 en la Universidad de Hawai. Se desarrolló un sistema llamado Alohanet para permitir que varias estaciones de las Islas de Hawai tuvieran acceso estructurado a la banda de

radiofrecuencia compartida en la atmósfera. Más tarde, este trabajo sentó las bases para el método de acceso a Ethernet conocido como CSMA/CD.

4.1.1 CSMA/CD

Carrier Sense Multiple Access with Collision Detection (Acceso Múltiple por Detección de Portadora con Detección de Colisiones), es una técnica usada en redes Ethernet para mejorar sus prestaciones.

En el método de acceso CSMA/CD, los dispositivos de red que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de red están ocupados o no.[5]

4.1.2 Familias

Ethernet no es una tecnología para networking, sino una familia de tecnologías para networking que incluye Legacy, Fast Ethernet y Gigabit Ethernet. Las velocidades de Ethernet pueden ser de 10, 100, 1000 ó 10000 Mbps. El formato básico de la trama y las subcapas del IEEE de las Capas OSI 1 y 2 siguen siendo los mismos para todas las formas de Ethernet.

Ethernet emplea señalización banda base, la cual utiliza todo el ancho de banda del medio de transmisión.

4.1.3 Ethernet y el modelo OSI

Ethernet opera en dos áreas del modelo OSI, la mitad inferior de la capa de enlace de datos, conocida como subcapa MAC y la capa física.

Para mover datos entre una estación Ethernet y otra, a menudo, estos pasan a través de un repetidor. Todas las demás estaciones del mismo dominio de colisión ven el tráfico que pasa a través del repetidor. Un dominio de colisión es entonces un recurso

5 Stallings, William *Comunicaciones y Redes de Computadores* Prentice Hall, p.123

compartido. Los problemas que se originan en una parte del dominio de colisión generalmente tienen impacto en todo el dominio.

Un repetidor es responsable de enviar todo el tráfico al resto de los puertos. El tráfico que el repetidor recibe nunca se envía al puerto por el cual lo recibe. Se enviará toda señal que el repetidor detecte. Si la señal se degrada por atenuación o ruido, el repetidor intenta reconstruirla y regenerarla.

Los estándares garantizan un mínimo ancho de banda y operabilidad especificando el máximo número de estaciones por segmento, la longitud máxima del mismo, el máximo número de repetidores entre estaciones, etc. Las estaciones separadas por repetidores se encuentran dentro del mismo domino de colisión. Las estaciones separadas por puentes o routers se encuentran en dominios de colisión diferentes.

Para permitir el envío local de las tramas en Ethernet, se debe contar con un sistema de direccionamiento, una forma de identificar los computadores y las interfaces de manera exclusiva. Ethernet utiliza direcciones MAC que tienen 48 bits de largo y se expresan como doce dígitos hexadecimales. Los primeros seis dígitos hexadecimales, que IEEE administra, identifican al fabricante o al vendedor. Esta porción de la dirección de MAC se conoce como Identificador Exclusivo Organizacional (OUI). Los seis dígitos hexadecimales restantes representan el número de serie de la interfaz u otro valor administrado por el proveedor mismo del equipo. Las direcciones MAC a veces se denominan direcciones grabadas (BIA) ya que estas direcciones se graban en la memoria de sólo lectura (ROM) y se copian en la memoria de acceso aleatorio (RAM) cuando se inicializa la network interface card.

En la capa MAC de enlace de datos se agregan encabezados e información final a los datos de la capa superior. El encabezado y la información final contienen información de control destinada a la capa de enlace de datos en el sistema destino. Los datos de las entidades de las capas superiores se encapsulan dentro de la trama de la capa de enlace, entre el encabezado y el cierre, para luego ser enviada sobre la red.

La NIC utiliza la dirección MAC para evaluar si el mensaje se debe pasar o no a las capas superiores del modelo OSI. La NIC realiza esta evaluación sin utilizar tiempo de procesamiento de la CPU permitiendo mejores tiempos de comunicación en una red Ethernet.

En una red Ethernet, cuando un dispositivo envía datos, puede abrir una ruta de comunicación hacia el otro dispositivo utilizando la dirección MAC destino. El dispositivo origen adjunta un encabezado con la dirección MAC del destino y envía los datos a la red. A medida que estos datos viajan a través de los medios de red, la NIC de cada dispositivo de la red verifica si su dirección MAC coincide con la dirección destino física que transporta la trama de datos. Si no hay concordancia, la NIC descarta la trama de datos. Cuando los datos llegan al nodo destino, la NIC hace una copia y pasa la trama hacia las capas superiores del modelo OSI. En una red Ethernet, todos los nodos deben examinar el encabezado MAC aunque los nodos que están comunicando estén lado a lado. Todos los dispositivos conectados a la LAN de Ethernet tienen interfaces con dirección MAC incluidas las estaciones de trabajo, impresoras, routers y switches.

4.1.4 Entramado de la Capa 2

Las corrientes de bits codificadas (datos) en medios físicos representan un logro tecnológico extraordinario, pero por sí solas no bastan para que las comunicaciones puedan llevarse a cabo. El entramado ayuda a obtener información esencial que, de otro modo, no se podría obtener solamente con las corrientes de bits codificadas:

Entre los ejemplos de dicha información se incluye:

- Cuáles son los computadores que se comunican entre sí
- Cuándo comienza y cuándo termina la comunicación entre computadores individuales
- Proporciona un método para detectar los errores que se produjeron durante la comunicación.
- Quién tiene el turno para “hablar” en una “conversación” entre computadores

El entramado es el proceso de encapsulamiento de la Capa 2. Una trama es la unidad de datos del protocolo de la Capa 2.

Hay varios tipos distintos de tramas que se describen en diversos estándares. Una trama genérica tiene secciones denominadas campos, y cada campo está formado por bytes. Los nombres de los campos son los siguientes:

- Campo de inicio de trama
- Campo de dirección
- Campos de longitud/tipo
- Campo de datos
- Campo de secuencia de verificación de trama

Cuando los computadores se conectan a un medio físico, debe existir alguna forma de informar a los otros computadores cuando están próximos a enviar una trama. Todas las tramas contienen información de denominación como, por ejemplo, el nombre del computador origen (dirección MAC) y el nombre del computador destino (dirección MAC).

La razón del envío de tramas es hacer que los datos de las capas superiores, especialmente los datos de aplicación del usuario, lleguen desde el origen hasta el destino.

Todas las tramas y los bits, bytes y campos ubicados dentro de ellas, están susceptibles a errores de distintos orígenes. El campo de Secuencia de verificación de trama (FCS) contiene un número calculado por el nodo de origen en función de los datos de la trama. Entonces, esta FCS se agrega al final de la trama que se envía. Cuando el computador destino recibe la trama, se vuelve a calcular el número FCS y se compara con el número FCS que se incluye en la trama. Si los dos números son distintos, se da por sentado que se ha producido un error, se descarta la trama y se le puede pedir al origen que vuelva a realizar la transmisión. Debido a que la fuente no puede detectar que la trama ha sido descartada, se deben iniciar retransmisiones por un protocolo de capa superior orientado a conexión que provea control de flujo de datos. Usualmente se dan retransmisiones debido a que los protocolos, como TCP/IP, requieren que las estaciones envíen tramas de reconocimiento, ACK, dentro de un tiempo preestablecido.

4.1.5 Campos de la trama de Ethernet

Algunos de los campos que se permiten o requieren en la Trama 802.3 de Ethernet son:

- Preámbulo
- Delimitador de inicio de trama.
- Dirección destino
- Dirección origen
- Longitud/Tipo
- Datos y relleno
- FCS

El Preámbulo: Es un patrón alternado de unos y ceros que se utiliza para la sincronización de los tiempos en implementaciones de 10 Mbps y menores de Ethernet. Las versiones más veloces de Ethernet son síncronas y esta información de temporización es redundante pero se retiene por cuestiones de compatibilidad.

Delimitador de Inicio de Trama: Es un campo de un octeto que marca el final de la información de temporización y contiene la secuencia de bits 10101011.

Dirección destino: Contiene la dirección destino MAC. La dirección destino puede ser unicast, multicast o de broadcast.

Dirección de origen: Contiene la dirección MAC de origen. La dirección origen generalmente es la dirección unicast del nodo de transmisión de Ethernet. Sin embargo, existe un número creciente de protocolos virtuales en uso que utilizan y a veces comparten una dirección MAC origen específica, para identificar la entidad virtual.

Longitud/Tipo: Admite dos usos diferentes. Si el valor es menor a 1536 decimal, 0×600 (hexadecimal), entonces el valor indica la longitud. La interpretación de la longitud se utiliza cuando la Capa LLC proporciona la identificación del protocolo. El valor del tipo especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento de Ethernet. La longitud indica la cantidad de bytes de datos que sigue este campo.

Campos de datos y de relleno: Pueden tener cualquier longitud, mientras que la trama no exceda el tamaño máximo permitido de trama. La unidad máxima de transmisión (MTU) para Ethernet es de 1500 octetos, de modo que los datos no deben

superar dicho tamaño. El contenido de este campo no está especificado. Se inserta un relleno no especificado inmediatamente después de los datos del usuario cuando no hay suficientes datos de usuario para que la trama cumpla con la longitud mínima especificada. Ethernet requiere que cada trama tenga entre 64 y 1518 octetos de longitud.

FCS: Contiene un valor de verificación CRC de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas. Ya que la corrupción de un solo bit en cualquier punto desde el inicio de la dirección destino hasta el extremo del campo de FCS hará que la checksum (suma de verificación) sea diferente, la cobertura de la FCS se auto-incluye. No es posible distinguir la corrupción de la FCS en sí y la corrupción de cualquier campo previo que se utilizó en el cálculo.

4.1.6 Control de acceso al medio (MAC)

MAC se refiere a los protocolos que determinan cuál de los computadores de un entorno de medios compartidos (dominio de colisión) puede transmitir los datos. La subcapa MAC, junto con la subcapa LLC, constituyen la versión IEEE de la Capa 2 del modelo OSI. Tanto MAC como LLC son subcapas de la Capa 2. Hay dos categorías amplias de Control de acceso al medio: determinística (por turnos) y la no determinística (el que primero llega, primero se sirve).

Los protocolos MAC no determinísticos utilizan el enfoque de “el primero que llega, el primero que se sirve”. CSMA/CD es un sistema sencillo. La NIC espera la ausencia de señal en el medio y comienza a transmitir. Si dos nodos transmiten al mismo tiempo, se produce una colisión y ningún nodo podrá transmitir.

4.1.7 Reglas de MAC y Manejo de los errores

Ethernet es una tecnología de broadcast de medios compartidos. El método de acceso CSMA/CD que se usa en Ethernet ejecuta tres funciones:

- Transmitir y recibir paquetes de datos

- Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI
- Detectar errores dentro de los paquetes de datos o en la red

En el método de acceso CSMA/CD, los dispositivos de networking que tienen datos para transmitir funcionan en el modo “escuchar antes de transmitir”. Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de networking están ocupados. Si el nodo determina que la red está ocupada, el nodo esperará un tiempo determinado al azar antes de reintentar. Si el nodo determina que el medio de networking no está ocupado, comenzará a transmitir y a escuchar. El nodo escucha para asegurarse que ninguna otra estación transmita al mismo tiempo. Una vez que ha terminado de transmitir los datos, el dispositivo vuelve al modo de escuchar.

Los dispositivos de networking detectan que se ha producido una colisión cuando aumenta la amplitud de la señal en los medios de networking.

Cuando se produce una colisión, cada nodo que se encuentra en transmisión continúa transmitiendo por poco tiempo a fin de asegurar que todos los dispositivos detecten la colisión. Una vez que todos los dispositivos la han detectado, se invoca el algoritmo de postergación y la transmisión se interrumpe. Los nodos interrumpen la transmisión por un período determinado al azar, que es diferente para cada dispositivo. Cuando caduca el período de retardo cada nodo puede intentar ganar acceso al medio de networking. Los dispositivos involucrados en la colisión no tienen prioridad para transmitir datos.

El estado de error más común en redes Ethernet son las colisiones. Las colisiones son el mecanismo para resolver la contención del acceso a la red. Unas pocas colisiones proporcionan una forma simple y sin problemas, que usa pocos recursos, para que los nodos de la red arbitren la contención para el recurso de red. Cuando la contención de la red se vuelve demasiado grave, las colisiones se convierten en un impedimento significativo para la operación útil de la red.

Las colisiones producen una pérdida del ancho de banda de la red equivalente a la transmisión inicial y a la señal de congestión de la colisión. Esto es una demora en el consumo y afecta a todos los nodos de la red causando posiblemente una significativa reducción en su rendimiento.

4.2 HUB

Un hub es un elemento de hardware que permite concentrar el tráfico de red que proviene de múltiples hosts y regenerar la señal. El concentrador es una entidad que cuenta con determinada cantidad de puertos. Su único objetivo es recuperar los datos binarios que ingresan a un puerto y enviarlos a los demás puertos. Al igual que un repetidor, el concentrador funciona en el nivel 1 del modelo OSI.

Dentro del modelo OSI el concentrador opera a nivel de la capa física, al igual que los repetidores, y puede ser implementado utilizando únicamente tecnología analógica. Simplemente une conexiones y no altera las tramas que le llegan.
Visto lo anterior podemos sacar las siguientes conclusiones:

- El concentrador envía información a ordenadores que no están interesados. A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el concentrador envía la información a todos los ordenadores que están conectados a él, así seguro que acierta.

- Este tráfico añadido genera más probabilidades de colisión. Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea con otro ordenador que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.

- Un concentrador funciona a la velocidad del dispositivo más lento de la red. Si observamos cómo funciona vemos que el concentrador no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 Mb/s le trasmitiera a otro de 10 Mb/s algo se perdería del mensaje. En el caso del ADSL los routers suelen funcionar a 10 Mb/s, si lo conectamos a nuestra red casera, toda la red funcionará a 10 Mb/s, aunque nuestras tarjetas sean 10/100 Mb/s.

- Un concentrador es un dispositivo simple, esto influye en dos características. El precio es barato. Añade retardos derivados de la transmisión del paquete a todos los equipos de la red (incluyendo los que no son destinatarios del mismo).

4.3 Switch

Switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).

Los puentes (bridges) y conmutadores (switches) pueden conectarse unos a los otros pero siempre hay que hacerlo de forma que exista un único camino entre dos puntos de la red. En caso de no seguir esta regla, se forma un bucle o loop en la red, que produce la transmisión infinita de tramas de un segmento al otro. Generalmente estos dispositivos utilizan el algoritmo de spanning tree para evitar bucles, haciendo la transmisión de datos de forma segura.

4.3.1 Funcionamiento de los conmutadores

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo vaya desde el puerto origen al puerto de destino. En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por lo tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

4.3.2 Bucles de red e inundaciones de tráfico

Uno de los puntos críticos de estos equipos son los bucles (ciclos) que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto

de conmutadores. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten alcanzar el equipo. Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones.

4.3.3 Switches de Capa 2 o Layer 2 Switches

Son los switches tradicionales, que funcionan como puentes multi-puertos. Su principal finalidad es dividir una LAN en múltiples dominios de colisión, o en los casos de las redes en anillo, segmentar la LAN en diversos anillos. Basan su decisión de envío en la dirección MAC destino que contiene cada trama.
Los switches de nivel 2 posibilitan múltiples transmisiones simultáneas sin interferir en otras sub-redes. Los switches de capa 2 no consiguen, sin embargo, filtrar difusiones o broadcasts, multicasts (en el caso en que más de una sub-red contenga las estaciones pertenecientes al grupo multicast de destino), ni tramas cuyo destino aún no haya sido incluido en la tabla de direccionamiento.

4.3.4 Switches de Capa 3 o Layer 3 Switches

Son los switches que, además de las funciones tradicionales de la capa 2, incorporan algunas funciones de enrutamiento o routing, como por ejemplo la determinación del camino basado en informaciones de capa de red, validación de la integridad del cableado de la capa 3 por checksum y soporte a los protocolos de routing tradicionales (RIP, OSPF, etc).

Los switches de capa 3 soportan también la definición de redes virtuales (VLAN's), y según modelos posibilitan la comunicación entre las diversas VLAN's sin la necesidad de utilizar un router externo.

Por permitir la unión de segmentos de diferentes dominios de difusión o broadcast, los switches de capa 3 son particularmente recomendados para la segmentación de redes LAN muy grandes, donde la simple utilización de switches de capa 2 provocaría una

pérdida de rendimiento y eficiencia de la LAN, debido a la cantidad excesiva de broadcasts.

Se puede afirmar que la implementación típica de un switch de capa 3 es más escalable que un router, pues éste último utiliza las técnicas de enrutamiento a nivel 3 y encaminamiento a nivel 2 como complementos, mientras que los switches sobreponen la función de enrutamiento encima del encaminamiento, aplicando el primero donde sea necesario.

4.3.5 Dominios de broadcast

Un dominio de broadcast es un grupo de dominios de colisión conectados por dos dispositivos de Capa 2. Dividir una LAN en varios dominios de colisión aumenta la posibilidad de que cada host de la red tenga acceso a los medios. Efectivamente, esto reduce la posibilidad de colisiones y aumenta el ancho de banda disponible para cada host. Pero los dispositivos de Capa 2 envían broadcasts, y si son excesivos, pueden reducir la eficiencia de toda la LAN. Los broadcasts deben controlarse en la Capa 3, ya que los dispositivos de Capa 1 y Capa 2 no pueden hacerlo. El tamaño total del dominio del broadcast puede identificarse al observar todos los dominios de colisión que procesan la misma trama de broadcast. En otras palabras, todos los nodos que forman parte de ese segmento de red delimitados por un dispositivo de Capa 3. Los dominios de broadcast están controlados en la Capa 3 porque los routers no envían broadcasts. Los routers, en realidad, funcionan en las Capas 1, 2 y 3. Ellos, al igual que los dispositivos de Capa 1, poseen una conexión física y transmiten datos a los medios. Ellos tienen una encapsulamiento de Capa 2 en todas las interfaces y se comportan como cualquier otro dispositivo de Capa 2. Es la Capa 3 la que permite que el router segmente dominios de broadcast.

Para que un paquete sea enviado a través del router, el dispositivo de Capa 2 debe ya haberlo procesado y la información de la trama debe haber sido eliminada. El envío de Capa 3 se basa en la dirección IP destino y no en la dirección MAC. Para que un paquete pueda enviarse, debe contener una dirección IP que esté por afuera del alcance de las direcciones asignadas a la LAN, y el router debe tener un destino al cual enviar el paquete específico en su tabla de enrutamiento.

4.4 Ruteador

Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Los enrutadores pueden proporcionar conectividad dentro de las empresas, entre las empresas e Internet, y en el interior de proveedores de servicios de Internet (ISP). Los enrutadores más grandes (por ejemplo, el CRS-1 de Cisco o el Juniper T1600) interconectan ISPs, se utilizan dentro de los ISPs, o pueden ser utilizados en grandes redes de empresas.

Todos los tamaños de enrutadores se pueden encontrar dentro de las empresas. Si bien los más poderosos tienden a ser encontrados en ISPs, instalaciones académicas y de investigación, las grandes empresas pueden necesitarlos grandes.

Las funciones primarias de un ruteador son:

- Segmentar la red dentro de dominios individuales de broadcast.
- Suministrar un envío inteligente de paquetes.
- Soportar rutas redundantes en la red.
- Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del ruteador es una subred separada, el tráfico de los broadcast no pasaran a través del ruteador.
- Proporcionar seguridad a través de sofisticados filtros de paquetes, en ambiente LAN y WAN.
- Permitir diseñar redes jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.
- Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, Fast Ethernet, Token Ring, FDDI y ATM.
- Se ajustan en tiempo real a las circunstancias cambiantes de la red.
- Si hay cambios en la red, entonces:
    - o Recalculan rutas.
    - o Actualizan tablas de ruteo.
    - o Envían esta información a sus vecinos.

4.5 DIRECCIONAMIENTO IP

Ip constituye el protocolo de direccionamiento de la suite de protocolos TCP/IP. Su función esta orientada a proveer direccionamiento en el nivel red e identificación de redes y host. IP es la base para el enrutamiento de los datagramas, da una identificación global y única de los elementos de la red. Algunas características del direccionamiento IP son:

- El tráfico es enrutado a través de la red basado en una dirección, en vez de un nombre.
- Cada compañía ubicada en la red es vista como una red única con una dirección única
- La escogencia de la ruta se basa en la ubicación.
- La ubicación es representada por una dirección.

Las direcciones IP tienen una longitud de 32 bits y constan de dos partes: La dirección de Red y la dirección de Host. Pero a la vez la dirección está divida en 4 octetos (grupos de ocho bits), representados por un número decimal de 0 a 255 separados por un punto.

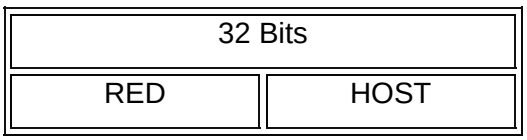


Figura 4.1 Partes de una dirección IP

4.5.1 Dirección de Red

En la parte de la dirección IP destinada para asignar la dirección de la red a la cual pertenece el host. El enrutamiento se basa en saber como conocer el camino hacia cada una de estas redes, sea Lan o Wan.

4.5.2 Dirección de Host

La dirección de host se utiliza para diferenciar (al nivel de red de la capa OSI y TCP/IP), cada elemento de la red que posea una dirección MAC dentro del segmento de red. Este juego de palabras, se traduce diciendo “todos los elementos de la red,

poseen una dirección que los identifica de los demás de la misma red, llamada dirección de host". Los PC, servidores, switch, routers, entre otros, son ejemplos de host, y por tanto deben ser direccionados. En otras palabras, todo equipo que necesite enviar y recibir datagramas o paquetes IP, se debe diferenciar con una dirección de host y debe ser ubicado en un segmento de red IP.

Para que dos sistemas se comuniquen, se deben poder identificar y localizar entre sí. Aunque las direcciones de la Figura 4.2 no son direcciones de red reales, representan el concepto de agrupamiento de las direcciones.

Este utiliza A o B para identificar la red y la secuencia de números para identificar el host individual.

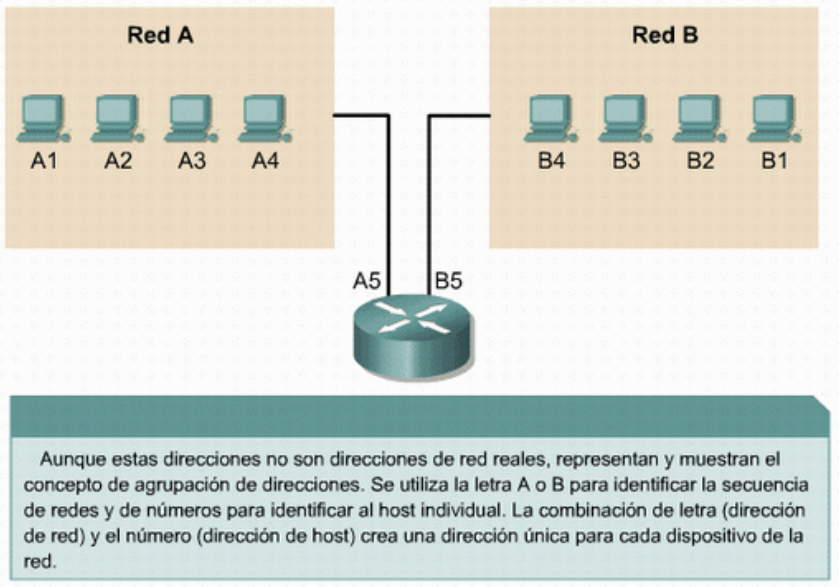


Figura 4.2 Agrupamiento de las direcciones

Un computador puede estar conectado a más de una red. En este caso, se le debe asignar al sistema más de una dirección. Cada dirección identificará la conexión del computador a una red diferente. No se suele decir que un dispositivo tiene una dirección sino que cada uno de los puntos de conexión (o interfaces) de dicho dispositivo tiene una dirección en una red. Esto permite que otros computadores localicen el dispositivo en una determinada red.

La combinación de letras (dirección de red) y el número (dirección del host) crean una dirección única para cada dispositivo conectado a la red. Cada computador conectado a una red TCP/IP debe recibir un identificador exclusivo o una dirección IP. Esta

dirección, que opera en la Capa 3, permite que un computador localice otro computador en la red.

Todos los computadores también cuentan con una dirección física exclusiva, conocida como dirección MAC. Estas son asignadas por el fabricante de la tarjeta de interfaz de la red. Las direcciones MAC operan en la Capa 2 del modelo OSI.

4.5.3 Clase A

Asigna el primer octeto (8 bits) para direccionar redes y los tres octetos restantes (24 bits) para host. Con este esquema se pueden direccionar hasta 16.777.214 host y 126 redes. El rango que comprende estas direcciones es 10.0.0.0 a 126.0.0.0.

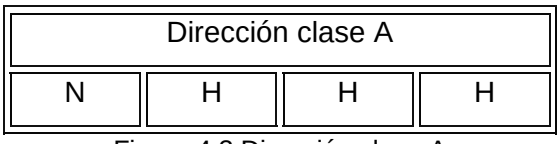


Figura 4.3 Dirección clase A

Esta clase, por las pocas direcciones de red que maneja, es bastante utilizada en redes Lan, donde generalmente se tienen pocas redes pero gran cantidad de host.

4.5.4 Clase B

Esta clase asigna equitativamente Los bits para red y host. 16 bits para redes y 16 bits para host. Bajo este esquema se pueden direccionar 65.534 host y 16.256 redes. El rango para clase B es el siguiente: 128.1.0.0 a 191.254.0.0. Esta clase es una de las más utilizadas para Internet, por su capacidad de direccionar gran cantidad de redes.

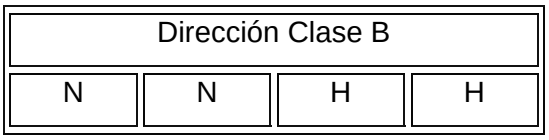


Figura 4.4 Dirección clase B

4.5.5 Clase C

Esta clase funciona en la distribución de bits, en forma contraria a la clase A, separa los primeros 24 bits para red y los 8 restantes para host. Con este esquema se tienen 2.072.640 redes y 254 host por cada red. El rango para esta clase es desde 192.0.1.0 a 223.255.255.0.

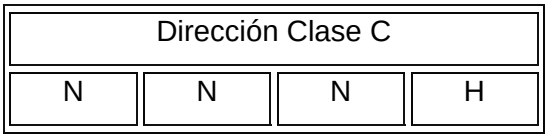


Figura 4.5 Dirección clase C

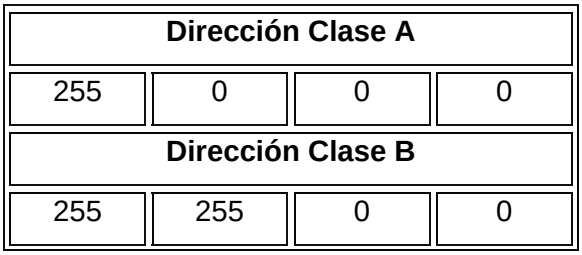
Estas clases no son de dominio público. Su utilización está restringida a entidades privadas de investigación. Clase D es para multicasting (servicios de difusión múltiple de datos), su rango está entre 224.0.0.0 y 239.255.255.254. La clase E es de investigación.

Clase	Rango	N° de Redes	N° de Host	Máscara de Red	Broadcast ID
A	1.0.0.0 - 127.255.255.255	126	16.777.214	255.0.0.0	x.255.255.255
B	128.0.0.0 - 191.255.255.255	16.382	65.534	255.255.0.0	x.x.255.255
C	192.0.0.0 - 223.255.255.255	2.097.150	254	255.255.255.0	x.x.x.255
D	224.0.0.0 - 239.255.255.255				
E	240.0.0.0 - 255.255.255.255				

Tabla 4.1 Clases de direcciones

4.5.6 Máscara de Red

Sirve para identificar la red a la cual pertenece una dirección IP. Una operación lógica binaria AND entre la dirección IP y la máscara dará como resultado el valor de la red. En la máscara se utiliza “1s” para diferenciar redes y “Os” para identificar host. Las siguientes son las máscaras para las direcciones clase A, B. y C.



Dirección Clase C			
255	255	255	0

Figura 4.6 Mascaras para clases A, B y C

4.5.7 División en Subredes

La división en subredes es otro método para administrar las direcciones IP. Este método, que consiste en dividir las clases de direcciones de red completas en partes de menor tamaño, ha evitado el completo agotamiento de las direcciones IP.

Resulta imposible hablar sobre el TCP/IP sin mencionar la división en subredes. Como administrador de sistemas, es importante comprender que la división en subredes constituye un medio para dividir e identificar las redes individuales en toda la LAN. No siempre es necesario subdividir una red pequeña. Sin embargo, en el caso de redes grandes a muy grandes, la división en subredes es necesaria.

Dividir una red en subredes significa utilizar una máscara de subred para dividir la red y convertir una gran red en segmentos más pequeños, más eficientes y administrables o subredes.

El administrador del sistema debe resolver estos problemas al agregar y expandir la red. Es importante saber cuántas subredes o redes son necesarias y cuántos hosts se requerirán en cada red. Con la división en subredes, la red no está limitada a las máscaras de red por defecto Clase A, B o C y se da una mayor flexibilidad en el diseño de la red.

Las direcciones de subredes incluyen la porción de red más el campo de subred y el campo de host. El campo de subred y el campo de host se crean a partir de la porción de host original de la red entera. La capacidad para decidir cómo se divide la porción de host original en los nuevos campos de subred y de host ofrece flexibilidad en el direccionamiento al administrador de red.

Para crear una dirección de subred, un administrador de red pide prestados bits del campo de host y los designa como campo de subred.

Notación decimal para el primer octeto de host	Número de subredes	Número de Hosts de clase A por subred	Número de Hosts de clase B por subred	Número de Hosts de clase C por subred
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

Tabla 4.2 División de Subredes

El número mínimo de bits que se puede pedir es dos. Al crear una subred, donde se solicita un sólo bit, el número de la red suele ser red .0. El número de broadcast entonces sería la red .255. El número máximo de bits que se puede pedir prestado puede ser cualquier número que deje por lo menos 2 bits restantes para el número de host.

4.5.8 ARP y RARP

El protocolo **ARP (**Address Resolution Protocol), permite que se conozca la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP.
Cada equipo conectado a la red tiene un número de identificación de 48 bits. Éste es un número único establecido en la fábrica en el momento de fabricación de la tarjeta. Sin embargo, la comunicación en Internet no utiliza directamente este número (ya que las direcciones de los equipos deberían cambiarse cada vez que se cambia la tarjeta de interfaz de red), sino que utiliza una dirección lógica asignada por un organismo: la dirección IP.

Para que las direcciones físicas se puedan conectar con las direcciones lógicas, el protocolo ARP interroga a los equipos de la red para averiguar sus direcciones físicas y luego crea una tabla de búsqueda entre las direcciones lógicas y físicas en una memoria caché.

Cuando un equipo debe comunicarse con otro, consulta la tabla de búsqueda. Si la dirección requerida no se encuentra en la tabla, el protocolo ARP envía una solicitud a la red. Todos los equipos en la red comparan esta dirección lógica con la suya. Si alguno de ellos se identifica con esta dirección, el equipo responderá al ARP, que

almacenará el par de direcciones en la tabla de búsqueda, y, a continuación, podrá establecerse la comunicación.

El protocolo RARP (Reverse Address Resolution Protocol) es mucho menos utilizado. Es un tipo de directorio inverso de direcciones lógicas y físicas. Este protocolo se usa esencialmente para las estaciones de trabajo sin discos duros que desean conocer su dirección física.

El protocolo RARP le permite a la estación de trabajo averiguar su dirección IP desde una tabla de búsqueda entre las direcciones MAC (direcciones físicas) y las direcciones IP alojadas por una pasarela ubicada en la misma red de área local (LAN). Para poder hacerlo, el administrador debe definir los parámetros de la pasarela (router) con la tabla de búsqueda para las direcciones MAC/IP. A diferencia del ARP, este protocolo es estático. Por lo que la tabla de búsqueda debe estar siempre actualizada para permitir la conexión de nuevas tarjetas de interfaz de red.

4.6 Enrutamiento

El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino. Un router toma decisiones en función de la dirección IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino.

4.6.1 Protocolo De Enrutamiento

Un protocolo de enrutamiento es el que define el esquema de comunicación entre routers. Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers. La información que un router obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento.[6]

6 Ariganello, Ernesto *Técnicas De Configuración De Routers* Cisco ra-Ma Editorial, p. 29

4.6.2 Tipos de protocolo

Los protocolos se pueden dividir según varios criterios. Pero antes se dará una breve explicación de lo que representan una ruta estática y una ruta dinámica.

- Una ruta estática es una ruta programada que el administrador de red introduce manualmente en el router.
- Una ruta dinámica utiliza una ruta que un protocolo de enrutamiento de red ajusta automáticamente ante los cambios en la topología de la red sin más intervención del administrador.

Las rutas estáticas se deben introducir una a una para obtener la tabla final de enrutamiento mientras que con las rutas dinámicas obtenemos automáticamente dicha tabla de enrutamiento.

4.6.3 Rutas Estáticas

Las operaciones con rutas estáticas pueden dividirse en tres partes, como sigue:

- El administrador de la red configura la ruta
- El router instala la ruta en la tabla de enrutamiento
- Los paquetes se enrutan de acuerdo a la ruta estática

Para definir una ruta estática deberemos conocer el rango de IPs de la red de destino, la máscara de subred de dicha red de destino, la puerta de enlace que generalmente es la dirección IP del salto siguiente es decir el router siguiente y como parámetro opcional la distancia administrativa que nos puede servir para dar mayor prioridad a una ruta que a otra.

Dicho tipo de ruta se utiliza en redes muy pequeñas ya que el coste de administración de la red es muy elevado. Además resulta más complicado enfrentarse a una falla de red ya que deberemos modificar todas las tablas de enrutamiento a mano.

4.6.4 Rutas Dinámicas

En la determinación de rutas dinámicas interviene el concepto fundamental de protocolo de enrutamiento. Definir las rutas dinámicas es definir los distintos protocolos de enrutamiento existentes.

Ventajas del enrutamiento dinámico

- En casos de fallas en las rutas preferidas ofrece rutas opcionales que convierte en preferentes mientras no se repare la falla.
- Se puede compartir la carga indicando una preferencia por ciertas rutas (balanceo).

Para poder definir los tipos de protocolos de enrutamiento tendremos en cuenta los distintos tipos de algoritmos que utilizan:

- Algoritmo de vector-distancia (Bellman Ford)
- Algoritmo de estado enlace (OSPF)

El enrutamiento por vector-distancia determina la dirección (vector) y la distancia hacia cualquier destino de la red. El enrutamiento de estado enlace utiliza su algoritmo para redibujar totalmente la topología de la red para así determinar la mejor ruta.

4.6.5 Protocolos de vector-distancia

Los protocolos de enrutamiento por vector-distancia envían copias periódicas de las tablas de enrutamiento de un router a otro siempre que estos estén directamente conectados. Estas actualizaciones periódicas entre routers informan de los cambios de topología. Los algoritmos de enrutamiento basados en el vector-distancia también se conocen como algoritmos Bellman-Ford.

El algoritmo finalmente acumula información acerca de las distancias de la red, la cual le permite mantener una base de datos de la topología de la red. Sin embargo, los algoritmos de vector-distancia no permiten que un router conozca la topología exacta de una red, ya que cada router solo ve a sus routers vecinos.

Las tablas de enrutamiento incluyen información acerca del costo total de la ruta (definido por su métrica) y la dirección lógica del primer router en la ruta hacia cada una de las redes indicadas en la tabla.

4.6.6 Protocolos de estado enlace

Los algoritmos de estado de enlace también se conocen como algoritmos Dijkstra o SPF ("primero la ruta más corta"). Los protocolos de enrutamiento de estado del enlace mantienen una base de datos compleja, con la información de la topología de la red. El algoritmo de enrutamiento de estado del enlace mantiene información completa sobre routers lejanos y su interconexión.

El enrutamiento de estado enlace utiliza:

- Publicaciones de estado del enlace (LSA): una publicación del estado del enlace es un paquete pequeño de información sobre el enrutamiento, el cual es enviado de router a router.
- Base de datos topológica: una base de datos topológica es un cúmulo de información que se ha reunido mediante las LSA.
- Algoritmo SPF: el algoritmo "primero la ruta más corta" (SPF) realiza cálculos en la base de datos, y el resultado es el árbol SPF.
- Tablas de enrutamiento: una lista de las rutas e interfaces conocidas.

Para llegar a la convergencia de la red es decir al descubrimiento de la red, los protocolos de estado enlace siguen los siguientes pasos:

- Inicio intercambio LSAs entre routers
- El Algoritmo SPF determina la conectividad de la red
- Generación de la tabla de enrutamiento
- Cuando hay un cambio en la topología el primer router que lo conoce envía la nueva información al resto de routers
- El router vuelve a generar la tabla de enrutamiento

4.6.7 Métricas

Cuando un protocolo de enrutamiento aprende sobre mas de una ruta para llegar a un mismo destino, debe poder diferenciar cual es la más conveniente para llegar a ese destino. Una métrica es una forma de evaluar cual ruta es la más conveniente basándose en uno o varios parámetros. Cada protocolo de enrutamiento usa su propia métrica.

Por ejemplo, RIP usa el conteo de saltos, EIGRP usa una combinación de ancho de banda y retardo, y la implementación de OSPF de Cisco usa el ancho de banda.

La métrica puede variar entre protocolos y no son comparables, esto implica que dos protocolos pueden elegir dos rutas DISTINTAS hacia el mismo destino. Por ejemplo RIP elegirá la ruta que implique menos “saltos” entre routers, mientras que OSPF elegirá aquella que presente el mayor ancho de banda aún cuando esta ruta lleve más saltos.

Dependiendo del protocolo utilizado, se puede evaluar con los siguientes parámetros.

- RIP: conteo de saltos, menor es mejor.
- IGRP e EIGRP: evalúa ancho de banda, retardo, confiabilidad y carga, se elige como mejor ruta la que se evalué con el resultado más bajo.
- OSPF: costo, la mejor ruta es la del costo mas bajo. La implementación de cisco evalúa ancho de banda.

4.6.8 Distancias administrativas

Un router puede aprender una ruta hacia la misma red/mascara de subred de varias formas, por ejemplo puede haber configurada una ruta estática y además puede aprender dinámicamente la misma ruta para llegar a esa red mediante un protocolo de enrutamiento. El router debe elegir una de las dos rutas para colocarla en la tabla.

En algunas redes puede ser necesario implementar más de un protocolo de enrutamiento, entonces un router puede aprender sobre una red haciendo uso de más de un protocolo de enrutamiento. Las distancias administrativas son una forma de dar

prioridad cuando hay información sobre una red proveniente de más de un origen de enrutamiento (protocolo).

La distancia administrativa define la preferencia de un origen de enrutamiento. A cada origen se le asigna un orden de preferencia, incluidas rutas estáticas y redes directamente conectadas.

4.6.9 IGPS Y EGPS

Para poder realizar la clasificación siguientes, debemos tener claro qué representa un sistema autónomo. Definimos un sistema autónomo (AS) como el conjunto de redes bajo una administración común, las cuales comparten una estrategia de enrutamiento común. Para el mundo exterior, el AS es una entidad única. El AS puede ser administrado por uno o más operadores, a la vez que presenta un esquema unificado de enrutamiento hacia el mundo exterior.

Los números de identificación de cada AS son asignados por el Registro Estadounidense de Números de Internet (ARIN), los proveedores de servicios o el administrador de la red. Este sistema autónomo es un número de 16 bits.

Esencialmente un AS nos permite aislar el tipo de enrutamiento elegido (rutas estáticas o protocolos de enrutamiento para rutas dinámicas) del enrutamiento utilizado fuera de nuestra red. Esta forma de separación es la elegida para hacer posible que distintas redes de varias organizaciones puedan entenderse entre si.

Por lo tanto teniendo siempre presente la definición de sistema autónomo podemos definir los protocolos de puerta de enlace interior (IGP) y los protocolos de puerta de enlace exterior (EGP).

Un IGP se puede definir como protocolo de enrutamiento interior diseñado para ser usado en redes cuyos segmentos se encuentran bajo el control de una sola organización. Los criterios de diseño de los protocolos de enrutamiento interior requieren que el protocolo encuentre la mejor ruta a través de la red. En otras palabras, la métrica y la forma en que esta se utiliza es el elemento más importante de un protocolo de enrutamiento interior.

Un EGP está diseñado para ser usado entre dos redes diferentes, las cuales se encuentran bajo el control de dos organizaciones diferentes. EGP es un protocolo estándar usado para intercambiar información de enrutamiento entre sistemas autónomos.

En general, se utilizan entre ISPs o entre una compañía y un ISP.

Los protocolos de enrutamiento exterior necesitan de estos tres conjuntos de información antes de comenzar su operación:

- Una lista de los routers vecinos, con los que intercambiarán la información de enrutamiento.
- Una lista de las redes a ser publicadas como de acceso directo.
- El número de sistema autónomo del router local.

4.6.10 RIP

Routing Information Protocol es un protocolo de vector-distancia. Evita que los bucles de enrutamiento se prolonguen de forma indefinida, mediante la fijación de un límite en el número de saltos permitidos en una ruta, desde su origen hasta su destino. El número máximo de saltos permitido en una ruta es de 15. Cuando un router recibe una actualización de enrutamiento que contiene una entrada nueva o cambiada, el valor de la métrica aumenta en 1, para incluir el salto correspondiente a sí mismo. Si este aumento hace que la métrica supere la cifra de 15, se considera que es infinita y la red de destino se considera fuera de alcance. RIP incluye diversas características las cuales están presentes en otros protocolos de enrutamiento. Por ejemplo, RIP implementa los mecanismos de espera y horizonte dividido para prevenir la propagación de información de enrutamiento errónea. RIP actualiza sus tablas de enrutamiento enviando la información de sus tablas de enrutamiento cada 30 segundos a los routers adyacentes.

4.6.11 IGRP

IGRP es un protocolo de enrutamiento de vector-distancia desarrollado por Cisco. Envía actualizaciones de enrutamiento a intervalos de 90 segundos, las cuales

publican las redes de un sistema autónomo en particular. Las características claves de IGRP son las siguientes:

- La versatilidad para manejar automáticamente topologías indefinidas y complejas.
- La flexibilidad necesaria para segmentarse con distintas características de ancho de banda y de retardo.
- La escalabilidad para operar en redes de gran tamaño.

IGRP es un protocolo de enrutamiento basado en la tecnología vector-distancia, aunque también tiene en cuenta el estado del enlace. Por defecto, el protocolo IGRP de enrutamiento usa el ancho de banda y el retardo como métrica. Además, IGRP puede configurarse para utilizar una combinación de variables para calcular una métrica compuesta. Estas variables incluyen:

- Ancho de banda
- Retardo
- Carga
- Confiabilidad

4.6.12 EIGRP

EIGRP es un protocolo de encaminamiento híbrido, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Aunque no garantiza el uso de la mejor ruta, es bastante usado porque EIGRP es algo más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP. Esto permite que una red tenga una arquitectura mejorada y pueda mantener las inversiones actuales en IGRP.

La tabla de vecinos es la más importante de EIGRP. Cada router EIGRP mantiene una tabla de vecinos que enumera a los routers adyacentes. Al conocer nuevos vecinos, se registran la dirección y la interfaz del vecino. Esta información se guarda en la estructura de datos del vecino.

Los routers EIGRP mantienen una tabla de topología por cada protocolo configurado de red. La tabla de enrutamiento mantiene las rutas que se aprenden de forma dinámica.

EIGRP es un protocolo de enrutamiento por vector-distancia avanzado, pero también actúa como protocolo del estado de enlace en la manera en que actualiza a los vecinos y mantiene la información de enrutamiento. A continuación se presentan algunas de las ventajas de EIGRP sobre los protocolos de vector-distancia simples:

EIGRP envía actualizaciones parciales y limitadas, y hace un uso eficiente del ancho de banda. EIGRP usa un ancho de banda mínimo cuando la red es estable. Los routers EIGRP no envían las tablas en su totalidad, sino que envían actualizaciones parciales e incrementales. Esto es parecido a la operación de OSPF, salvo que los routers EIGRP envían estas actualizaciones parciales sólo a los routers que necesitan la información, no a todos los routers del área. Por este motivo, se denominan actualizaciones limitadas.

4.6.13 OSPF

Open Shortest Path First es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo enlace-estado (LSA - *Link State Algorithm*) para calcular la ruta más corta posible. OSPF esta basado en estándares abiertos.

Reúne la información de los routers vecinos acerca del estado de enlace de cada router OSPF. Con esta información se inunda a todos los vecinos. Un router OSPF publica sus propios estados de enlace y traslada los estados de enlace recibidos.
Cada router del área OSPF tendrá la misma base de datos del estado de enlace. Por lo tanto, cada router tiene la misma información sobre el estado del enlace y los vecinos de cada uno de los demás routers.

Cada router luego aplica el algoritmo SPF a su propia copia de la base de datos. Este cálculo determina la mejor ruta hacia un destino. El algoritmo SPF va sumando el costo, un valor que corresponde generalmente al ancho de banda. La ruta de menor costo se agrega a la tabla de enrutamiento, que se conoce también como la base de datos de envío.

Para reducir la cantidad de intercambios de la información de enrutamiento entre los distintos vecinos de una misma red, los routers de OSPF seleccionan un router designado (DR) y un router designado de respaldo (BDR) que sirven como puntos de enfoque para el intercambio de información de enrutamiento.

Por ultimo fue desarrollado para solventar problemas de RIP, soporta topologías jerárquicas y manda los LSA cada 30 minutos

OSPF es probablemente el tipo de protocolo IGP más utilizado en grandes redes. Puede operar con seguridad usando MD5 para autentificar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado.

4.6.14 BGP

El BGP o Border Gateway Protocol es un protocolo mediante el cual se intercambian prefijos los ISP registrados en Internet. Actualmente la totalidad de los ISP intercambian sus tablas de rutas a través del protocolo BGP. Este protocolo requiere un router que tenga configurado cada uno de los vecinos que intercambiarán información de las rutas que cada uno conozca. Se trata del protocolo más utilizado para redes con intención de configurar un EGP.

El protocolo de Gateway fronterizo (BGP) es un ejemplo de protocolo de Gateway exterior (EGP). BGP intercambia información de enrutamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de loops. BGP es el protocolo principal de publicación de rutas utilizado por las compañías más importantes e ISP en la Internet. BGP4 es la primera versión de BGP que admite enrutamiento entre dominios sin clase (CIDR) y agregado de rutas. A diferencia de los protocolos de Gateway internos (IGP), como RIP, OSPF y EIGRP, BGP no usa métricas como número de saltos, ancho de banda, o retardo. En cambio, BGP toma decisiones de enrutamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP.

MODULO 5

TELEFONÍA CELULAR Y SISTEMAS DE TECNOLOGÍA PERSONAL

MODULO 5: TELEFONÍA CELULAR Y SISTEMAS DE TECNOLOGÍA PERSONAL

Las tecnologías inalámbricas han tenido mucho auge y desarrollo en estos últimos años. Una de las que ha tenido un gran desarrollo ha sido la telefonía celular.

Desde sus inicios a finales de los 70´s ha revolucionado enormemente las actividades que realizamos diariamente. Los teléfonos celulares se han convertido en una herramienta primordial para la gente común y de negocios; las hace sentir más seguras y más productivas.

A pesar de que la telefonía celular fue concebida estrictamente para la voz, la tecnología celular de hoy es capaz de brindar otro tipo de servicios, como datos, audio y video.

5.1 La primer generación 1G

La 1G de la telefonía móvil hizo su aparición en 1979, se caracterizó por ser analógica y estrictamente para voz. La calidad de los enlaces de voz era muy baja, baja velocidad, la transferencia entre celdas era muy imprecisa, tenían baja capacidad basadas en FDMA, (Frequency Divison Multiple Access) y la seguridad no existía. La tecnología predominante de esta generación es AMPS (Advanced Mobile Phone System).

AMPS (Sistema telefónico móvil avanzado): Se presentó en 1976 en Estados Unidos y fue el primer estándar de redes celulares. Utilizada principalmente en el continente americano, Rusia y Asia, la primera generación de redes analógicas contaba con mecanismos de seguridad endebles que permitían hackear las líneas telefónicas.
En esta generación el tamaño de los celulares era mayor al de hoy día; fueron originalmente diseñados para el uso en los automóviles. Motorola fue la primera compañía en introducir un teléfono realmente portátil.

5.2 La segunda generación 2G

La 2G arribó hasta 1990 y a diferencia de la primera se caracterizó por ser digital. El

sistema 2G utiliza protocolos de codificación más sofisticados. Las tecnologías predominantes son: GSM (Global System for Mobile Communications).

Los protocolos empleados en los sistemas 2G soportan velocidades de información más altas para voz pero limitados en comunicaciones de datos. Se pueden ofrecer servicios auxiliares tales como datos, fax y SMS (Short Message Service).

La primera llamada digital entre teléfonos Celulares fue realizada en Estados Unidos en 1990. En 1991 la primera red GSM fue instalada en Europa.

La generación se caracterizó por circuitos digitales de datos conmutados por circuito y la introducción de la telefonía rápida y avanzada a las redes. Usó a su vez acceso múltiple de tiempo dividido (TDMA) para permitir que hasta ocho usuarios utilizaran los canales separados por 200MHz. Los sistemas básicos usaron frecuencias de banda de 900MHz, mientras otros de 1800 y 1900MHz. Nuevas bandas de 850MHz fueron agregadas en forma posterior. Los principales estándares de telefonía móvil de G2 son: GSM, CDMA y TDMA.

Gracias a la G2, es posible transmitir voz y datos digitales de volúmenes bajos, por ejemplo, mensajes de texto (SMS siglas en inglés de Servicio de mensajes cortos) o mensajes multimedia (MMS siglas en inglés de Servicio de mensajes multimedia). El estándar GSM permite una velocidad de datos máxima de 9,6 kbps.

5.2.1 El estándar GSM

La red GSM (Sistema global de comunicaciones móviles) es, a comienzos del siglo XXI, el estándar más usado de Europa. Se denomina estándar "de segunda generación" (2G) porque, a diferencia de la primera generación de teléfonos portátiles, las comunicaciones se producen de un modo completamente digital.
En 1982, cuando fue estandarizado por primera vez, fue denominado "Groupe Spécial Mobile" y en 1991 se convirtió en un estándar internacional llamado "Sistema Global de Comunicaciones Móviles".
En Europa, el estándar GSM usa las bandas de frecuencia de 900MHz y 1800 MHz. Sin embargo, en los Estados Unidos se usa la banda de frecuencia de 1900 MHz. Por esa razón, los teléfonos portátiles que funcionan tanto en Europa como en los Estados

Unidos se llaman tribanda y aquellos que funcionan sólo en Europa se denominan bibanda.

El estándar GSM permite un rendimiento máximo de 9,6 kbps, que permite transmisiones de voz y de datos digitales de volumen bajo, por ejemplo, mensajes de texto (SMS, Servicio de mensajes cortos) o mensajes multimedia (MMS, Servicio de mensajes multimedia).

5.2.1.1 El concepto de red celular

Las redes de telefonía móvil se basan en el concepto de celdas, es decir zonas circulares que se superponen para cubrir un área geográfica.

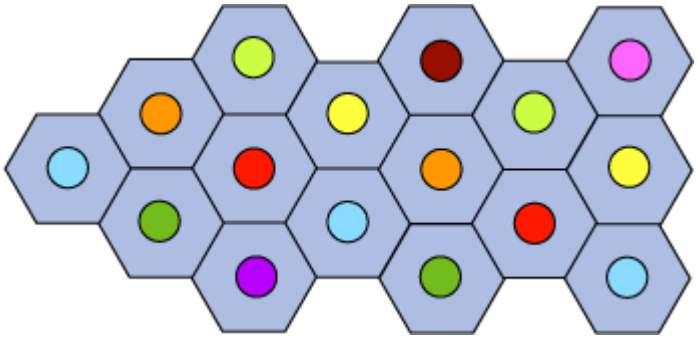


Figura 5.1 Celdas en una red celular

Las redes celulares se basan en el uso de un transmisor-receptor central en cada celda, denominado "estación base" (o Estación base transceptora, BTS).

Cuanto menor sea el radio de una celda, mayor será el ancho de banda disponible. Por lo tanto, en zonas urbanas muy pobladas, hay celdas con un radio de unos cientos de metros mientras que en zonas rurales hay celdas enormes de hasta 30 kilómetros que proporcionan cobertura.

En una red celular, cada celda está rodeada por 6 celdas contiguas (por esto las celdas generalmente se dibujan como un hexágono). Para evitar interferencia, las celdas adyacentes no pueden usar la misma frecuencia. En la práctica, dos celdas que usan el mismo rango de frecuencia deben estar separadas por una distancia equivalente a dos o tres veces el diámetro de la celda.[7]

7 Jordi Julia Sort Redes Metropolitanas = Metropolitan Networks Editorial Gustavo Gili, p. 67

5.2.1.2 Arquitectura de la red GSM

En una red GSM, la terminal del usuario se llama estación móvil. Una estación móvil está constituida por una tarjeta SIM (Módulo de identificación de abonado), que permite identificar de manera única al usuario y a la terminal móvil, o sea, al dispositivo del usuario (normalmente un teléfono portátil).

Las terminales (dispositivos) se identifican por medio de un número único de identificación de 15 dígitos denominado IMEI (Identificador internacional de equipos móviles). Cada tarjeta SIM posee un número de identificación único (y secreto) denominado IMSI (Identificador internacional de abonados móviles). Este código se puede proteger con una clave de 4 dígitos llamada código PIN.

Por lo tanto, la tarjeta SIM permite identificar a cada usuario independientemente de la terminal utilizada durante la comunicación con la estación base. Las comunicaciones entre una estación móvil y una estación base se producen a través de un vínculo de radio, por lo general denominado interfaz de aire.

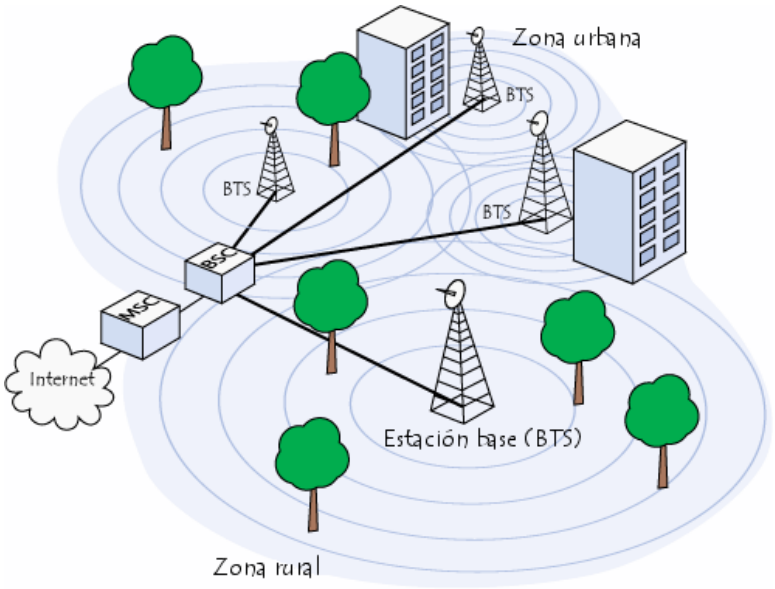


Figura 5.2 Arquitectura de la red GSM

Todas las estaciones base de una red celular están conectadas a un controlador de estaciones base (o BSC), que administra la distribución de los recursos. El sistema compuesto del controlador de estaciones base y sus estaciones base conectadas es el Subsistema de estaciones base (o BSS).

Por último, los controladores de estaciones base están físicamente conectados al Centro de conmutación móvil (MSC) que los conecta con la red de telefonía pública y con Internet; lo administra el operador de la red telefónica. El MSC pertenece a un Subsistema de conmutación de red (NSS) que gestiona las identidades de los usuarios, su ubicación y el establecimiento de comunicaciones con otros usuarios.
Generalmente, el MSC se conecta a bases de datos que proporcionan funciones adicionales:

El Registro de ubicación de origen (HLR): es una base de datos que contiene información (posición geográfica, información administrativa, etc.) de los abonados registrados dentro de la zona del conmutador (MSC).

El Registro de ubicación de visitante (VLR): es una base de datos que contiene información de usuarios que no son abonados locales. El VLR recupera los datos de un usuario nuevo del HLR de la zona de abonado del usuario. Los datos se conservan mientras el usuario está dentro de la zona y se eliminan en cuanto abandona la zona o después de un período de inactividad prolongado (terminal apagada).

El Registro de identificación del equipo (EIR): es una base de datos que contiene la lista de terminales móviles.

El Centro de autenticación (AUC): verifica las identidades de los usuarios.
La red celular compuesta de esta manera está diseñada para admitir movilidad a través de la gestión de traspasos (movimientos que se realizan de una celda a otra).

5.3 La Generación 2.5

Si bien la tercera generación estaba en el horizonte, algunos servicios se hicieron necesarios previa a su llegada. El General Packet Radio Service (GPRS) desarrollado para el sistema GSM fue de los primeros en ser visto. Hasta este momento, todos los circuitos eran dedicados en forma exclusiva a cada usuario. Este enfoque es conocido como “Circuit Switched”, donde por ejemplo un circuito es establecido para cada usuario del sistema. Esto era ineficiente cuando un canal transfería información sólo en un pequeño porcentaje. El nuevo sistema permitía a los usuarios compartir un mismo canal, dirigiendo los paquetes de información desde el emisor al receptor. Esto

permite el uso más eficiente de los canales de comunicación, lo que habilita a las compañías proveedoras de servicios a cobrar menos por ellos.

Aún más cantidad de mejoras fueron realizadas a la taza de transferencia de información al introducirse el sistema conocido como EDGE (Enhanced Data rates aplicado a GSM Evolution). Éste básicamente es el sistema GPRS con un nuevo esquema de modulación de frecuencia.

Muchos de los proveedores de servicios de telecomunicaciones (carriers) se migraron a las redes 2.5G antes de entrar masivamente a 3G. La tecnología 2.5G es más rápida y más económica para actualizar a 3G.

5.3.1 EL Estándar GPRS

El estándar GPRS (General Packet Radio Service) es una evolución del estándar GSM. Dado que es un estándar de telefonía de segunda generación que permite una transición hacia la tercera generación (3G), el estándar GPRS por lo general se clasifica como 2.5G.

GPRS extiende la arquitectura del estándar GSM para permitir la transferencia de datos del paquete con una tasa de datos teóricos de alrededor de 171,2 Kbits/s (hasta 114 Kbits/s en la práctica). Gracias a su modo de transferencia en paquetes, las transmisiones de datos sólo usan la red cuando es necesario. Por lo tanto, el estándar GPRS permite que el usuario reciba facturas por volumen de datos en lugar de la duración de la conexión, lo que significa especialmente que el usuario puede permanecer conectado sin costo adicional.

GPRS admite características nuevas que no están disponibles en el estándar GSM y que se pueden clasificar en los siguientes tipos de servicios:

- Servicio de punto a punto (PTP): es la capacidad de conectarse en modo cliente-servidor a un equipo en una red IP.
- Servicio de punto a multipunto (PTMP): constituye la capacidad de enviar paquetes a un grupo de destinatarios (Multidifusión).
- Servicio de mensajes cortos (SMS).

5.3.2 El estándar EDGE

El estándar EDGE (Enhanced Data Rates for GSM Evolution, Tasas de datos mejoradas para la evolución de GSM) es la evolución del estándar GSM que modifica el tipo de modulación. Al igual que el estándar GPRS, el EDGE está pensado para ser una transición hacia la tercera generación de la telefonía móvil (3G). También se utiliza el término 2.75G para describir el estándar EDGE.

El EDGE utiliza una modulación diferente a la modulación usada por GSM (EDGE emplea la modulación 8-PSK), lo que implica que las estaciones base y las terminales móviles deben ser modificadas para poder admitirlo.

El EDGE triplica la velocidad de datos, pero ofrece un área de cobertura menor. En teoría, el EDGE posee un rendimiento de hasta 384 Kbits/s en el caso de estaciones fijas (peatones y vehículos lentos) y hasta 144 Kbits/s para estaciones móviles (vehículos veloces).

5.4 La Tercera generación 3G

La 3G es tipificada por la convergencia de la voz y datos con acceso inalámbrico a Internet, aplicaciones multimedia y altas transmisiones de datos. Los protocolos empleados en los sistemas 3G soportan altas velocidades de información enfocados para aplicaciones mas allá de la voz tales como audio (MP3), video en movimiento, video conferencia y acceso rápido a Internet, sólo por nombrar algunos.

Los sistemas 3G alcanzaran velocidades de hasta 384 Kbps permitiendo una movilidad total a usuarios viajando a 120 kilómetros por hora en ambientes exteriores y alcanzará una velocidad máxima de 2 Mbps permitiendo una movilidad limitada a usuarios caminando a menos de 10 kilómetros por hora en ambientes estacionarios de corto alcance o en interiores. Entre las tecnologías contendientes de la tercera generación se encuentran UMTS (Universal Mobile Telephone Service) y cdma2000.

El impulso de los estándares de la 3G está siendo apoyando por la ITU (International Telecomunications Union) y a este esfuerzo se le conoce como IMT-2000 (International Mobile Telephone).

Las características más importantes de la tecnología 3G son:

- Alta velocidad de transmisión de datos
- 144 Kbps con cobertura total para uso móvil
- 384 Kbps con cobertura media para uso de peatones
- 2 Mbps con áreas de cobertura reducida para uso fijo
- Compatibilidad mundial
- Compatibilidad de los servicios móviles de G3 con las redes de segunda generación.

La G3 ofrece velocidades de datos de más de 144 Kbit/s y de este modo brinda la posibilidad de usos multimedia, por ejemplo, transmisión de videos, video conferencias o acceso a Internet de alta velocidad. Las redes de G3 utilizan bandas con diferentes frecuencias a las redes anteriores: 1885 a 2025 MHz y 2110 a 2200 MHz.

5.4.1 El Estándar UMTS

El estándar UMTS (Universal Mobile Telecommunications System) es una de las tecnologías usadas por los móviles de tercera generación (3G, también llamado W-CDMA), sucesora de GSM, debido a que la tecnología GSM propiamente dicha no podía seguir un camino evolutivo para llegar a brindar servicios considerados de Tercera Generación.

Sus tres grandes características son las capacidades multimedia, una velocidad de acceso a Internet elevada, la cual también le permite transmitir audio y video en tiempo real; y una transmisión de voz con calidad equiparable a la de las redes fijas.

UMTS permite introducir muchos más usuarios a la red global del sistema, y además permite incrementar la velocidad a 2 Mbps por usuario móvil, esta tecnología ofrece los siguientes servicios:

- Facilidad de uso y bajos costes: UMTS proporcionará servicios de uso fácil y adaptable para abordar las necesidades y preferencias de los usuarios, amplia gama de terminales para realizar un fácil acceso a los distintos servicios y bajo coste de los servicios para asegurar un mercado masivo. Como el roaming internacional o la capacidad de ofrecer diferentes formas de tarificación.

- Acceso rápido: La principal ventaja de UMTS sobre la segunda generación móvil (2G), es la capacidad de soportar altas velocidades de transmisión de datos de hasta 144 kbit/s sobre vehículos a gran velocidad, 384 kbit/s en espacios abiertos de extrarradios y 7.2 Mbit/s con baja movilidad (interior de edificios)[1]. Esta capacidad sumada al soporte inherente del protocolo de Internet (IP), se combinan poderosamente para prestar servicios multimedia interactivos y nuevas aplicaciones de banda ancha, tales como servicios de video telefonía y video conferencia y transmisión de audio y video en tiempo real.

MODULO 6

REDES INALÁMBRICAS

MODULO 6: REDES INALÁMBRICAS

Una red inalámbrica es, como su nombre lo indica, una red en la que dos o más terminales pueden comunicar sin la necesidad de una conexión por cable.

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

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar. Hay muchas tecnologías diferentes que se diferencian por la frecuencia de transmisión que utilizan, y el alcance y la velocidad de sus transmisiones. Existen tres formas de clasificar a las redes inalámbricas, esta clasificación se describe a continuación.

6.1 Redes inalámbricas personales PAN

Dentro del ámbito de estas redes podemos integrar a dos principales actores:

- Las redes que se usan actualmente mediante el intercambio de información mediante infrarrojos. Estas redes son muy limitadas dado su corto alcance, necesidad de "visión sin obstáculos" entre los dispositivos que se comunican y su baja velocidad (hasta 115 kbps). Se encuentran principalmente en ordenadores portátiles, PDAs (Agendas electrónicas personales), teléfonos móviles y algunas impresoras.

- En segundo lugar el Bluetooth, estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDAs, teléfonos móviles de nueva generación y algún que otro ordenador portátil. Opera dentro de la banda de los 2'4 Ghz.

6.2 Redes inalámbricas de consumo MAN y WAN

- Redes CDMA (estándar de telefonía móvil estadounidense) y GSM (estándar de telefonía móvil europeo y asiático). Son los estándares que usa la telefonía móvil empleados alrededor de todo el mundo en sus diferentes variantes.

- 802.16 son redes que pretenden complementar a las anteriores estableciendo redes inalámbricas metropolitanas (MAN) en la banda de entre los 2 y los 11 Ghz.

6.3 Redes inalámbricas LAN

Las redes inalámbricas básicamente se diferencian de las redes conocidas hasta ahora por el enfoque que toman de los niveles más bajos de la pila OSI, el nivel físico y el nivel de enlace, los cuales se definen por el 802.11 del IEEE (Organismo de estandarización internacional).

6.3.1 Ventajas y desventajas de las redes inalámbricas.

Las ventajas que presentan las redes de este tipo son su libertad de movimientos, sencillez en la reubicación de terminales y la rapidez consecuente de instalación. La solución inalámbrica resuelve la instalación de una red en aquellos lugares donde el cableado resulta inviable, por ejemplo en edificios históricos o en grandes naves industriales, donde la realización de canaletas para cableado podría dificultar el paso de transportes, así como en situaciones que impliquen una gran movilidad de los terminales del usuario o la necesidad de disponer de vías alternativas por motivos de seguridad.

Por otra parte en las redes inalámbricas hay elementos intermedios como las paredes, campos magnéticos o eléctricos u otros elementos interpuestos entre el punto de acceso y la tarjeta de red que modifican la velocidad de transmisión a la baja.

Otro punto negativo es la saturación del espectro e interferencias (cuantos más usuarios inalámbricos haya en las cercanías más colisiones habrá en las transmisiones por lo que la velocidad se reducirá, esto también es aplicable para las interferencias. Estas redes son más inseguras que otras, ya que cualquiera podría acceder a la red inalámbrica.

6.3.2 Estándares

802.11a: fue la primera aproximación a las WN y llega a alcanzar velocidades de hasta 54 Mbps dentro de los estándares del IEEE y hasta 72 y 108 Mbps con tecnologías de

desdoblamiento de la velocidad ofrecidas por diferentes fabricantes, pero que no están (a día de hoy) estandarizadas por el IEEE. Esta variante opera dentro del rango de los 5 Ghz. Inicialmente se soportan hasta 64 usuarios por Punto de Acceso.

Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, la gratuidad de la frecuencia que usa y la ausencia de interferencias en la misma.

Sus principales desventajas son su incompatibilidad con los estándares 802.11b y g, la no incorporación a la misma de QoS.

802.11b: es la segunda aproximación de las WN. Alcanza una velocidad de 11 Mbps estandarizada por el IEEE y una velocidad de 22 Mbps por el desdoblamiento de la velocidad que ofrecen algunos fabricantes pero sin la estandarización (a día de hoy) del IEEE. Opera dentro de la frecuencia de los 2'4 Ghz. Inicialmente se soportan hasta 32 usuarios por PA.

802.11g: Es la tercera aproximación a las WN, y se basa en la compatibilidad con los dispositivos 802.11b y en el ofrecer unas velocidades de hasta 54 Mbps.

En este documento vamos a referirnos principalmente al 802.11g, por ser el estándar mas utilizado hoy día.

6.3.3 Dispositivos

En las redes inalámbricas vamos a disponer de dos dispositivos los cuales son las tarjetas de red y los puntos de acceso.

Tarjetas de red o TR (inalámbricas): estas sustituyen a las tarjetas de red Ethernet a las que estábamos acostumbrados. Recibirán y enviarán la información hacia su destino desde el ordenador en el que estemos trabajando. La velocidad de transmisión/recepción de los mismos es variable dependiendo del fabricante y de los estándares que cumpla.

Puntos de Acceso ó PA: serán los encargados de recibir la información de los diferentes TR de los que conste la red bien para su centralización bien para su encaminamiento. Complementan a los Hubs, Switches o Routers, si bien los PAs

pueden substituir a los últimos pues muchos de ellos ya incorporan su funcionalidad. La velocidad de transmisión/recepción de los mismos es variable, las diferentes velocidades que alcanzan varían según el fabricante y los estándares que cumpla.

6.3.4 Funcionamiento de los dispositivos

Actualmente ya hay fabricantes que ofrecen antenas que aumentan la capacidad de TX/RX (transmisión y recepción) de los dispositivos wireless.

Dentro de los PAs (actualmente ya se puede comenzar a aplicar también a los TRs) se puede modificar enormemente la capacidad de TX/RX gracias al uso de antenas especiales. Estas antenas se pueden dividir en: direccionales y omnidireccionales.

Las antenas Direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.

Las antenas Omnidireccionales "envían" la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

6.3.5 Topología y Modos de funcionamiento de los dispositivos

Es conveniente el hacer una división entre la topología y el modo de funcionamiento de los dispositivos WiFi. Con topología nos referimos a la disposición lógica (aunque la disposición física también se pueda ver influida) de los dispositivos.
En el mundo Wireless existen dos topologías básicas:

Topología Ad-Hoc: Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red Peer to Peer o de igual a igual, para lo cual sólo vamos a necesitar el disponer de un SSID igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento.

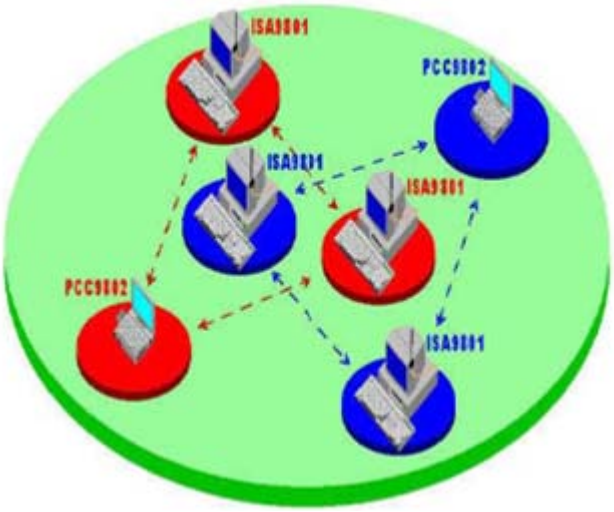


Figura 6.1 Topología Ad-Hoc

Topología Infraestructura: En esta existe un nodo central (Punto de Acceso WiFi) que sirve de enlace para todos los demás (Tarjetas de Red Wifi). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del AP.

Permiten trabajar con las distintas redes, dejando el trabajo de canalizar los datos al punto de acceso educiendo así la labor de la tarjeta de red de encontrar a la tarjeta que reciba los datos, por lo que si se desea unir dos redes, una cableada y una inalámbrica, es mejor usar esta topología.

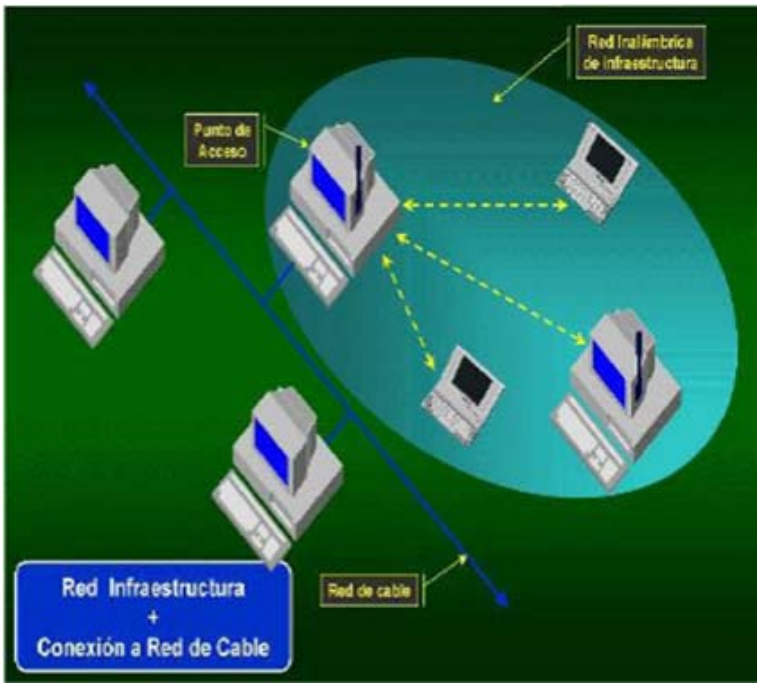


Figura 6.2 Topología Infraestructura

6.3.6 Seguridad

Existen varias alternativas para garantizar la seguridad en las redes inalámbricas. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes:

WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire. Este tipo de cifrado no está muy recomendado, debido a las grandes vulnerabilidades que presenta.

WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud.

IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.

Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos.

Ocultación del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.

WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

MODULO 7

PROYECTO DE NEGOCIO: OPTIMIZACIÓN DE APPLICATIONS SERVERS

MODULO 7: PROYECTO DE NEGOCIO OPTIMIZACIÓN DE SERVIDOR DE APLICACIONES

El objetivo de este modulo fue desarrollar, implementar, o presentar algún componente relacionado con el campo de las telecomunicaciones y como es que este producto o desarrollo puede ser implementado como una solución de negocio.

En mi caso elegí la optimización de applications servers, mediante balanceadores de carga F5 Local Traffic Manager BIG-IP, ya que este producto es un componente de hardware, que permite redireccionar el trafico de un servidor a otro sin que la aplicación se vea afectada y el servicio siempre este disponible.

7.1 Definición de Servidor de Aplicación

Es un dispositivo de software/hardware que proporciona servicios de aplicación a las computadoras cliente. Un servidor de aplicaciones generalmente gestiona la mayor parte (o la totalidad) de las funciones de lógica de negocio y de acceso a los datos de la aplicación. Los principales beneficios de la aplicación de la tecnología de servidores de aplicación son la centralización y la disminución de la complejidad en el desarrollo de aplicaciones.

Un ejemplo común del uso de servidores de aplicación (y de sus componentes) son los portales de Internet, que permiten a las empresas la gestión y divulgación de su información, y un punto único de entrada a los usuarios internos y externos. Teniendo como base un servidor de aplicación, dichos portales permiten tener acceso a información y servicios (como servicios Web) de manera segura y transparente, desde cualquier dispositivo.

Una vez explicado que es un servidor de aplicaciones se comenzara explicando las características y funcionalidades del balanceador de carga F5 Local Traffic Manager.

7.2 Conceptos Básicos de Local Traffic Manager BIG-IP

Para entender más a detalle que es Local Traffic Manager, se explicaran conceptos basicos, ya que este equipo se puede configurar de diferente forma, pero siempre teniendo la misma lógica.

En el corazón del sistema BIG-IP LTM se encuentran características como virtual server, pools, profiles, iRules y monitores, para asegurar la funcionalidad del sistema BIG-IP. A continuación se describen dichos conceptos.

7.2.1 Nodo

Un nodo representa la dirección IP real de un determinado servidor físico de la red que deberá ser monitoreado por el sistema BIG-IP para determinar su disponibilidad. Un nodo tiene una única dirección IP.

7.2.2 Miembro de pool

Un miembro de pool es una combinación real de dirección IP y puerto destino que se encuentra hospedado en un servidor físico real. Un único servidor físico real puede hospedar varios miembros de pool.

7.2.3 Virtual Server

Un virtual server recibe los requerimientos del cliente, y los distribuye acordemente a un determinado miembro (nodo/servidor) que forma parte de un determinado pool de servidores. El servidor físico real seleccionado depende del algoritmo de balanceo que posea configurado el pool de servidores en cuestión.

Cada Virtual Server está compuesto de la combinación de una dirección IP virtual y de un puerto de servicio virtual: <IP:servicio>. La dirección IP virtual debe de poder ser accedida a través de la red por los diferentes clientes que harán uso de la correspondiente aplicación.

Un virtual Server define la relación entre una dupla virtual <dirección IP, puerto> que conoce el cliente de una aplicación y la dupla real <dirección IP, puerto> que se encuentra disponible en un determinado servidor/nodo.

A través de un virtual Server se puede aplicar una iRule, es decir, un script definido por el usuario para inspeccionar y dirigir conexiones particulares de una manera específica. Por ejemplo, es posible definir una iRule que busque en el contenido de la conexión TCP una cadena de caracteres en particular y en caso de encontrarla, indicar al virtual server que envíe dicha conexión a un cierto pool de servidores o miembro de pool en particular. En la figura se muestra la forma en que trabajan los servidores virtuales.

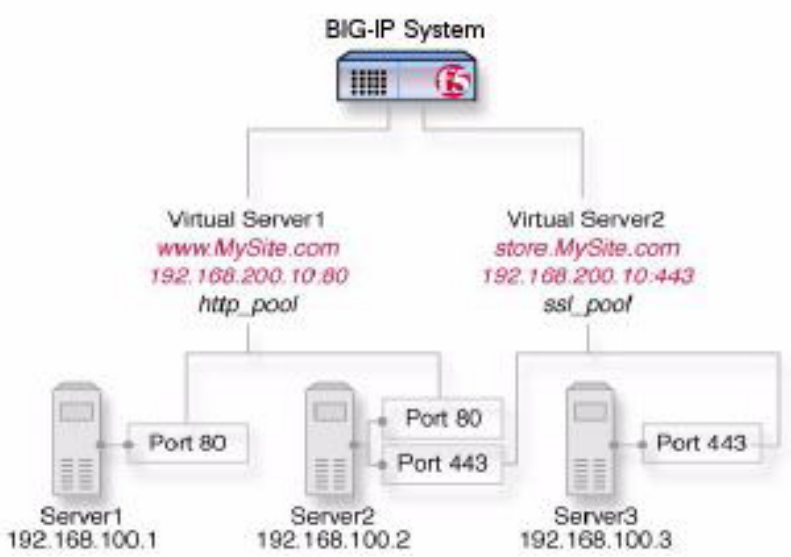


Figura 7.2 Forma de implementer el LTM

7.2.4 Pool

Un pool es un conjunto de dispositivos de red (llamados miembros o nodos), como por ejemplo, servidores web, servidores de correo, etc., que se agrupan para recibir y procesar un determinado tipo de tráfico (servicio).

Permite el balanceo de los requerimientos clientes entre los diferentes nodos pertenecientes a dicho grupo de acuerdo al método/algoritmo de balanceo de carga y el método de persistencia asignado a dicho pool.

Cuando se crea un pool, se asigna un conjunto de servidores al mismo, llamados miembros o nodos del pool, y luego se asocia el pool a un determinado servidor virtual

(virtual server) que es quien recibirá el requerimiento inicial. Si el pool NO se encuentra asociado directa o indirectamente a un virtual Server, el mismo no será utilizado.

De esta forma, cuando se inicia una nueva conexión la misma es recibida por el correspondiente Virtual Server, quien direccionará la conexión a un cierto miembro del pool de acuerdo al método de balanceo de carga que posea asignado dicho pool.

7.2.5 Monitores

Los monitores son herramientas del sistema BIG-IP LTM que verifican la disponibilidad de los nodos y servicios de la red y permiten determinar la disponibilidad de cada uno de los miembros de pool definidos en el sistema. Un monitor verifica un cierto dispositivo por una determinada respuesta en un período de tiempo definido. De esta forma, si un miembro del pool o un nodo que está siendo monitoreado no responde dentro de un período de tiempo específico o el estado de un miembro del pool o nodo indica que su rendimiento está degradado el sistema BIG-IP LTM puede redireccionar el tráfico a otro miembro del pool o nodo.

El sistema LTM posee ciertos monitores definidos por defecto (monitores pre-configurados), y permite definir otros monitores de acuerdo a las necesidades del usuario. Los monitores creados por el usuario son llamados monitores personalizados. Cada monitor, sin importar si es pre-configurado o personalizado, verifica el estado de un protocolo particular, servicio o aplicación. Por ejemplo, un tipo de monitor “http” permite monitorear la disponibilidad del servicio http en un pool, miembro del pool o nodo.

7.2.6 SNAT (Secure Network Address Translations)

La característica de SNAT permite traducir la dirección IP de origen de un requerimiento cliente, permitiendo que varios hosts compartan la misma dirección IP. SNAT provee el mapeo entre varios nodos (a menudo dispositivos internos), y una dirección IP SNAT.

Los puertos de origen generalmente son mantenidos, al menos que fuera necesario su traducción durante el establecimiento de la conexión para asegurar que todas las combinaciones de puerto/dirección IP de las conexiones son únicas.

7.3 Definición del LTM BIG-IP

Es un equipo destinado a proporcionar la redundancia de servidores, necesaria como para que el servicio quede asegurado aún en el caso de que se produzcan caídas.

El balanceador distribuye el tráfico de red o aplicación en un amplio número de servidores, como se muestra en la figura 7.1.

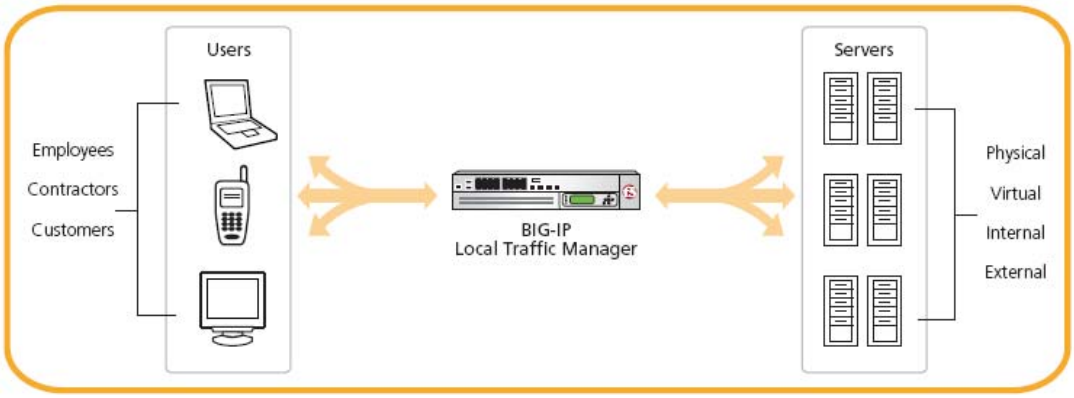


Figura 7.1 Forma de trabajar del LTM

Los balanceadores de carga se utilizan para aumentar la capacidad (usuarios simultáneos) y la fiabilidad de las aplicaciones. Mejoran el rendimiento global de las aplicaciones al reducir la carga de los servidores asociados con la administración y mantenimiento de aplicaciones y sesiones de red, así como mediante la realización de tareas específicas de la aplicación.

El Local Traffic Manager (LTM) es un sistema de entrega de aplicaciones de red que proporciona una solución para asegurar, optimizar y distribuir aplicaciones, permitiendo a las organizaciones una entrega de la aplicación competitiva.

El equipo Big-IP se comporta de cara a la red como un router, debiendo situarse entre dos redes con distinto direccionamiento. Para ello, dispone de dos conectores Ethernet, uno destinado a la red externa por donde entrarán todas las peticiones a los servidores Web, y otro para la red interna, en la que deben estar situados todos los equipos balanceados.

Propone un diseño integrado y organizado para garantizar una organización y orden en la red. Crea un modelo piramidal, que permite a las redes ir creciendo de forma ordenada. También proporciona alta disponibilidad (redundancia de equipos). Mediante el balanceo de carga se va a conseguir más eficacia, rapidez, a la vez eliminar congestión en servidores y carga en la red.

Al igual que otros dispositivos similares, ofrece balanceo de diversos servicios, incluyendo http, ftp y cortafuegos, pero la característica más destacable es que incorpora, si se adquiere la configuración correspondiente, un chip acelerador SSL que permite que el propio equipo maneje las conexiones SSL con los clientes encriptando y desencriptando los mensajes directamente y reenviando el tráfico a un servidor Web estándar. Esto permite ofrecer a los clientes el nivel de seguridad propio del tráfico encriptado al tiempo que descarga a los servidores Web, normalmente encargados de soportar páginas dinámicas, enlaces a bases de datos y otros procesos similares de la tarea de encriptar los paquetes, proceso que se realiza en el equipo aprovechando la potencia que le aporta el hardware dedicado a tal efecto.

F5 Networks, al igual que hacen otros fabricantes, no ha diseñado el producto para ser completamente redundante a fallos y por tanto, no dispone, de doble fuente de alimentación, ni de dobles puertos de entrada y salida. La solución redundante se proporciona mediante combinaciones redundantes de varios de ellos. Es de destacar que, al contrario de lo que sucede con los equipos de otras firmas, las soluciones para Big-IP funcionan en configuraciones activo-activo, permitiendo que los dos balanceadores soporten parte de la carga. En una configuración activo-pasivo sólo uno de los dispositivos maneja todo el tráfico, entrando en acción el segundo elemento únicamente si falla el primero.

7.4 Características del LTM

BIG-IP Local Traffic Manager (LTM) convierte su red en una infraestructura ágil para la entrega de aplicaciones. Es un proxy completo entre los usuarios y los servidores de aplicaciones, creando una capa de abstracción para asegurar, optimizar y equilibrar la carga de tráfico de aplicaciones. Esto le da el control para agregar servidores fácilmente, eliminar el tiempo de inactividad, mejorar el rendimiento de la aplicación, y cumplir con sus requisitos de seguridad.

Proporciona balanceo de carga Avanzado y el health monitoring le ayuda a agregar más servidores y dirigir el tráfico. También reduce el volumen de tráfico y minimiza los cuellos de botella, así como el impacto de la WAN, LAN, y la latencia de Internet en el rendimiento de aplicación.

Optimiza la infraestructura existente y proporciona una fácil administración de la plataforma, elimina los puntos únicos de fallo y virtualiza la red y aplicaciones. Esto garantiza que todas las aplicaciones sean fácil de administrar y fácil de escalar.

Ofrece monitoreos para la comprobación de los dispositivos, aplicaciones y disponibilidad de contenidos, incluidos los monitores especializados para muchas aplicaciones (incluyendo servidores de aplicaciones diversas), así como monitores para comprobar el contenido personalizado y simular las llamadas de solicitud.

El LTM establece un objetivo, centralizado y eficiente para la reducción de tráfico y minimizar el efecto de la latencia de Internet y la conexión de cliente en los cuellos de botella.

Virtualiza y oculta todas las aplicaciones, los códigos de error de servidor, y las referencias URL que pueden proporcionar pistas sobre los piratas informáticos con infraestructura, servicios, y sus vulnerabilidades asociadas.

La interfaz gráfica de usuario ofrece una fácil configuración que reduce los costes de instalación y mantenimiento en curso. La GUI incluye ayuda en línea, búsqueda y selección, reduciendo el tiempo para establecer y mantener configuraciones de gran tamaño.

Permite dominios administrativos que le permiten diseñar a medida particiones y asignar diferentes grados de derechos administrativos. Los administradores pueden diseñar vistas personalizadas por el servicio, los propietarios de aplicaciones, o esquema de segmentación, proporcionando la escala de gestión y eficiencia de la organización.

7.5 Métodos de balanceo de carga

Un método es un algoritmo que utiliza el sistema LTM para determinar el nodo al cual enviará el tráfico. Por ejemplo, el método de balanceo por defecto es Round Robin, lo

cual produce que el sistema LTM envíe cada requerimiento entrante al próximo miembro del pool disponible, distribuyendo de esta forma los requerimientos en forma pareja entre los servidores del pool.

Existen diferentes métodos de balanceo de carga. Se debe seleccionar aquel que mayor se corresponda con el entorno en particular donde se implementa la solución. Los algoritmos de balanceo de carga son:

- Round Robin
- Ratio (member) and Ratio (node)
- Dynamic Ratio
- Fastest (node) and Fastest (application)
- Least Connections (member) and Least Connections (node)
- Observed (member) and Observed (node)
- Predictive (member) and Predictive (node)

A continuación se listan las características de estos métodos de balanceo:

Round Robin: es el método de balanceo de carga por defecto. El modo Round Robin pasa cada nuevo requerimiento de conexión al próximo nodo/miembro en línea del pool, finalmente distribuyendo el tráfico entre todos los servidores del pool. Este modo funciona correctamente en la mayoría de las configuraciones, especialmente en aquellas en las cuales los miembros son equivalente (misma velocidad de procesamiento, cantidad de memoria).

Ratio: el sistema LTM distribuye las conexiones entre un conjunto de servidores de acuerdo al peso del ratio definido, donde el número de conexiones que recibirá cada servidor a través del tiempo es proporcional al peso del ratio definido para cada servidor. Este es un método de balanceo de carga estático, basando la distribución de carga en un peso de ratio estático definido por el usuario que es proporcional a la capacidad de los servidores.

Ratio dinámico: este método es similar al descrito anteriormente, excepto que los pesos de ratio se basan en un monitoreo continuo de los servidores, por lo cual cambian continuamente. Este es un método de balanceo de carga dinámico, dado que las conexiones se distribuyen basándose en diferentes aspectos del análisis de

performance del servidor en tiempo real, como por ejemplo el número actual de conexiones por nodo o el tiempo más rápido de respuesta del nodo. Este método es utilizado específicamente para balancear tráfico de plataformas RealNetworks RealSystem Server, plataformas Windows equipadas con Windows Management Instrumentation (WMI), o cualquier servidor equipado con un agente SNMP.

Fastest (nodo/aplicación): este método direcciona una nueva conexión a un cierto servidor basándose en el mejor tiempo de respuesta de todos los nodos activos del pool. Este método puede ser particularmente útil en entornos donde los nodos se encuentran distribuidos en redes lógicas diferentes.

Least Connections: este método direcciona la nueva conexión al servidor que posee menor cantidad de conexiones establecidas. Este método funciona bien en entornos donde los servidores que se están balanceando poseen capacidades similares. Es un algoritmo de balanceo dinámico, dado que distribuye las conexiones basándose en el análisis de performance en tiempo real de los servidores involucrados en el pool.

Observed: este método utiliza una combinación de la lógica utilizada en los métodos de balanceo Least Connections y Fastest. Con este método, los servidores son clasificados y ordenados de acuerdo a la combinación de los valores de cantidad de conexiones actuales y tiempo de respuesta. Los nodos que tienen el mejor equilibrio entre mínima cantidad de conexiones y mejor tiempo de respuesta recibe una mayor proporción de las conexiones. Este método es útil en entornos donde la performance de los nodos varía considerablemente.

Predictive: este método de balanceo también utiliza el método de clasificación o ranking usado por el modo Observed. Sin embargo, en este modo, el sistema LTM analiza la tendencia de la clasificación/ranking a través del tiempo, determinando si la performance de un cierto servidor está mejorando o disminuyendo. Los nodos con mayor ranking de performance que están actualmente mejorando, reciben una mayor proporción de las conexiones.

7.6 Ejemplo de topología de red con LTM

En la siguiente diapositiva, se muestra el funcionamiento del BIG-IP en un ambiente productivo y como es que el F5 interactúa con lo elementos de la red.

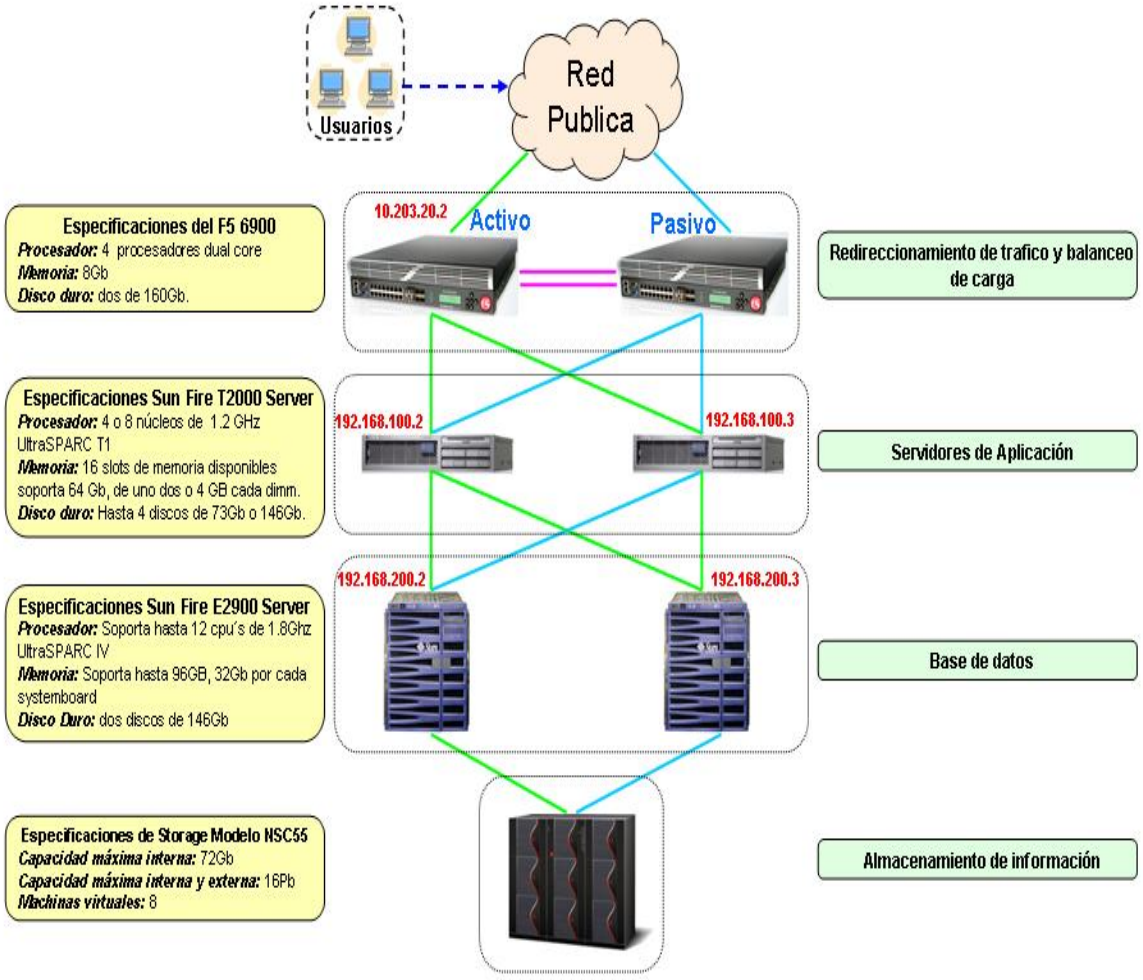


Figura 7.3 Arquitectura del Proyecto

Supongamos que existe un desarrollo en los servidores de aplicación. Para que el LTM pueda empezar a trabajar, se necesita que el cliente realicé una petición al application server o a la dirección 10.203.20.2, una vez que se tiene dicha petición el BIG-IP se encarga de traducir esa IP, al segmento 192.168.100.XX mediante el proceso de snat, en este nuevo segmento tenemos dos direcciones IP (192.168.100.2 y 192.168.100.3), estas direcciones pertenecen a los sun fire t2000 y juntos estos nodos forman un pool de servidores, los cuales están asignados a un virtual Server que es el encargado de recibir los requerimientos del cliente.

Cuando la petición es hecha al virtual Server, este se encarga de redirigir el tráfico a cualquiera de los dos miembros del pool, el destino del requerimiento depende del método de balanceo de carga.

Una vez que la demanda a pasado por el application Server continuará con los servidores de Base de datos o el destino de dicha petición será transferida según el desarrollo.

Teniendo este tipo de arquitectura, podemos asegurar que el servicio siempre estará disponible y será menos probable que la aplicación se vea afectada.

CONCLUSIONES

Hoy día las telecomunicaciones representan una parte importante en la vida cotidiana, ya que están presentes en el campo económico, cultural, educativo, empresarial, etc. Este diplomado ofrece la ventaja de generar una perspectiva y una visión más amplia que otros seminarios. Se dice que amplía el conocimiento, por que se tocan diversos temas, no solo se toca un punto en especial, si no que se presenta un resumen muy completo de cada tecnología.

En este diplomado se presento la oportunidad de poder relacionarte con diferentes áreas, ya que se tocan puntos que se interrelacionan con soporte técnico, Implementación de Proyectos, Redes, etc. Lo que permite que el trabajo diario sea realizado con mayor eficiencia y rapidez.

Por otra parte se presento que para cada tipo de problema existe una o más posibles soluciones y en todas estas opciones que se pueden manejar, hay ventajas y desventajas por lo tanto se debe de hacer un estudio acerca de que es lo que mas nos conviene y cual es el mejor camino para llegar al objetivo.

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean, esto suscitará que no solo se maneje un argumento y este curso tiene la puntualidad de formar una idea general del tipo de tecnología que podemos usar para cada situación.

En cada modulo se trataron diversas tecnologías, protocolos, procedimientos, estándares, componentes etc. Pero algo que tienen en común todos estos elementos es que fueron diseñados para la comunicación y el flujo de información, esto representa que el concepto de telecomunicaciones esta presente en cualquier lugar y que se ha vuelto una herramienta primordial para el desarrollo humano.

La información a la que se accede a través de las redes combina el texto con la imagen y el sonido, es decir, se trata de una información multimedia, una forma de comunicación que esta teniendo un enorme desarrollo gracias a toda la infraestructura de red y telecomunicaciones, esto hace notar la importancia de este concepto.

Para finalizar considero que el Diplomado Integral en Telecomunicaciones representa un gran aporte profesional para el egresado, ya que permite obtener cierto grado de conocimiento no solo en un área especifica sino que tiene la peculiaridad de manejar distintos temas los cuales son necesarios para el progreso como ingeniero.

GLOSARIO

Algoritmo.- Es un conjunto preescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien lo ejecute. Dados un estado inicial y una entrada, siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución.

Ancho de banda.- Es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado.

Bit.- El bit es la unidad mínima de información empleada en informática.

Broadcast.- Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

CDMA (Code division multiple access).- Es una técnica que emplea una serie de códigos especiales para proporcionar múltiples canales de comunicación dentro de un solo segmento dedicado del espectro electromagnético.

Cisco.- Es una empresa multinacional, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones

Diafonía.- Se dice que entre dos circuitos existe diafonía, denominada en inglés Crosstalk (XT), cuando parte de las señales presentes en uno de ellos, considerado perturbador, aparece en el otro, considerado perturbado.

Dieléctrico.- Son los materiales que no conducen la electricidad, por lo que se pueden utilizar como aislantes eléctricos.

Espectro electromagnético.- El rango completo de longitudes de onda es lo que se denomina el espectro electromagnético.

FDMA (Frequency Division Multiple Access).- Es una técnica de control de acceso al medio en la cual el espectro radioeléctrico se divide en una serie de secciones o ranuras dependiendo del número de usuarios que tengamos en ese momento.

FTP.- Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

Hertz.- Es la unidad de frecuencia del Sistema Internacional de Unidades.

HTTP.- Define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web.

IEEE (Instituto de Ingenieros Electricistas y Electrónicos).- Es una asociación técnico-profesional mundial dedicada a la estandarización.

ISP (Internet Service Provider).- Es una empresa que brinda conexión a Internet a sus clientes.

ITU (International Telecomunications Union).- es el organismo especializado de la Organización de las Naciones Unidas encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

Longitud de onda.- La longitud de una onda es la distancia que recorre la onda en el intervalo de tiempo transcurrido entre dos máximos consecutivos de una de sus propiedades.

Modulación.- Engloba el conjunto de técnicas para transportar información sobre una onda portadora. Estas técnicas permiten un mejor aprovechamiento del canal de comunicación lo que posibilita transmitir más información en forma simultánea, protegiéndola de posibles interferencias y ruidos.

Multicast.- Es el envío de la información en una red a múltiples destinos simultáneamente

Proxy.- Programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Radiofrecuencia.- Es la porción menos energética del espectro electromagnético, situada entre unos 3 Hz y unos 300 GHz.

RealNetworks.- Es un proveedor de software para Internet y servicios. La compañia es conocida por la creación de RealAudio, un formato de audio comprimido, RealVideo, un formato de video comprimido y RealPlayer, un reproductor multimedia.

Servidor.- Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

SMTP (Simple Mail Transfer Protocol).- Es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico.

SNMP (Simple Network Management Protocol).- Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

SUN.- Es una empresa informática recientemente comprada por Oracle Corporation, fabricante de semiconductores y software.

TDMA (Time division multiple access).- Técnica de acceso totalmente digital mediante la cual varias estaciones acceden u ocupan el ancho de banda existente. Todo un grupo de estaciones tienen asignada una misma ranura, con cierto ancho de banda fijo y se comparte entre ellas secuencialmente en el tiempo.

Unicast.- Es el envío de información desde un único emisor a un único receptor.

URL.- Es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación

VPN (virtual private network).- Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada

Wi-Fi.- Es una marca de la Wi-Fi Alliance, la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

Windows Management Instrumentation (WMI).- es una iniciativa que pretende establecer normas estándar para tener acceso y compartir la información de administración a través de la red de una empresa.

REFERENCIAS

- Bruce A. Hallberg Fundamentos De Redes Mcgraw-Hill Interamericana
- Jordi Julia Sort Redes Metropolitanas = Metropolitan Networks Editorial Gustavo Gili
- William Stallings Redes E Internet De Alta Velocidad: Rendimiento Y Calidad De Servicio Prentice Hall
- William Stallings Comunicaciones Y Redes De Computadoras Prentice Hall
- Andrew S. Tanenbaum Redes De Computadora Pearson
- Ariganello, Ernesto Técnicas De Configuración De Routers Cisco ra-Ma Editorial
- Ariganello, Ernesto / Barrientos Sevilla, Enrique Redes Cisco Ccnp A Fondo ra-Ma
- William Stallings. Data and Computer Communications. Prentice Hall
- Andrew S. Tanenbaum. Computer Networks. Prentice Hall
- Douglas E. Comer. Internetworking with TCP/IP. Prentice Hall
- Stallings, William Comunicaciones y Redes de Computadores, Prentice Hall
- Comer, Douglas (2000). Redes Globales de Información con Internet y TCP/ IP, Prentice Hall
- http://www.monografias.com/trabajos29/direccionamiento-ip/direccionamiento-ip.shtml
- http://www.wikipedia.org/
- http://es.kioskea.net/contents/lan/concentrateurs.php3?part=2
- http://tech-freaks.net/wp-content/uploads/CCNA4.0-Capitulo03.pdf
- http://es.kioskea.net/contents/telephonie-mobile/edge.php3
- http://www.eveliux.com/mx/la-evolucion-de-la-telefonia-movil.php
- http://www.mailxmail.com/curso-redes-inalambricas-wi-fi-futuro-comunicacion/anexos-estandares-si-estandares-no-que-hacer
- http://www.cabinas.net/monografias/tecnologia/generaciones_de_la_telefonia_celular.asp