# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

**PROPUESTA DE INSTALACIÓN DE CORE SWITCH EN LA UACM FUNDAMENTADA EN LOS CONOCIMIENTOS ADQUIRIDOS EN EL DIPLOMADO INTEGRAL EN TELECOMUNICACIONES**

TRABAJO ESCRITO EN LA MODALIDAD DE SEMINARIOS
Y CURSOS DE ACTUALIZACIÓN PROFESIONAL

QUE PARA OBTENER EL TITULO DE

**INGENIERO EN COMPUTACIÓN**

PRESENTA:

**JUAN CARLOS ROCHA PEÑA**

ASESOR: ING. JOSÉ MANUEL QUINTERO CERVANTES

**BOSQUES DE ARAGÓN ESTADO DE MÉXICO, 2010**

# Agradecimientos

A Dios por darme vida e inteligencia y permitir así concluir esta etapa importante de mi vida.

A mis padres por darme la vida, su tiempo, atención y apoyo; así como la orientación y consejos que han hecho de mí una persona preparada y madura con carácter para enfrentar la vida; carácter que me ha permitido culminar mi carrera universitaria y obtener un título profesional, que es la mejor herencia que puedo obtener y que no defraudaré.

A mis hermanos por su ayuda incondicional que me han brindado y me siguen brindando y que ha permitido culminar mis estudios de manera satisfactoria.

Al Ingeniero David Sánchez por brindarme la confianza para poder desempeñar mi carrera en el ámbito laboral y por todo el apoyo dado para permitirme tomar este diplomado, así como todas las facilidades laborales y de conocimiento para poder llevar a cabo el siguiente trabajo.

A las personas que han sido especiales en mi vida, a la traviesa Fabi y a los verdaderos amigos los cuales son los que tienen la oportunidad de leer estas líneas y que de manera desinteresada con sus ánimos y orientación me han impulsado para poder culminar esta meta.

Y a los profesores asesores por la paciencia para orientarme durante todo este proceso de titulación.

"*El conocimiento y la experiencia nos dan la formación que nos permite tener carácter propio para enfrentar la vida"*

JUAN CARLOS

# ÍNDICE

CAPÍTULO PÁGINA

# INTRODUCCIÓN

El cambio y evolución de la tecnología exigen que las personas se encuentren cada día más capacitadas en el uso de las nuevas tecnologías; es el ingeniero el profesionista encargado de desarrollar dicha tecnología buscando resolver algún tipo de problema que encuentra en la sociedad o hacer que ésta cuente con las herramientas o equipo que hagan que las actividades que realiza en su vida cotidiana sean más fácil de llevar a cabo.

Por tal motivo el ingeniero debe ser un profesionista que esté en constante actualización de sus conocimientos, para que de esta manera pueda proponer la utilización de alguna nueva tecnología que permita hacer un uso eficiente de algún recurso material o financiero, o simplemente pueda hacer uso eficaz de algún tipo de tecnología ya existente en su ambiente de trabajo.

La UNAM es una institución que brinda la posibilidad de lograr dicha actualización de conocimientos a través de algún tipo de curso complementario a sus materias curriculares, como lo son los diplomados, los cuales en algunos casos son considerados como una opción para obtener un título profesional.

Tomando en consideración lo anterior fue que decidí tomar el diplomado Integral en Telecomunicaciones que ofrece la UNAM, ya que por medio él es posible obtener una visión práctica de todos los conocimientos adquiridos durante la carrera, además de ayudar a fortalecer los conceptos teóricos que exige el ámbito laboral para un correcto desempeño de mis funciones, y así ser partícipe de manera activa en los proyectos que se desarrollan en el mismo.

El diplomado Integral en Telecomunicaciones se desarrolla a lo largo de 12 módulos, los cuales de manera general tienen como objetivo brindar los conocimientos teórico-prácticos básicos que hacen posible la transmisión de voz y datos en forma alámbrica e inalámbrica tanto a gran escala como los son las redes de microondas como en redes locales pequeñas.

Con respecto a las redes de datos se estudian los diferentes tipos de protocolos y tecnologías que existen y que permiten la interconexión de las mismas, sin embargo se hace especial énfasis en la redes de datos IP debido a su popularización entre la mayoría de usuarios.

Por lo que respecta a la redes de voz, se estudian las diversas tecnologías existentes tanto en las redes de telefonía fija como en móviles, los protocolos que rigen a cada una de ellas y los cambios que han sufrido éstas a lo largo de los años.

El presente trabajo muestra una síntesis de los conocimientos adquiridos en el diplomado, los cuales sirvieron como fundamento para poder presentar un proyecto de propuesta de cambio de equipos de red en la UACM y que da título a este trabajo. Dicho proyecto pretende dar solución a la problemática de congestión de tráfico existente en la universidad lo cual se refleja en un aumento de tiempo en el transporte de archivos entre máquinas, así como el tiempo que se toma en hacer una consulta a las aplicaciones internas.

# CAPITULO 1

# MÓDULOS DEL DIPLOMADO

## MÓDULO I

## INTRODUCCIÓN A LAS TELECOMUNICACIONES

Desde sus orígenes el hombre tuvo la necesidad de comunicarse, expresar ideas, sentimientos o pensamientos; es la comunicación la que permite al hombre desarrollarse en su vida diaria con los demás, y permite a su vez el desarrollo de la ciencia y la tecnología ya que por medio de la comunicación se intercambian experiencias y conocimientos.

En sus orígenes la comunicación entre el hombre se limitaba a señas, gestos o ademanes, al paso del tiempo se comienza a expresar por medio de pinturas o símbolos que podían ser interpretados por las demás personas. En algunas ocasiones esto no era del todo posible, ya que surge la necesidad de comunicarse de manera secreta y que sólo la gente que tenía o conocía un cierto código podía interpretar la información, así surge lo que se conoce como el cifrado de la información en donde el hombre desea comunicarse procurando que su información sea secreta.

Al avanzar la ciencia las comunicaciones sufrieron un gran cambio, ya no sólo se podían expresar las ideas y pensamientos con alguna otra persona estando de frente a ella, si no que ahora era posible hacerlo a distancia gracias al descubrimiento de la electrónica surgiendo de así el concepto de telecomunicaciones; es entonces cuando el hombre pudo darse cuenta que no sólo podía comunicarse con una sola persona si no que lo podía hacer con varias a la vez.

Es el descubrimiento de la electricidad así como de las propiedades que posee lo que permitió sembrar las bases de lo que posteriormente se llamaría electrónica y de sus componentes. Hoy en día no sería posible poder comunicarnos de manera rápida y fácil sin el desarrollo de la electrónica; han sido muchas las personas que han brindado su aporte para el desarrollo de esta disciplina desde que el físico James Clerk Maxwell siembra las bases teóricas del electromagnetismo, que después Heinrich Hertz comprobaría a nivel de laboratorio, sin embargo fue el italiano Guillermo Marconi quien logra generar ya de manera práctica ondas de radio. No podemos dejar de mencionar un paso importante en el desarrollo de los sistemas electrónicos como lo es el invento de la válvula electrónica con la cual fue posible desarrollar sistemas electrónicos más complejos, así como su evolución al transistor el cual condujo a que los sistemas fueran más pequeños y baratos; vendría después la encapsulación de varios transistores en un solo dispositivo el cual llevaría el nombre de circuito integrado, hasta llegar a lo que hoy en día es el “cerebro” de todo sistema electrónico de telecomunicaciones el llamado microprocesador el cual nos permite realizar miles de operaciones en muy poco tiempo.

Sin embargo pese a que han sido muchas las personas que han intervenido en el desarrollo de los sistemas electrónicos de telecomunicaciones, no se puede dejar de mencionar que gran parte de estos avances se ha logrado por medio de las guerras, ya que es en tiempo de guerra cuando los países buscan desarrollar su propia tecnología buscando por supuesto ser superior a la del contrario. Podemos mencionar por ejemplo el caso de internet y los protocolos TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet) los cuales fueron desarrollados por la milicia de los Estados Unidos.

Debido a la diversidad de dispositivos y fabricantes de sistemas de comunicación surge la necesidad obligada de normar o estandarizar procesos, métodos, especificaciones técnicas, definiciones de características, etc., para asegurar que los materiales, productos, procesos y

servicios se ajusten a su propósito. El propósito de la estandarización es permitir la interoperabilidad de los dispositivos de comunicaciones, que éstos puedan cumplir con la calidad requerida para su correcto funcionamiento, además que se evitan las llamadas arquitecturas cerradas en las cuales un solo fabricante pueda crear sistemas de comunicaciones propietarios. Surge también el concepto de protocolo en las telecomunicaciones en el cual se establecen los diferentes pasos a seguir que debe realizar un sistema para poder entablar algún tipo de comunicación con otro.

En un principio la tecnología de las telecomunicaciones por su alto costo sólo era accesible para la gente con un nivel económico alto ya que era cara, sin embargo al paso del tiempo dicha tecnología fue abaratándose en costos y reduciendo tamaños, esto por supuesto propició que el mundo de las telecomunicaciones tuviese un gran alcance para la sociedad y que cualquier persona hoy en día pueda contar con algún dispositivo que le permita comunicarse de manera rápida y sencilla. Hoy es posible estar en contacto con familiares a distancias muy grandes, explorar el universo, recibir información del mundo en tan sólo unos instantes, incluso no sólo podemos hablar si no que es posible ver a nuestros familiares aunque éstos estén distantes.

Si bien aunque han sido grandes los beneficios que ha tenido el desarrollo de las telecomunicaciones, algunas veces se han utilizado para malos propósitos como lo son robos de identidades, difundir información errónea, grandes fraudes, difamaciones, espionaje, etc., Es entonces que surge un problema para el mundo de las telecomunicaciones "la seguridad" y sus interrogantes ¿qué tan seguras son las telecomunicaciones?, ¿realmente al comunicarnos gozamos de privacidad?, ¿qué tanto puedo confiar en las telecomunicaciones para difundir datos personales?. Son interrogantes que se plantean después que se ha visto que es posible que cualquier gente pueda vulnerar la integridad de los datos, lo cual provoca un gasto extra ya que se busca que toda la información viaje de manera íntegra, por lo que se tiene que recurrir a las herramientas que permitan asegurar que nuestra información viaje sin que sufra ningún tipo de alteración, como es el caso del Internet y la utilización de herramientas como lo son firewalls. Éste es un punto malo que propicia el alejamiento de la sociedad al mundo de las telecomunicaciones ya que todavía hay gente que por ejemplo que no realiza trasferencias bancarias o que no proporciona ningún dato personal porque cree que su información será vulnerada. Es por esto que en las telecomunicaciones ahora no sólo se persigue la comunicación a distancia si no que también se tenga la certeza de que la información que mandemos llegue íntegra a su destino.

Son tres los aspectos que se buscan al enviar información: 1.- La confidencialidad, que tiene que ver con la protección de la información frente acceso no autorizados a ella. 2.- La integridad, que se refiere a que no haya alteración de la información ya sea de manera intencional o no autorizada o de manera casual 3.-Disponibilidad, que se refiere a que la información pueda ser consultada en todo momento que el usuario lo requiera sin que haya negación del servicio.

Debido a lo anterior se empiezan a considerar métodos que permitan tener una integridad en los datos y que la información sólo sea legible por las personas autorizadas para ello; de esta manera las telecomunicaciones tienen que hacer uso de técnicas que le permitan dicho fin, como lo es la criptografía. La criptografía surge con el propósito de mantener oculta la información y que permanezca secreta durante su generación, transportación o almacenamiento. Esta ciencia tuvo su mayor desarrollo durante las guerras mundiales, en las cuales se buscaba establecer comunicaciones secretas entre militares. Se trata de hacer que las telecomunicaciones sean seguras y que la información que viaja por ellas no sea alterada.

Sin embargo el hombre no sólo exige que su información sea segura también pide que sea legible en su totalidad, enfoquémonos en lo que fue el principio de las comunicaciones, la voz. En un sistema de telecomunicaciones por medio del cual se pretende transmitir voz, se busca que dicho sistema no altere las propiedades elementales de la señal de voz, el hombre no puede pasar por alto ruidos o interferencias cuando establece una conversación, por lo cual se ha

buscado mejorar los sistemas de telecomunicaciones pero cuidando siempre la calidad de la señal lo cual se traduce a una mejor calidad de voz.

Es por eso que en todo sistema de comunicaciones se debe tratar que tanto en el emisor como el receptor la información que se transmite por los dos sea compatible, de no ser así alguno de los dos tendrá que hacer la operación de traducción o codificación. La codificación es la acción en la cual un sistema interpreta de manera adecuada por medio de un protocolo toda la información que le llega y dependiendo de la complejidad del sistema puede tener subsistemas de comprobación de errores e integridad de la información.

A través del tiempo estos sistemas de comprobación de la integridad de la información han cambiado a tal grado que hoy en día no se puede entablar una comunicación entre dos dispositivos si no existe antes una serie de pasos que aseguren esta comunicación, de no ser así dicha comunicación no se establece.

Otro aspecto que ha marcado al mundo de la comunicaciones es la capacidad de poder enviar por un solo par de alambres más de un canal de información, estamos hablando de la llamada multiplexación que es una técnica que nos permite enviar por ejemplo hasta 30 conversaciones por un solo par de alambres al mismo tiempo sin que haya ningún tipo de interferencia entre ellas, es una técnica de vital importancia, sin ella se tendría que poner 30 pares de alambres para poder así tener 30 conversaciones, lo cual se traduce en mayores costos así como de la utilización de espacio físicos importantes.

Así con este panorama introductorio se ha comenzado a plantear el contenido del diplomado Integral de Telecomunicaciones el cual se desarrolla en 12 módulos en los que se estudiaron con profundidad los temas antes mencionados. Es precisamente este módulo introductorio el que nos permite dar cuenta de que son las telecomunicaciones y su importancia en la vida cotidiana.

## MÓDULO II

## NORMATIVIDAD Y REGULACIÓN DE LAS TELECOMUNICACIONES

Este módulo fue de gran importancia ya que por medio de él pudimos darnos cuenta como es que el mercado de las telecomunicaciones se encuentra actualmente, como es regulado a nivel mundial y el por que los países deben someterse a esta regularización para poder garantizar que su sector de telecomunicaciones cuente con los requerimientos de calidad necesarios para poder tener una buena interconexión en sus redes y así estar comunicado con los demás países del mundo.

El sector de las telecomunicaciones ha llegado a ser una actividad internacional en la cual los países se han integrado paulatinamente siendo este sector un motor clave para su crecimiento económico ya que permiten acortar tiempos y distancias. Sin embargo para poder lograr la llamada globalización de las telecomunicaciones los países han tenido que recurrir a realizar diversas reformas en su marco normativo. Todo parte de las privatizaciones que se han llevado acabo de las redes de comunicaciones. Son las privatizaciones las que han permitido que se realicen alianzas estratégicas, fusiones y que haya competencia entre los prestadores de servicios de comunicaciones y que éstos a su vez inviertan en este sector.

### ➢ Organismos reguladores de telecomunicaciones en México y a nivel mundial

El estado ha dejado de ser un prestador de servicios de telecomunicaciones denegando esta actividad al sector privado, sin embargo ha conservado la tarea de establecer políticas públicas y regular los servicios de telecomunicaciones para lo cual ha creado organismos, leyes y reglamentos. En la mayoría de los países existe un organismo regulador el cual es el encargado de llevar a cabo el otorgamiento de concesiones o licencias, emite regulaciones, planes fundamentales y normalización, establece políticas tarifarias, define políticas de interconexión de redes, administra el espectro electromagnético y se encarga de asuntos internacionales en materia de telecomunicaciones.

En México todo este proceso inicia a principios de los 90´s con la privatización de Telmex, con lo cual se busca que el sector cuente con los recursos financieros necesarios para poder adquirir nueva tecnología y de esta manera el sector pueda cubrir las necesidades de la sociedad. Con la privatización de la red de telefonía se buscaba que en el mercado hubiera varios competidores los cuales brindarían un buen servicio, que la red de telefonía pudiera llegar a lugares en donde por la falta de inversión antes no era posible. La privatización de la red de telefonía mexicana buscaba dar un impulso a la competencia, que hubiera en el mercado varias empresas de telecomunicaciones lo que provocaría el abaratamiento del servicio; sin embargo no podemos decir que estos objetivos se hayan cumplido pues aunque existen competidores como Axtel o Maxcom, Telmex sigue siendo el operador dominante en el país.

México tardo cerca de 3 años en fijar las reglas que deberían de regir el sector de las redes de telecomunicaciones, es hasta 1995 cuando se decreta la ley federal de Telecomunicaciones y se crea a su vez el organismo regulador de las mismas en el país. Es importante recalcar que en esta ley se deja claro que el estado es el rector que rige dicho sector, que en todo momento será el estado el encargo de definir las políticas públicas que lo rijan. De igual manera se define los conceptos básicos de las telecomunicaciones y se deja de manifiesto lo que es una red pública de telecomunicaciones quedando definida como: *un sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario*[1].

[1] Ley Federal de Telecomunicaciones, México 1995

En México la COFETEL (Comisión Federal de Telecomunicaciones) es la encargada de regular las telecomunicaciones, sin embargo esto no ha sido del todo posible debido a que no cuenta con un marco normativo que le brinde auténtica autonomía de gestión. Por lo anterior no es raro encontrar que existan varias irregularidades en este sector y que aún exista el monopolio dominante en el sector telefónico.

Hay un aspecto importante que no puede dejar de mencionarse y que tiene que ver con los objetivos que persigue el mercado de las telecomunicaciones, la interconectividad de redes. Es el propósito que incluso en el caso de México se persigue y que el organismo regulador debe de propiciar, estableciendo las reglas para que todos los operadores de telecomunicaciones puedan interconectar sus redes siempre y cuando cumplan con las normas internacionales de calidad e interoperabilidad; no puede existir ningún prestador de servicios públicos de telecomunicaciones que no admita o que no desee la interconexión ya que ésta es la tendencia mundial.

A nivel mundial se han creado diversos organismos que buscan regular este mercado. Se entiende por organismos o foros de regulación aquellos en los que los países trabajan para lograr la coordinación y armonización técnico-legal, (conceptos, definiciones, normas y reglamentación) necesaria para la adecuada prestación de los servicios de telecomunicaciones. Entre los más importantes que podemos mencionar se encuentran:

*La UIT (La Unión Internacional de Telecomunicaciones)*

Es el organismo intergubernamental especializado de la Organización de las Naciones Unidas (ONU). Cuenta con 189 miembros y tiene su sede en Ginebra, Suiza. Elabora reglamentos y normas de telecomunicaciones con miras a garantizar el funcionamiento y la interconectividad mundial de las redes de telecomunicaciones, garantizar una utilización racional y eficaz del espectro de frecuencias radioeléctricas y de la órbita de los satélites geoestacionarios.

Elabora normas mundiales de telecomunicaciones para garantizar el diseño, la modernización y el crecimiento armonioso de las redes mundiales de telecomunicaciones. Armoniza los estudios técnicos encaminados a la introducción de nuevas tecnologías, técnicas y servicios. Promueve además la conectividad mundial a la infraestructura de telecomunicaciones. México es miembro del Consejo ininterrumpidamente desde el año 1952.

La UIT está conformada en dos grandes bloques, una representada por las Conferencias, que son los foros en los que se toman todas las decisiones y otra, que es la Secretaría, la cual está encargada del funcionamiento de la UIT.

Se compone además de tres sectores: Radiocomunicaciones (UIT-R), Normalización (UIT-T) y Desarrollo (UITD). Estos tres sectores realizan conferencias periódicamente.

En la Conferencia Mundial de Radiocomunicaciones los países acuerdan el futuro uso del espectro radioeléctrico y las orbitas satelitales y actualiza el Reglamento de Radiocomunicaciones (Cuadro Internacional de Atribución de Frecuencias). Se busca garantizar la utilización racional, equitativa, eficaz y económica del espectro de frecuencias radioeléctricas para todos los servicios de radiocomunicaciones, incluidos los que utilizan la órbita de los satélites geoestacionarios u otras órbitas, y realizar estudios sobre radiocomunicaciones.

En las Asambleas de Normalización se aprueban el programa de trabajo de la UIT-T, determinando las prioridades de los trabajos referentes a estándares técnicos.

En la conferencia de Desarrollo se fijan los objetivos y las estrategias para el desarrollo mundial y regional de telecomunicaciones, dando prioridad a la extensión, la modernización de redes y la asignación de los recursos para elevar la penetración.

Al formar parte del Convenio de la UIT los estados se obligan a cumplir con lo que ahí se acuerde. Considerando la Ley sobre la Celebración de Tratados, en México este convenio tiene rango jurídico de ley.

*CITEL (Comisión Interamericana de Telecomunicaciones)*

Es la entidad de la Organización de los Estados Americanos (OEA), encargada del facilitar y promover el desarrollo de las telecomunicaciones en la región. La OEA/CITEL agrupa a 34 estados miembros y más de 200 miembros asociados. México es miembro de la OEA desde 1948, e influyó directamente en la creación de CITEL en 1959 a través de la llamada Red Interamericana de Telecomunicaciones, con el fin de adelantar estudios regionales antes de llegar las Conferencias de la UIT.

La importancia de participar en CITEL radica en la oportunidad de encontrarse con países con niveles de desarrollo económico e intereses similares, asigna posiciones orbitales nacionales, lleva a cabo los procedimientos de coordinación internacional ante la UIT.

- **Los organismos internacionales de cooperación**

Los foros de cooperación son creados para que los países intercambien principalmente información sobre nuevas corrientes en el diseño de los programas de desarrollo del sector, la implementación de nuevas tecnologías, los resultados de la adopción de cierta regulación, capacitación de recursos humanos y el diseño de recomendaciones para los foros de regulación, comercio y financieros. Los foros de cooperación pueden ser multilaterales o bilaterales. Entre los foros más importantes se encuentran:

**- APEC** (Asia-Pacific Economic Cooperation). Es un foro gubernamental de cooperación en materia económica, "no vinculante", establecido en 1989. Entre sus objetivos está el de mantener el crecimiento económico y el desarrollo de la región, a través del sistema multilateral de comercio, reducir las barreras al comercio de bienes, servicios y flujos de inversión. La APEC cuenta con instancias donde se discuten temas del sector de telecomunicaciones y servicios de información, como lo son APEC-TEL y TELEMIN para logar el desarrollo del sector en cada uno de los miembros integrantes.

**- OCDE.** La Organización de Cooperación para el Desarrollo Económico (OCDE) es un organismo internacional de carácter gubernamental en el que sus miembros analizan e intercambian experiencias sobre temas de interés común. Para tratar el tema de las Tecnologías de la Información y las Comunicaciones se encuentra el Comité de Políticas de Información, Informática y Comunicaciones (ICCP), el cual fue creado el 1 de abril de 1982 que examina los temas de política derivados del desarrollo y aplicación de las tecnologías en el campo de la información, computación y sistemas y servicios de comunicación, incluyendo su impacto en la economía y en la sociedad en general. Derivado de este comité se han creado los siguientes cuatro Grupos de Trabajo:

- *Grupo de Trabajo sobre Políticas de Telecomunicaciones y Servicios de Información* (WPTISP). Examina los temas relacionados con la regulación de las telecomunicaciones, así como, el análisis y solución de los problemas derivados de la apertura del mercado de telecomunicaciones en los países miembros.

- *Grupo de Trabajo sobre Economía de la Información* (WPIE). Analiza los marcos de política para la economía de la información, requeridos para fortalecer el crecimiento económico, la productividad, el empleo y la competitividad industrial en conjunto con el despliegue de una nueva Infraestructura Informática Global, de comercio electrónico y de la Sociedad Global de la Información.

- *Grupo de Trabajo sobre Seguridad y Confidencialidad de la Información* (WPISP). Tiene como objetivo favorecer el Intercambio de experiencias entre países miembros respecto a la seguridad de la información y de los sistemas de comunicaciones, así como la protección de datos personales y confidencialidad.

- *Grupo de Trabajo sobre Indicadores para la Sociedad de la Información* (WPIIS). Tiene como objetivo monitorear, supervisar, dirigir y coordinar el trabajo estadístico y contribuir al desarrollo de indicadores y análisis cuantitativos.

**- Tratados de libre comercio.** Los TLC´s son mecanismos de negociación comercial que fomentan el comercio y la inversión como medio para impulsar la producción. Permite el acceso preferencial a los mercados y brinda certidumbre jurídica que permite que fluya inversión extranjera. La estructura de los TLC´s reglamentan los plazos y condiciones en que se eliminan aranceles a los productos industriales, agrícolas y agroindustriales.

La mayoría de los tratados de libre comercio, incluyen un capítulo dedicado a las telecomunicaciones, dentro de su apartado de comercio de servicios. En algunos TLC´s no se incluyó el sector de telecomunicaciones debido a que, en su momento, no se habían llevado a cabo reformas para la liberalización de las telecomunicaciones. Los capítulos sobre telecomunicaciones tienen como ámbito y alcance de aplicación tres puntos fundamentales:

1. *Acceso y uso de redes*. Con esto se busca la flexibilidad de conexión a las redes y la transparencia para su uso, evitando tratos discriminatorios para quienes las utilicen.

2. *La prestación de los servicios de valor agregado*. Se reconoce a estos servicios como un elemento de primer orden para la competitividad de los negocios y su liberalización.

3. *La normalización para el equipo terminal*. Flexibilidad para la conexión del equipo terminal a las redes públicas de telecomunicaciones, tomando en cuenta el evitar daños técnicos a las propias redes, interferencias y aspectos de seguridad al público usuario.

Habiendo mencionado las características generales de los organismos internacionales que tienen como propósito la regularización del sector de las telecomunicaciones se mencionarán ahora en los próximos módulos los aspectos teóricos y prácticos que hacen posible que existan las redes de telecomunicaciones.

## MÓDULO III

## MEDIOS DE TRANSMISIÓN ALÁMBRICOS

Ya pudimos ver de manera general como es que las telecomunicaciones son importantes para el ser humano, como es que han evolucionado y porque gracias a la ciencia hoy en día es posible entablar una comunicación a grandes distancias. Se ha visto que a nivel mundial existen organismos que regulan el mundo de las telecomunicaciones. Este módulo tuvo como objetivo darnos a conocer los diferentes medios físicos por medio de los cuales los equipos de telecomunicaciones pueden ser interconectados.

El primer elemento de vital importancia para lograr la interconexión de los diferentes dispositivos de telecomunicaciones es el cable de cobre, el elemento básico es el par de cobre usado generalmente en la telefónica convencional.

Todo cable de cobre está determinado por su calibre, el cual es llamado también por sus siglas en ingles AWG (American Wire Gauge) y que determina el diámetro (grosor) del cable. Esta medida puede ser engañosa ya que sí su valor es mayor no quiere decir que el cable tenga un mayor diámetro pues al contrario a un valor mayor de AWG el cable será más delgado y viceversa entre menor sea su valor de AWG mayor será el diámetro del cable.

Por otra parte, es importante recalcar que los cables de cobre como todo elemento conductor de electricidad está propenso a variables físicas que afectan su funcionamiento como lo es la resistencia, la capacitancia y la inductancia, que son fenómenos que se presentan a nivel de conductores eléctricos; sin embargo hay factores que también repercuten en el buen desempeño de los cables, factores como lo son las interferencias electromagnéticas provocadas por elementos externos al sistema, temperatura y condiciones ambientales.

Lo anterior son factores importantes que debemos tomar en cuenta al momento de seleccionar un cable, debido a la diversidad de ambientes así como de sistemas existen diferentes tipos de cables que son fabricados para cubrir alguna necesidad en especial, por ejemplo cables que son para ambientes de mucho ruido, otros para exteriores que viajan sobre los postes como los son los autosoportados, otros tantos que poseen aislante o recubrimiento de polietileno para alta temperaturas, algunos que son multipares y que pueden contener hasta 2400 pares, entre muchos otros.

### ➢ Cable UTP

El cable UTP es el más usado en redes de datos LAN, además que se pretende que sea utilizado en las redes de voz debido a su convergencia con los datos. El cable UTP se divide en las siguientes categorías (Cat) dependiendo de características como lo es la velocidad a la cual transmiten:

- *Categoría 1*: cable de teléfono tradicional (transmisión de voz pero no de datos), tiene 1 KHz. de ancho de banda.

- *Categoría 2*: transmisión de datos hasta un máximo de 4 Mb/s. Este tipo de cable contiene 4 pares trenzados, 1 MHz. de ancho de banda.

- *Categoría 3*: máximo de hasta 10 Mb/s. Este tipo de cable contiene 4 pares trenzados y 3 trenzas por pie, 16 MHz. de ancho de banda.

- *Categoría 4*: máximo de hasta 16 Mb/s. Este tipo de cable contiene 4 pares de hilos de cobre

trenzados. 20 MHz. de ancho de banda.

- *Categoría 5*: máximo de hasta 100 Mb/s. Este tipo de cable contiene 4 pares de hilos de cobre trenzados. 100 MHz. de ancho de banda.

- *Categoría 5e*: máximo de hasta 1000 Mb/s. Este tipo de cable contiene 4 pares de hilos de cobre trenzados. 100 MHz. de ancho de banda.

El cable UTP cumple con la especificación X BaseT en donde la X pude ser 10, 100, o 1000 que indica la velocidad de datos en Mbps, la palabra base indica que la red es banda base es decir sólo transporta una seña a la vez y T significa que se trata de un cable de par trenzado.

Es conveniente aclarar que hoy en día la categoría de cable UTP que se encuentra estandarizado es la categoría 6 con un ancho de banda de 250 MHz. y con una transmisión de datos de hasta 10 Gbps; sin embargo en el mercado existen categorías como la Cat 6A (500MHz.), Cat 7 (600MHz.) e incluso Cat 7A (1000MHz.) que aún no se encuentran estandarizadas.

Existen otros tipos de cables que son usados para la instalación de redes de datos los cuales cuentan con blindaje que permite reducir las interferencias causadas por fenómenos externos. Entre este tipo de cables podemos mencionar el cable FTP (Foiled Twisted Pair*),* el cual es un cable que contiene múltiples pares de cobre en una envoltura de aluminio. La desventaja del cable FTP es que requiere de un muy buen aterrizaje a tierra. Fig 3.1. El otro tipo de cable utilizado es el STP (Shielded Twisted Pair), en un cable STP cada par trenzado está envuelto en una lámina y colocado justo a continuación de la malla metálica del blindaje. Estos componentes reducen las interferencias externas, las interferencias entre pares y la emisión de señales producidas por las corrientes que circulan por el cable cuando el blindaje está adecuadamente aterrizado.

Fig.3.1 Cable FTP

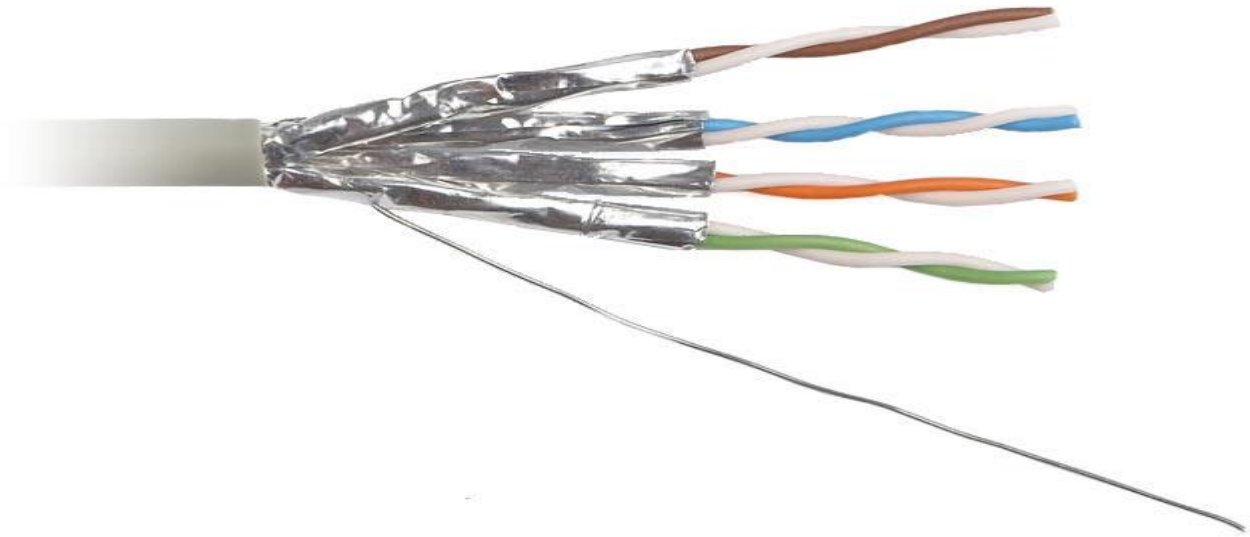


Fig.3.2 Cable STP

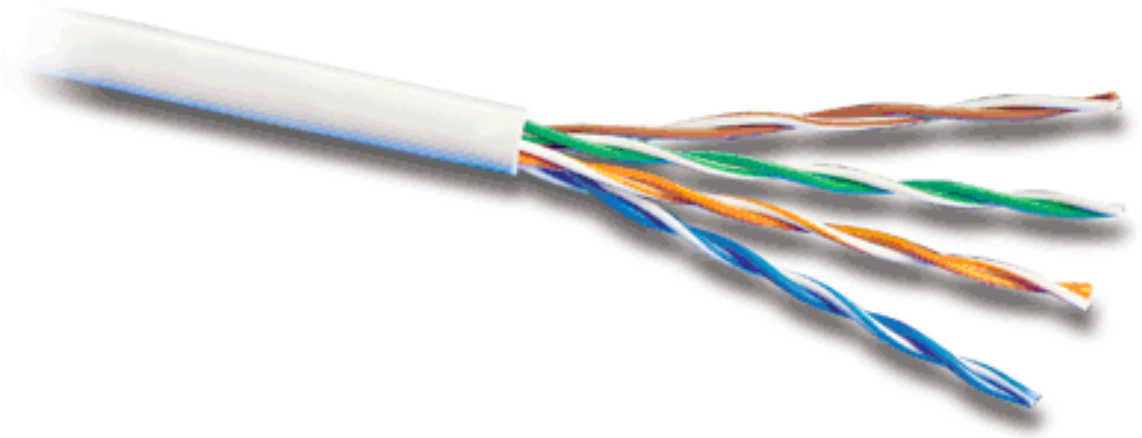


Fig. 3.3 Cable UTP

- **Fibra Óptica**

Otro de los elementos que se estudió en este módulo y que nos permiten hacer la interconexión entre los diferentes dispositivos de red es la fibra óptica; la fibra óptica se puede considerar como una guía de onda dieléctrica, es decir es un tubo de vidrio macizo muy pequeño, en dos capas, integrada por un núcleo y un revestimiento. El principio de operación se basa en los fenómenos de reflexión y refracción de la luz. Cuenta con las siguientes características:

- No es conductiva
- No requiere conexión a tierra
- Tiene la capacidad de manejar mayor capacidad de datos
- Su costo de instalación es menor
- No es propensa a interferencias debido a radiaciones electromagnéticas
- Mayor ancho de banda

Existen de manera general 2 tipos de fibra: monomodo y multimodo.

Una *fibra multimodo* es aquella en la que el haz de luz puede circular por más de un modo o camino. Esto supone que no llegan todos a la vez. Una fibra multimodo puede tener más de mil modos de propagación de luz, se usan comúnmente en aplicaciones de corta distancia, menores a 1 km; el núcleo de una fibra multimodo tiene un índice de refracción superior, pero del mismo orden de magnitud, que el revestimiento. Debido al gran tamaño del núcleo de una fibra multimodo, es más fácil de conectar y tiene una mayor tolerancia a componentes de menor precisión.

Una *fibra monomodo* es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micras) que sólo permite un modo de propagación. Su transmisión es paralela al eje de la fibra. Las fibras monomodo permiten alcanzar grandes distancias (hasta 100 Km. máximo, mediante un láser de alta intensidad).

Dependiendo el tipo de índice de refracción del núcleo, tenemos dos tipos de índices de refracción:

1. Fibras de índice gradual.- El índice de refracción es constante en el revestimiento, pero en el núcleo varía gradualmente (en forma parabólica) y se tiene un máximo en el centro del núcleo. Este tipo de perfil es utilizado en las fibras multimodo pues disminuye la dispersión de las señales al variar la velocidad para las distintas longitudes de los caminos en el centro y próximos a la frontera. En la figura 3.4 se ilustra el fenómeno.

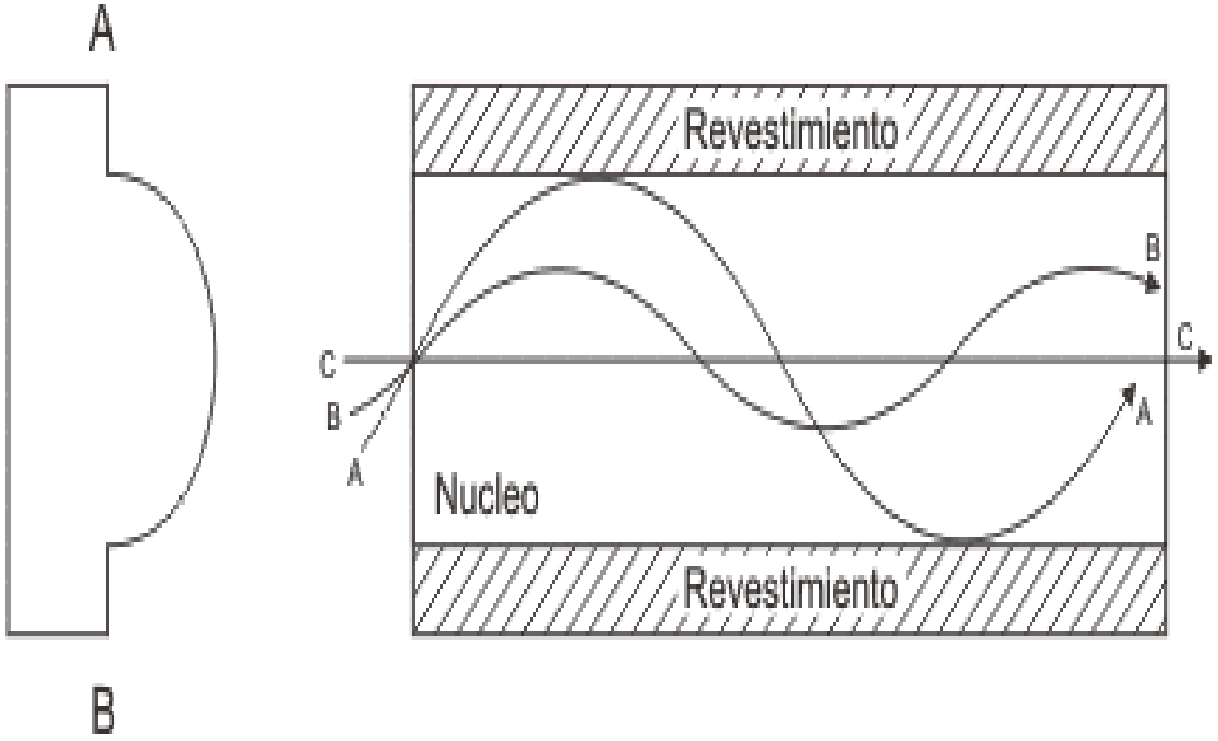



Fig. 3.4 Índice gradual

2. Fibras de índice escalón o también llamadas salto de índice (SI), son aquellas en las que el índice de refracción toma un valor constante desde el punto A hasta el punto donde termina el revestimiento y empieza el núcleo. Este tipo de perfil es utilizado en las fibras monomodo. Como se muestra en la figura.

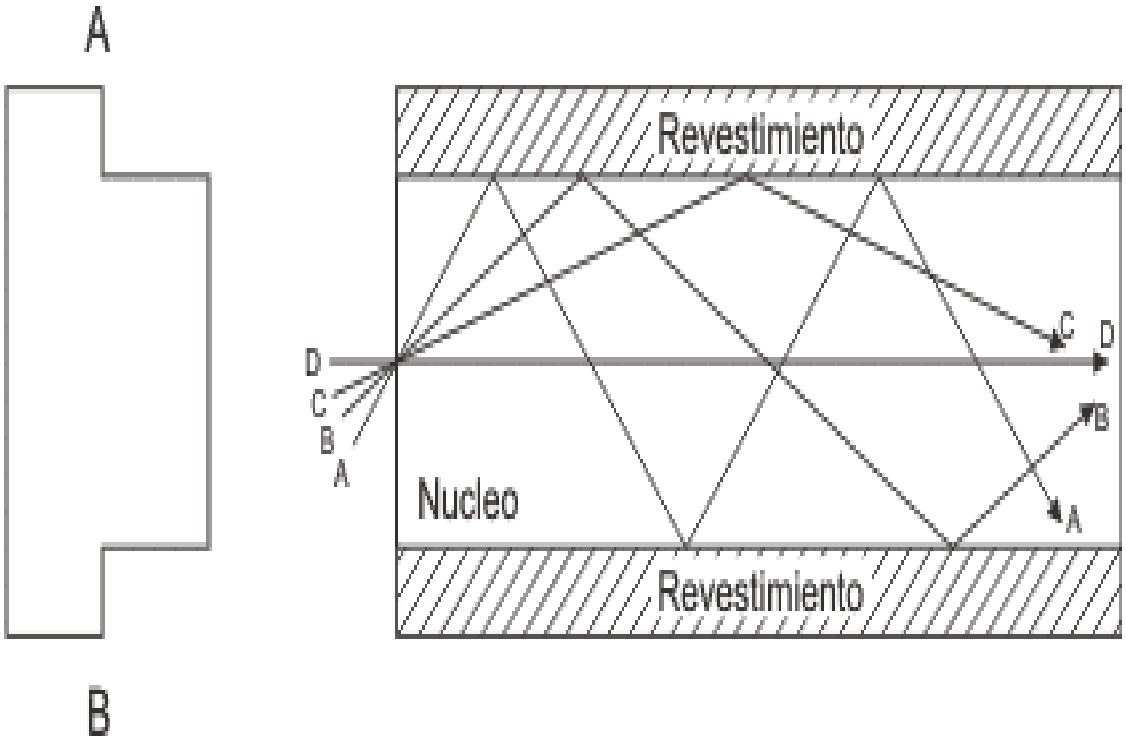



Fig. 3.5 Índice escalón

En las fibras de índice escalón multimodo la dispersión del haz de luz ocasionado por retardo de los distintos caminos de los modos de propagación, limita en ancho de banda.

Existe otro parámetro importante que caracteriza a una fibra óptica, la Apertura Numérica (NA). Es un parámetro que da idea de la cantidad de luz que puede ser guiada por una fibra óptica. Por lo tanto cuanto mayor es la magnitud de la apertura numérica de una fibra, mayor es la cantidad de luz que puede guiar.

Por otro lado la fibra estará propensa a los siguientes fenómenos:

- *Dispersión cromática*. Es el fenómeno mediante el cual diferentes componentes espectrales de un pulso luminoso viajan a diferentes velocidades. Es el principal fenómeno que limita el ancho de banda de los sistemas monomodo. Diferentes longitudes de onda viajan a diferentes velocidades en la fibra óptica.

- *Atenuación*. Es el decremento de la potencia de una señal óptica desde la entrada hasta la salida.

- **Métodos de prueba en el cableado**

Son varias las pruebas y mediciones que se deben de realizar para garantizar la correcta instalación de un cableado estructurado. En todo momento el cableado de datos debe estar separado del cableado eléctrico. Entre los aspectos importantes a medir en un cableado estructurado se encuentran:

- *Atenuación.* Es la perdida de una señal mientras viaja a través de un cableado. Es la diferencia entre la señal de entrada y la señal de salida. Mientras más atenuación se tenga, menor es la señal que se tiene en el receptor.

- *NEXT* (NEAR-END-CROSSTALK). Es una medida de señal que es electromagnéticamente acoplada de un circuito a otro. Se mide transmitiendo una señal por medio de un par y midiendo la señal acoplada en el otro par. Es importante medirla a lo largo de un número de frecuencias, típicamente de 1-100 Mhz. para Cat 5e y hasta 250 MHz. para Cat 6. El Next generalmente se presenta por malas conexiones, demasiado destorcido en el cable y eventualmente por la presencia de cordones de parcheo de baja categoría o mala calidad. La unidad de medida es el dB (decibel).

- *FEXT* (FAR END CROSSTALK). Se aplica la señal de prueba, y se mide la señal inducida en otro par, pero en el otro extremo del cable. Debido a la atenuación, la diafonía que ocurre a mayor distancia del transmisor genera menos ruido en un cable que la NEXT. A esto se le conoce como telediafonía, o FEXT. El ruido causado por FEXT también regresa a la fuente, pero se va atenuando en el trayecto.

- *ELFEXT* (EQUAL LEVEL FAR END CROSSTALK). Es una medida del acoplamiento de una señal no deseada de un transmisor en el extremo cercano, dentro de un par medido en el extremo lejano, y relativo al nivel de señal recibida.

- *ACR.* Es la diferencia entre el Next y la atenuación en el par del enlace que está siendo probado. Determina la calidad de la transmisión en el cableado y es la relación entre la atenuación y NEXT (la atenuación de la diafonía del extremo cercano o paradiafonía). El valor de ACR ha de ser lo mayor posible -debe superar un mínimo-, ya que eso implica una NEXT elevada y una baja atenuación.

- *Power sum*. Consiste en realizar cualquiera las mediciones de NEXT, ELFENEXT y ACR, pero en vez de hacerlo de un par contra un par como se hacía tradicionalmente, se realiza la medición de un par contra los tres restantes y así sucesivamente.

- *Propagación delay.* Es una medida del tiempo requerido por una señal para propagarse desde el extremo de un circuito a otro. Su unidad de medida es el nS (nanosegundo).

- *Propagación* (DELAY SKEW). Es la diferencia que hay entre el retardo de propagación de los pares más rápidos contra los pares más lentos de un cable. En un enlace de 100 mts se debe tener un skew menor a 50 nS.

- *Perdidas de retorno* (RETURN LOSS). Es la relación entre lo que se emite por un par y lo que vuelve por el mismo par, debido a rebotes en los empalmes. Esta pérdida debe ser lo más alta posible. Se mide en dB.

- *Alien crosstalk.* Interferencia entre cables adyacentes.

Ya hemos visto las diversas pruebas que se deben realizar al cableado para garantizar que exista una buena comunicación entre nuestros equipos de red, sin embargo también se deben considerar aspectos importantes en el cuarto de telecomunicaciones como lo son tener un buen aterrizaje a tierra tanto del equipo de telecomunicaciones como del rack y escalerillas; en el cuarto de telecomunicaciones debe existir un aire acondicionado que permita mantener una temperatura de entre 18 y 24 °C, debe contar con sistemas de respaldo de energía UPS para garantizar así que el equipo de telecomunicaciones no sufra ninguna pérdida de alimentación eléctrica.

## MÓDULO IV

## REDES DE DATOS Y TECNOLOGÍAS DE TRANSPORTE

En este módulo se estudió los diferentes elementos por medio de los cuales es posible entablar una comunicación entre los diferentes dispositivos de una red de datos.

- **Redes de datos fundamentos básicos**

Una red de datos es un conjunto de computadoras y/o equipos de cómputo conectados por un medio físico ó inalámbrico, que comparten recursos físicos y lógicos.

Cuando la transmisión de los datos se realiza en un solo sentido se dice que es una transmisión *Simplex*, cuando se realiza en ambos sentido pero no al mismo tiempo se dice que es una transmisión ***Half-duplex***, y cuando se realiza la transmisión en ambos sentidos de forma simultánea se dice que es una transmisión ***Full-duplex***.

Por otra parte dependiendo el número de destinatarios a los cuales los datos van dirigidos las transmisiones se clasifican en Unicast (un solo destinatario en concreto), Broadcast (todos los destinatarios posibles), Multicast (se envían paquetes a un determinado grupo de destinatarios).

Las redes de datos se pueden clasificar a su vez dependiendo de la cobertura que tengan en una área geográfica, existen redes de área personal llamadas PAN generalmente cubren distancia menores a 10 metros, como lo son los infrarrojos o bluetooth; redes de área local LAN las cuales normalmente cubren pequeñas empresas o edificios; redes MAN que se extienden a áreas más grandes como ciudades; y las redes WAN que cubre redes amplias como lo pueden ser países o continentes.

Según el tipo de conmutación existen dos tipos de redes: 1.- La red conmutada por circuitos en la cual se reserva una trayectoria (se crea un circuito) entre los usuarios y se mantendrá sólo mientras se realice la transmisión, por ejemplo la red pública de telefonía. 2.- Red conmutada por paquetes, en esta red el mensaje se divide en pequeños paquetes a cada uno se le agrega información de control y así los paquetes circulan de nodo en nodo, al llegar a su destino se regeneran los paquetes y se establecerá la comunicación.

Dependiendo la forma de interconexión de las redes éstas pueden tener diversas topologías tanto de forma física como lógica, la topología física determina la forma en la que los nodos de red están realmente conectados entre sí; mientras que la topología lógica determina la forma como los nodos acceden al medio físico. En la figura 4.1 se muestran dichas topologías.

Entre las características más importantes de estas topologías encontramos:

- *Topología estrella*. Todos los dispositivos están conectados a un nodo central, si el nodo central falla, toda la red se desconecta.

- *Topología bus*. En esta topología todos los nodos de red están conectados a un cable, si algún nodo falla la red continua operando, si el bus falla la red deja de funcionar.

- *Topología anillo*. Es un conjunto de enlaces de punto a punto entre los elementos de la red, si un enlace se pierde o falla algún equipo la red deja de funcionar.

Se debe mencionar que pude haber topologías que son el resultado de la combinación de las anteriores como lo son las topologías en malla y jerárquica.

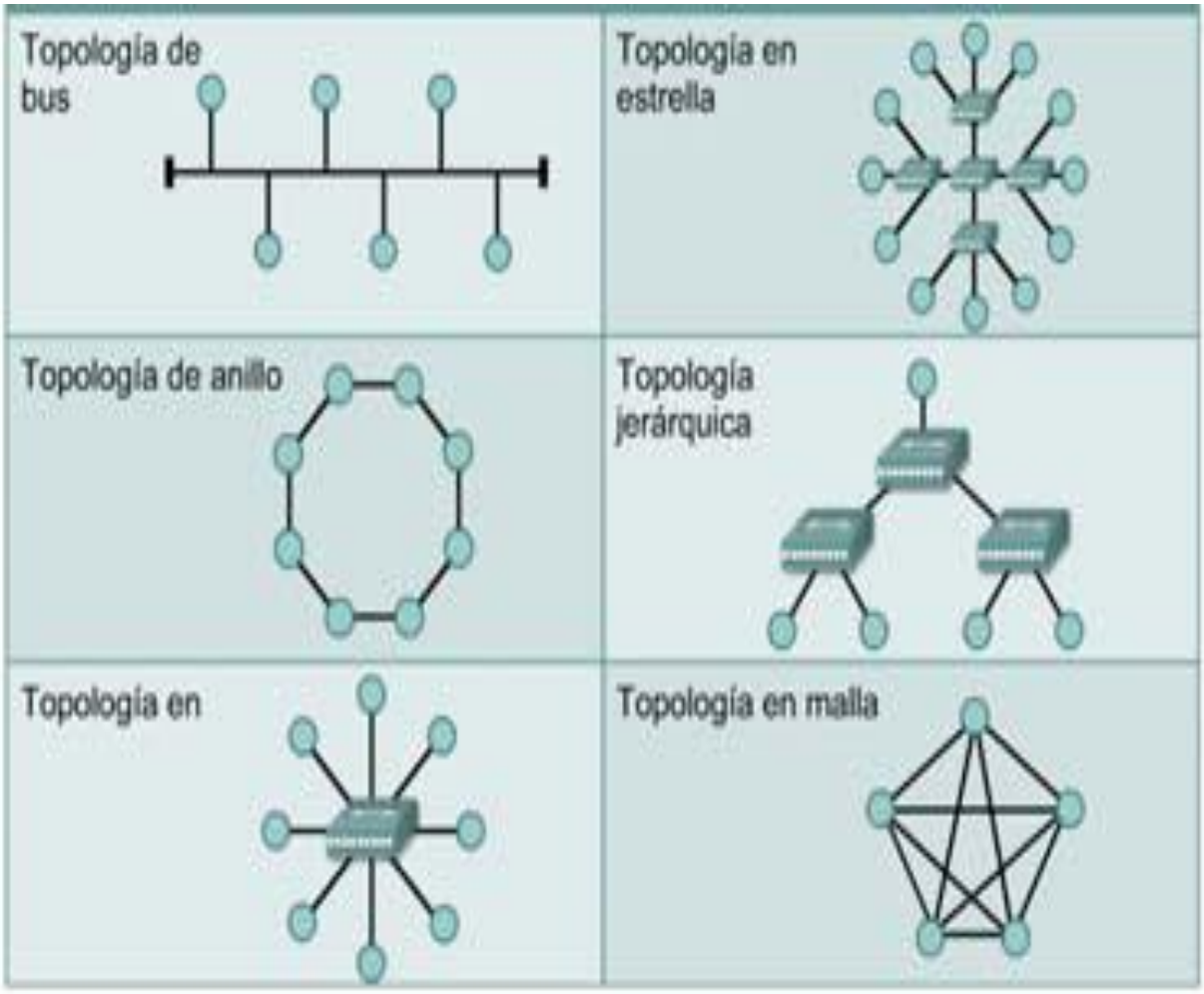



Fig. 4.1 Topologías de red

- **Modelo OSI**

El modelo OSI (Open System Interconnection) es un modelo de referencia que describe las reglas o manera en como la información en una computadora es transferida a una aplicación residente en otro equipo; organiza las funciones de la red en 7 capas.


Fig.4.2 Modelo OSI

1. *FISICA*.- Define características materiales y eléctricas, sincronización, medios de transmisión, codificación, especifica cables, conectores y componentes de interfaz con el medio de transmisión.
2. *ENLACE DE DATOS*.- 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, es donde se define la dirección MAC.
3. *RED*.- Define el direccionamiento lógico, identifica host en base a direcciones de red, es donde se determina que ruta seguirán los datos para llegar a su destino final, conoce la topología de red.
4. *TRANSPORTE*.- Segmenta los datos de la capa de sesión y los reensambla en el sistema receptor, establece y mantiene circuitos virtuales. Garantiza que se reciban todos los datos en orden correcto, hace acciones de detección y corrección de errores.
5. *SESIÓN*.- Inicia, mantiene y termina las sesiones entre las aplicaciones de los equipos en comunicación.
6. *PRESENTACIÓN*.- Traduce entre varios formatos de datos a un formato común de red, aplica procesos de cifrado cuando se requiera, comprime datos.
7. *APLICACIÓN*.-Proporciona servicios de red a las aplicaciones de usuario, abarca aplicaciones de HTTP, FTP, DNS etc.

En este modelo cuando se realiza la comunicación entre dos equipos cada capa sólo entablará comunicación con la capa igual que se encuentra en el otro equipo, es decir cada capa del modelo OSI sólo podrá interpretar la información que le envié su capa equivalente en el otro equipo.

- **Dispositivos de interconexión**

En toda red de datos es necesario contar con los dispositivos que nos permitan tener una interconexión hacia los demás dispositivos de red. El primer elemento que nos permite tener una interfaz entre nuestra estación y la red es la tarjeta de red la cual trabaja en la capa 2 del modelo OSI y tiene una dirección física única que le es asignada por el fabricante, esta dirección también es conocida como dirección MAC.

Se mencionarán ahora los elementos que permiten la interconexión a otras redes; los primeros dispositivos de este tipo eran los repetidores los cuales sólo se encargaban de regenerar la señal,

se encuentran también los hubs los cuales propagan la señal que recibe por un puerto en todos los demás que contiene, estos dos dispositivo prácticamente ya se encuentran en desuso.

Los bribges, son dispositivos que proporcionan conexiones entre LAN, trabajan en la capa 2 del modelo OSI, examinan las direcciones de origen y destino, si ambas direcciones pertenecen a diferentes segmentos se cruza el bridge, si los paquetes pertenecen al mismo segmento de red el bridge los descarta.

Los switch son otro dispositivos de red que se puede decir que son bridges multipuerto en los cuales se toman decisiones en base a direcciones físicas, conmutando los datos entre los puertos que requieren comunicarse, hoy en día es el dispositivo más usado ya que los switch pueden hacer labores multicapa pudiendo tener funciones de segmentación de la red y así evitar problemas de tráfico.

El router es un dispositivo que trabaja en la capa 3 del modelo OSI toma decisiones en base a direcciones de red es el encargado de encaminar los paquetes hacia su destino final y puede conectar diferentes tecnologías de LAN.

- **Tecnologías de Interconexión de Redes**

Hasta ahora se han mencionado los diferentes elementos que conforman una tecnología de red de datos IP, sin embargo existen otras tantas tecnologías que nos permiten realizar una interconexión de redes, estas tecnologías cuentan con características propias y elementos particulares.

Entre este tipo de tecnologías encontramos la X.25, que es un estándar para el acceso a redes públicas de conmutación de paquetes, es orientado a conexión (previamente a usar el servicio es necesario realizar una conexión y liberar la conexión cuando se deja de usar el servicio), fiable, en el sentido de que no duplica, ni pierde ni desordena (por ser orientado a conexión), y ofrece multiplexación por medio de TDM (multiplexación por división de tiempo) estadístico asíncrono, lo que quiere decir que a través de una única interfaz se mantienen abiertas distintas comunicaciones. Con X.25 no hay conexiones multipunto es un servicio punto a punto. X.25 utiliza circuitos virtuales permanentes para el envío de paquetes, opera en los niveles físico, enlace de datos y red del modelo OSI.

Entre otras de las tecnologías en WAN encontramos FRAME RELAY sus especificaciones fueron definidas por ANSI, fundamentalmente como medida para superar la lentitud de X.25, se define, como un servicio portador de servicios digitales de banda estrecha en modo de paquetes, y ha sido especialmente adaptado para velocidades de hasta 2,048 Mbps. Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un solo enlace a la red, opera en los niveles Físico y de Enlace de Datos del Modelo OSI.

Sin embargo existen tecnologías que por sus características son muy usadas hoy en día entre las cuales encontramos las siguientes:

- **ATM** (Asynchronous Transfer Mode). Al contrario de las redes sincrónicas en donde el ancho de banda se comparte (multiplexado) entre los usuarios, una red ATM transfiere datos de manera asíncrona, lo que significa que transmitirá los datos cuando pueda. Mientras que las redes sincrónicas no transmiten nada si el usuario no tiene nada para transmitir, la red ATM usará estos vacíos para transmitir otros datos, lo que garantiza un ancho de banda más óptimo.

Además, las redes ATM sólo transmiten paquetes en forma de celdas con una longitud de 53 bytes (5 bytes de encabezado y 48 bytes de datos) e incluyen identificadores que permiten dar a conocer la calidad del servicio (QoS), entre otras cosas. Por lo tanto, ATM posibilita la transferencia de datos a velocidades que van desde 25 Mbps a más de 622 Mbps.

- **MPLS** (Multi-Protocol Label Switching). Es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios Frame Relay o ATM. Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia todo ello en una única red. MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS). La idea de MPLS es realizar la conmutación de los paquetes o datagramas en función de las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por la QoS, lo cual a su vez permite ofrecer servicio multiprotocolo y ser portable sobre multitud de tecnologías de capa de enlace: ATM, Frame Relay, líneas dedicadas y LANs.

- **SDH**. Es el estándar internacional de comunicaciones aceptado por la UIT para redes de transmisión de alta capacidad. Tecnologías como ATM, IP/MPLS o ADSL se apoyan en SDH para lograr un mayor ancho de banda.

SDH y el equivalente norteamericano SONET son las tecnologías dominantes en la capa física de transporte de las actuales redes de fibra óptica de banda ancha. Esencialmente, SDH es un protocolo de transporte (primera capa en el modelo OSI) basado en la existencia de una referencia temporal común (reloj primario), que multiplexa diferentes señales dentro de una jerarquía común flexible, y gestiona su transmisión de forma eficiente a través de fibra óptica, con mecanismos internos de protección. SDH actúa como el portador físico de aplicaciones de nivel 2 a 4, permite el transporte de muchos tipos de tráfico tales como voz, video, multimedia, y paquetes de datos como los que genera IP.

Las recomendaciones de la UIT-T definen un número de tasas básicas, la primera de estas tasas es 155.52 Mbps, normalmente referidas como un STM-1 (donde STM significa Módulo de Transporte Síncrono). Mayores tasas de transmisión como el STM-4, el STM-16, y el STM-64 (622.08 Mbps, 2488.32 Mbps y 9953.28 Mbps respectivamente), también están definidas.

**DSL (Digital Suscriber Line Línea De Suscriptor Digital)**

La línea de suscriptor digital es una tecnología de transmisión de datos que permite interactuar con la red actual de telefonía utilizando el mismo cable de par trenzado. Las tecnologías de la familia DSL denominadas xDSL, son capaces ofrecer a los usuarios servicios de conexión de banda ancha a Internet.

Existe una clasificación para las líneas DSL, las líneas simétricas y las líneas asimétricas. Entre las líneas simétricas se encuentra:

- *HDSL* (High Rate DSL, DSL de alta frecuencia y tecnologías derivadas como HDSL2). Es capaz de transmitir y recibir datos de forma simétrica a velocidades de transferencia que pueden alcanzar los 2.048 Mbps. Utiliza tres pares de cable de cobre para funcionar y puede mantener la velocidad de transmisión si el usuario se encuentra a una distancia de hasta 4.5 Km. de la central. La diferencia con HDSL2, es que éste sólo necesita un par de cobre para obtener las mismas prestaciones.

- *SDSL* (Symmetric Single Pair SDLS, DSL de par simple simétrica). Utiliza un solo par de hilos de cobre para obtener velocidades de transmisión que alcanzan como máximo los 768 Kbps, sólo garantiza su funcionamiento hasta los 3 kilómetros.

- *IDSL* (Integrated Services Digital Network DSL, DSL de la Red Integrada de Servicios Digitales). Toma el acceso básico de la tecnología ISDN. Utiliza los mismos canales 2B+D y alcanza los 144 kbps. Funciona sobre un par de hilos y alcanza los 5.5 kilómetros.

- *SHDSL* (Single pair High Speed DSL, DSL de par simple de alta velocidad). Puede operar a distintas velocidades de conexión, desde 192 Kbps hasta 2,3 Mbps. Es posible hacer funcionar SHDSL tanto con un solo par de cobre como con dos, para aumentar la distancia máxima al nodo. Con dos pares de cobre es posible transmitir hasta 1,2 Mbps a una distancia de 6 kilómetros (según la calidad del cable).

Entras las líneas asimétricas encontramos las siguientes:

- *ADSL* (Asymetric DSL, DSL asimétrica). Opera en un rango de frecuencias que va desde los 24 KHz. hasta 1,100 KHz., aproximadamente. ADSL es la primera y actualmente la más popular de las tecnologías asimétricas. Gracias a que no es necesaria una velocidad igual tanto de bajada como de subida se tiene más ancho de banda de la red al cliente (downstream) que en la dirección cliente a red (upstream); esta tecnología permite distancias de hasta 5,5 Km. La velocidad de subida de datos en una ADSL puede ser desde 16 hasta los 768 Kbps. La velocidad de bajada varía dependiendo la distancia. Las velocidades de bajada en base a la distancia para ADSL son:

- 1.544 Mbps 5.5 km
- 2.048 Mbps 4.8 km
- 6.312 Mbps 3.6 km
- 8.448 Mbps 2.7 km

- *RADSL* (Rate Adaptive DSL, DSL de velocidad adaptable). Es una tecnología de conexión asimétrica que utiliza una técnica de prueba para comprobar la velocidad máxima de transmisión según la calidad de la línea. En sus demás características es prácticamente igual a ADSL.

- *ADSL G.Lite* (ADSL G.lite o simplemente G.lite). Se basa en ADSL, pero ocupa un ancho de banda medio dentro de la línea telefónica. Proporciona velocidades de bajada de datos de hasta 1,5 Mbp, y de subida de hasta 500 kbps.

- *VDSL* (Very High bit rate DSL, DSL de muy alta frecuencia de bits). Se suele utilizar para aplicaciones muy concretas. Funciona en distancias extremadamente cortas, hasta 50 metros, pero ofrece velocidades de conexión de hasta 26 Mbps. VDSL puede ser configurada tanto en modo simétrico como en modo asimétrico, con lo que puede adaptarse a la aplicación.

De esta manera nos damos cuenta que existen diversas tecnologías que nos permiten realizar la interconexión de las redes de datos, la elección de alguna de ellas dependerá del tipo de tráfico que se desea transmitir, así como de las prioridades de los datos y la calidad de servicio que se requiera.

## MÓDULO V

## INTERCONEXIÓN DE REDES
## Y PROTOCOLOS DE ENRUTAMIENTO

En este módulo profundizamos en el conocimiento acerca de las redes de datos Ethernet, cómo funcionan las redes de datos a nivel de capa 2 y 3, que dispositivos de usan para dicho fin y la forma en cómo se programan.

Prácticamente el módulo tuvo como objetivo responder a la pregunta ¿cómo es que se conectan 2 o más equipos en red?. Como ya se ha mencionado anteriormente todo equipo que desee conectarse a una red debe contar con una interfaz adecuada para dicho propósito, esta interfaz está representada por la tarjeta de red, todos los dispositivos de red cuentan un una dirección física, que es única en el mundo y que consta de 6 bytes los cuales son asignados por la IEEE y se representan comúnmente en forma hexadecimal.

08:00:20:8f:96:b3

Sin embargo el direccionamiento físico sólo es válido para equipos que se encuentran en una misma red, si nosotros quisiéramos conectarnos con otro equipo que se encuentra en otra red diferente no podríamos ya que el equipo de interconexión sólo conoce el direccionamiento físico de su red local. Así surge el concepto de direccionamiento lógico, el cual es asignado vía software al equipo y que comúnmente en redes TCP/IP es conocido como dirección IP. La dirección IP posee una longitud de 32 bits y nos brinda información del host y de la red a la que pertenece, por ejemplo:

10000100 11111000 11001100 00110001
132.248.204.49

Complementario a la dirección IP se encuentra la máscara de red que es otro parámetro que se debe configurar para determinar a qué red pertenece nuestro host, la máscara de red también determinará el número máximo de host que podremos conectar a la red. Se debe tener en claro que las mascaras se clasifican en clases de acuerdo al tipo de red que se aplican, así tenemos diferentes tipos de mascaras las cuales se muestran en el siguiente cuadro.

| Dirección Clase | Mascara Natural | Decimal |
|---|---|---|
| A | 255.0.0.0 | /8 |
| B | 255. 255.0.0 | /16 |
| C | 255. 255. 255.0 | /24 |

Lo que conduce a que se definan rangos de direccionamiento IP dependiendo del tipo de máscara que sea usado, por lo cual se ha definido las siguientes tipos de clases de direcciones IP, las cuales cubren un rango determinado y poseen una máscara particular.

CLASE A

| Rango | Decimal | Máscara Natural |
|---|---|---|
| | 0.0.0.0 - 127.255.255.255 | 255.0.0.0 |

CLASE B

| Rango | Decimal | Máscara |
|---|---|---|
| | 128.0.0.0 - 191.255.255.255 | 255.255.0.0 |

CLASE C

| Rango | Decimal | Máscara |
|---|---|---|
| | 192.0.0.0 - 223.255.255.255 | 255.255.255.0 |

CLASE D

| Decimal |
|---|
| 224.0.0.0 - 239.255.255.255 |

CLASE E

| Decimal |
|---|
| 240.0.0.0 - 255.255.255.255 |

Existen direcciones especiales que se deben tomar en cuenta, ya que no podrán ser usadas para montar alguna red, las direcciones son: 127.0.0.0 y la 127.0.0.1, las cuales son direcciones que se encuentran asignadas a nuestra propia interfaz de red. Por otra parte existen las llamadas direcciones no homologadas las cuales se han reservado para que sean asignadas a redes privadas, por lo cual no podrán ser asignadas a redes públicas, las direcciones no homologadas son: 10.0.0.0, 172.16.0.0 y 192.168.0.0.

¿Qué pasaría si se quisieran tener varias subredes dentro de una red privada y limitar el número de equipos dentro de esas subredes?, ante estos casos existe el llamado subneteo o VLSM (Variable Length Subnet Mask) el cual permite asignar direccionamiento de acuerdo a nuestras necesidades, variando el valor de la máscara de subred.

Ya que se ha asignado direcciones IP a la red, se mencionarán ahora los dispositivos que permiten la interconexión de nuestra red hacia las demás redes. El primer dispositivo que encontramos de esta categoría es el switch. El swicth es un dispositivo que trabaja en la capa 2 y algunos en la capa 3 del modelo OSI, provee ancho de banda dedicado en cada uno de sus puertos, segmenta el tráfico de colisiones (en otras palabras elimina las colisiones), aprende y genera una tabla de direcciones MAC de los dispositivos que “ve” por cada uno de sus puertos. El switch puede ser muticapa quiere decir que puede contener funcionalidades de ruteo, calidades de servicio, o control de tráfico, listas de control de acceso, etc; sin embargo la funcionalidad principal del switch multicapa es la creación de la llamadas vlan (virtual LAN) que nos permite segmentar la red para así evitar problemas de congestionamiento. Una característica importante en los switch multicapa es que cuentan con el estándar 802.1Q de la IEEE el cual establece el método para etiquetado de los frames de ethernet dentro de una VLAN que permite segmentar redes extensas, permitiendo seccionarlas en segmentos pequeños y así evitar grupos de broadcast demasiado extensos, además que proporciona seguridad y la funcionalidad de tagged que permite que por un solo puerto haya más de una vlan a la vez.

Fig. 5.1 Aspecto físico del switch

- **El router y protocolos de enrutamiento**

Hasta el momento ya se han mencionado los diferentes elementos que nos permiten formar nuestra red interna, sin embargo si nosotros quisiéramos conectarnos con otra red privada o tener por ejemplo una conexión hacia el mundo atreves de internet esto no podría llevarse a cabo con los elementos que hasta ahora se han mencionado, ya que necesitaremos un dispositivo que permita tener una intercomunicación hacia otras redes; es en donde entra en juego el ruteador.

Los ruteadores o routers son conmutadores de paquetes que operan en el nivel (capa) 3 del modelo OSI y tienen la función de interconectar redes LAN y WAN, proporcionando control de tráfico y filtrado de funciones, esto se logra por medio de protocolos, los cuales tiene la finalidad de establecer las reglas para que los routers puedan comunicarse entre sí. Dependiendo de las características del enlace que se desea será el tipo de protocolos que se use.

Los ruteadores son dispositivos programables por el usuario, en ellos se establece la ruta que seguirá los datos para llegar a su destino a través del direccionamiento IP, el enrutamiento más sencillo que podemos programar son rutas estáticas en las cuales sólo indicamos la dirección del siguiente router a donde deberá ir la información para llegar a su destino, éste otro router también estará programado para poder enviar la información a otro router y así sucesivamente hasta que el paquete llegue a su destino. Las rutas estáticas son recomendables para redes pequeñas.

Fig. 5.2 Aspecto físico del router

El enrutamiento dinámico en cambio es un tipo de enrutamiento que se ajusta en tiempo real a las circunstancias cambiantes de la red. Si hay cambios en la red, entonces se recalculan rutas enviando esta información a sus vecinos. En casos de fallas en las rutas preferidas ofrece rutas opcionales que convierte en preferentes mientras no se repare la falla. Existen diversos algoritmos

que permiten que los routes puedan actualizar sus tablas de enrutamiento, entre estos algoritmos encontramos:

- **Distance-Vector**. Es un algoritmo en el cual el ruteador mantiene una tabla (un vector) que almacena las mejores distancias conocidas a cada destino y las rutas a usar para cada destino. Se actualizan las tablas intercambiando información con los vecinos. El ruteador usa las tablas de sus vecinos y sus mediciones de las distancias para calcular una nueva tabla. Con este algoritmo hay una convergencia más lenta y es más fácil que caigan en loops de ruteo, pero requieren menor procesamiento y memoria.

- **Linck State**. Es un algoritmo que manda el estado de sus interfaces (enlaces) directamente conectadas a los demás ruteadores en su mismo dominio (zona), y si alguna sufre modificaciones, mandan actualizaciones, convergen más rápidamente y es difícil que caigan en loops de ruteo, pero requieren mayor procesamiento y memoria.

Como ya se mencionó es posible programar los ruteadores con protocolos que nos permitan establecer las rutas que nosotros deseemos, antes de mencionar que protocolos son, tenemos que definir algunos conceptos de ruteo básico.

METRICA. Son medidas asignadas a los anuncios de ruteo. Se obtienen al evaluar diferentes variables que intervienen en la determinación de la ruta más óptima hacia una red destino y depende del protocolo de ruteo. Las variables que se consideran para dicho fin son: número de saltos que hará el paquete para llegar a su destino, confiabilidad, ancho de banda (Bandwidth), carga o grado de ocupación del ruteador y la cantidad de tiempo requerido para mover un paquete.

DISTANCIA. Es otra medida utilizada para enviar un anuncio de ruteo hacia una red destino proveniente de dos o más protocolos de ruteo diferentes.

SISTEMA AUTÓNOMO. Es un grupo de redes IP que poseen una política de rutas propia e independiente, realiza su propia gestión del tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet.

Por último y tomando como base los conceptos anteriores se mencionarán las principales características de los protocolos de ruteo más usados en la programación. Los protocolos de ruteo pueden dividirse en dos grandes categorías: IGP (Interior GatewayProtocol) aquellos que se utilizan dentro de los sistemas autónomos (SA) y EGP (Exterior GatewayProtocol) aquellos que se utilizan entre los SA.

***RIP***

RIP es un protocolo de vector distancia IGP, busca su camino óptimo mediante el conteo de saltos, no tiene en cuenta datos tales como ancho de banda o congestión del enlace. RIP no permite más de quince saltos, El protocolo utiliza métricas fijas para comparar rutas alternativas. RIP v2 permite la implementación de VLSM.

***OSPF***

Es un protocolo de enrutamiento interior (IGP) para redes corporativas medianas y grandes, opera como protocolo de estado de enlace, e implementa el algoritmo de Dijkstra para calcular la ruta más corta a cada red de destino. Su métrica de enrutamiento es el costo de los enlaces, parámetro que se calcula en función del ancho de banda; por este motivo es de gran importancia la configuración del parámetro bandwidth en las interfaces que participan de este proceso de enrutamiento. Opera estableciendo relaciones de adyacencia con los dispositivos vecinos, a los

que envía periódicamente paquetes hello. Adicionalmente, cada vez que un enlace cambia de estado inunda la red con la notificación de este cambio. OSPF envía cada 30 minutos a los dispositivos vecinos (o adyacentes) una actualización conteniendo todos los cambios de estado de enlaces de ese período.

Converge con mayor velocidad que los protocolos de vector distancia. Sus actualizaciones son pequeñas ya que no envía toda la tabla de enrutamiento. No es propenso a bucles de enrutamiento. Utiliza el ancho de banda de los enlaces como base de la métrica, además soporta VLSM y brinda múltiples opciones de configuración lo que permite adaptarlo a requerimientos muy específicos.

***BGP***

Es un protocolo EGP mediante el cual se intercambian prefijos los ISP (proveedor de servicios de internet) 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.

La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando el Sistema Autónomo. Cada sistema autónomo (AS) tendrá conexiones o, mejor dicho, sesiones internas (iBGP) y además sesiones externas (eBGP). 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, no usa métricas como número de saltos, ancho de banda, o retardo, si no que toma decisiones de enrutamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP.

Con este protocolo se han mencionado los conceptos básicos que hacen posible que existan redes tan populares como los son la Ethernet sus protocolos, direccionamiento y equipos de interconexión. Ahora en los próximos módulos se mencionarán los principios de operación de otras de las redes más populares como lo es la red telefónica fija y móvil.

## MÓDULO VI

## REDES DE TELEFONÍA INTELIGENTES

En este módulo estudiamos la red más importante en el mundo de las telecomunicaciones que a pesar de que a través del tiempo ha cambiado su tecnología de manera importante y que hoy en día tiene que competir con las nuevas tecnologías de redes sigue siendo la red más extensa a nivel tanto nacional como mundial, a la cual cualquier persona puede tener acceso a un bajo costo. Es la red telefónica la que ha permitido el desarrollo de las nuevas tecnologías en las redes.

La palabra teléfono tiene su origen en dos palabras *tele* que significa distancia y *fono* que significa sonido. Está compuesto básicamente por un circuito de voz, una campana, una bocina, un micrófono y un teclado. Pero llama la atención preguntarse ¿qué sucede cuando recibimos una llamada?, cuando se recibe una llamada la central telefónica envía una señal de corriente alterna de 90V. a 25 Hz. que activará la campana avisándonos que hay una llamada entrante, al momento de descolgar se activan entonces el circuito de voz y el teclado desactivando a su vez la campana, el circuito de voz separa entonces las señales de entrada y salida, además que permite retroalimentar a la bocina una parte de la señal del micrófono. En la figura 6.1 se muestra esquemáticamente las partes que componen un teléfono.

Si por el contrario nosotros somos quienes realizamos la llamada el circuito de voz es activado, activando a su vez el teclado y desactivando la campana, con lo cual avisa a la central de que se desea realizar una llamada enviándole una señal de 19 a 45 mA. y a su vez la central responde enviando un tono de invitación a marcar.

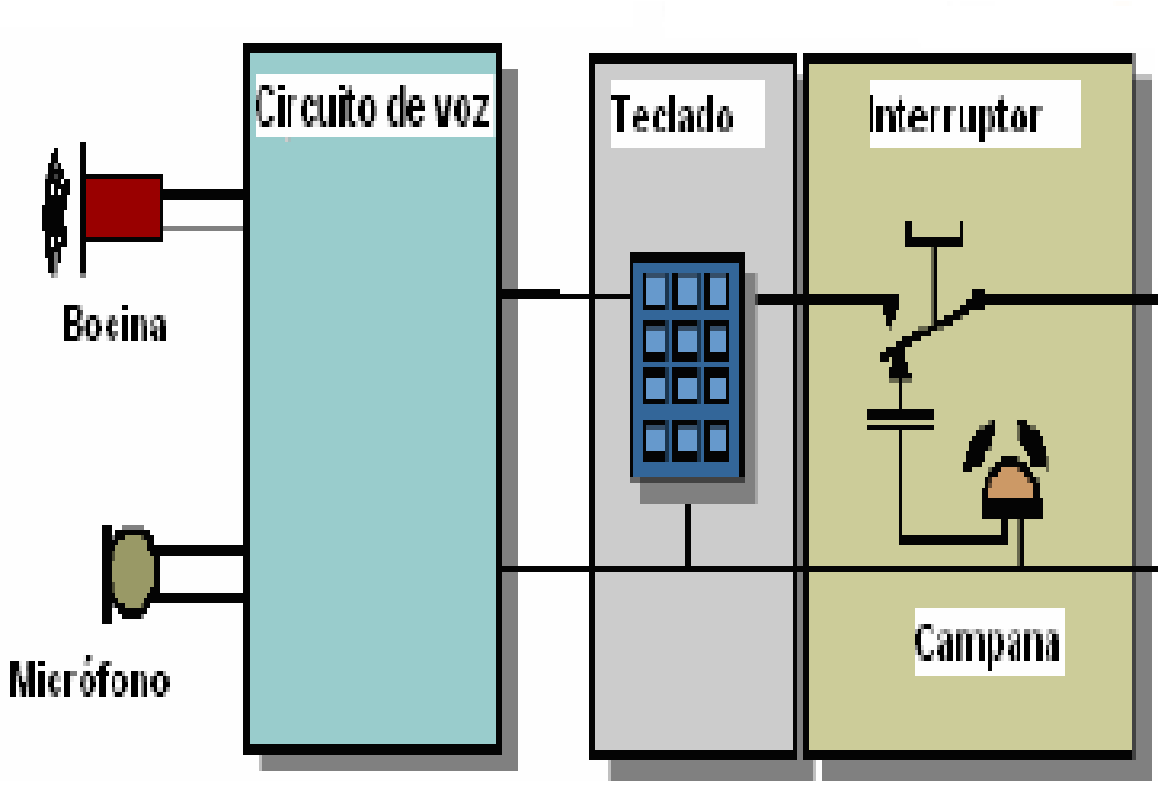



Fig. 6.1 Esquema básico de un sistema telefónico

Al activar el teclado y nosotros marcar el número deseado se genera un tono que es el resultado de la combinación de dos frecuencias el cual es único por cada una de las teclas. En la figura 6.2 se muestra la combinación de las frecuencias de dichas teclas. Para completar la llamada la central checa el estado de la línea del usuario a llamar (abonado B), si hay circulación de

corriente, esto indica que B está usando el teléfono y entonces se envía un tono de ocupado al usuario llamante (abonado A). Si no hay circulación de corriente, se envía un tono a A, indicando que se está llamando a B. Al abonado B se le envía la señal de llamada, que es un voltaje alterno de 90V. Al descolgar B, la central lo detecta por la corriente que circula, procediendo entonces a conectar a los dos abonados. En cuanto cuelga uno de los dos abonados se interrumpe la corriente, lo cual es detectado por la central, procediendo a terminar la llamada y a mandar tono de ocupado rápido al otro abonado.

La central de conmutación aparte de enlazar las llamadas es el ente encargado de conectar los abonados a los equipos de la misma central que proporcionan algún servicio (mensajes, hora , etc.), conecta a los abonados de la central con los abonados de otra central, hace la conexión con un PBX (Private Branch Exchange), contiene maquinas de anuncios y grabaciones, alimenta la línea de abonado, realiza servicios de llamada en espera, llamada tripartita, funciones de acceso a internet y lleva un registro de todas las conexiones (llamadas) a fin de poder efectuar la tasación y cobro de cada una de ellas.

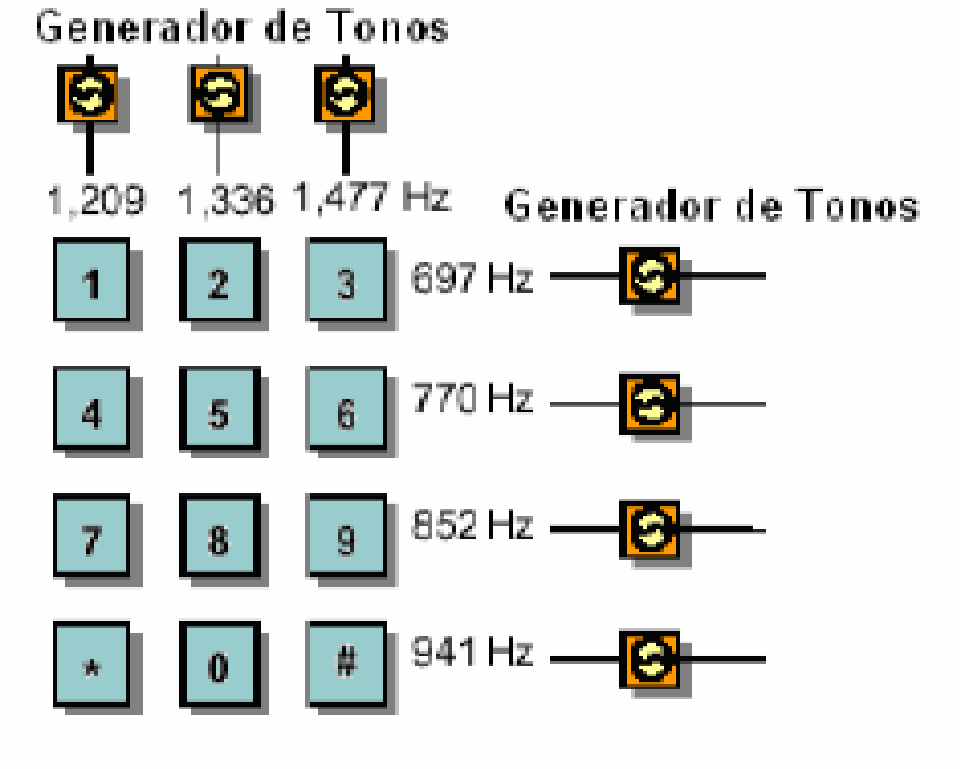



Fig. 6.2 Combinación de frecuencias en el teclado telefónico

Las centrales actuales contienen dos elementos básicos:

- *Matriz Principal de Conmutació*n (Group Switch). Se encarga de efectuar la conmutación de todas las llamadas entrantes a la central, puede manejar desde 10 000 hasta 100 000 abonados por central.

- *Conmutador de Etapa de Abonado o Concentrador*. A través de él se conecta equipo a la central, además de concentrar el tráfico que se dirigirá hacia la matriz principal. El principal componente de esta etapa son los LIC (Line Interface Circuit) al cual se conectan todos los abonados tanto analógicos como digitales.

Las centrales se clasifican de acuerdo a su posición o jerarquía dentro de la red, de manera general se dividen en centrales de abonados y centrales “tándem” las cuales no contienen

abonados. Se encuentran también clasificaciones con respecto al tipo de transito que manejan, ya sea local, mundial, por zona urbana, o por población.

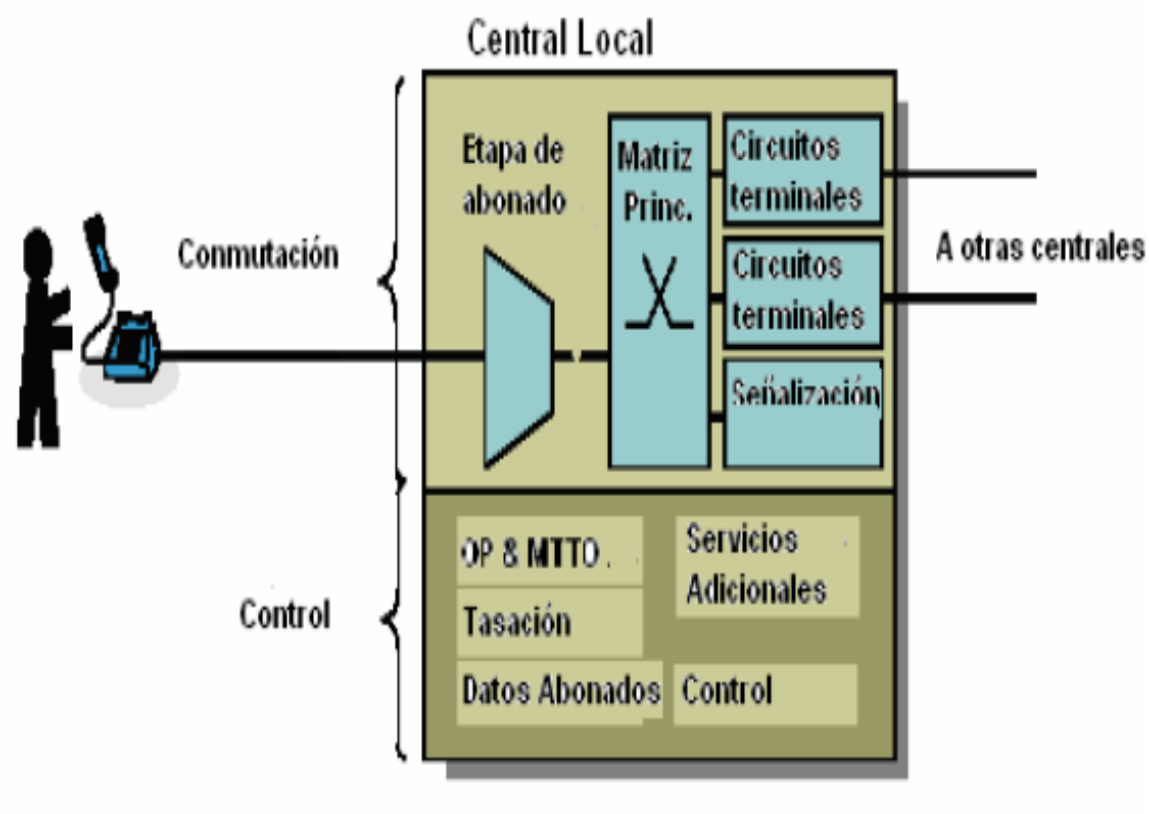



Fig. 6.3 Componentes de una de una telefónica

- **Digitalización de la voz**

Ahora bien ¿cómo es que nuestra voz viaja por el cable?, la respuesta se encuentra en la técnica de digitalización de la misma, esto se logra a través de la modulación PCM (Pulse Code Modulation), la cual consiste en tomar muestras instantáneas de una señal analógica y representarlas por medio de palabras digitales en un tren de pulsos en serie.

La técnica básicamente consta de un ***filtro*** el cual se encarga de limitar el ancho de banda al rango de 3000 a 3400 Hz., esto debido a que la voz humana genera frecuencias que van desde los 0 hasta los 4 KHz. La técnica PCM toma cerca de 8000 muestras en cada segundo, ya que para poder reconstruir una señal muestreada sin distorsión alguna es necesario que la tasa de muestreo sea al menos el doble de la frecuencia máxima de señal original. Si partimos de que la frecuencia máxima que genera el humano es de 4000 Hz. entonces la frecuencia de muestreo será del doble, es decir 8000 Hz.

A cada valor muestreado se le asigna una palabra de 8 bits por lo que el resultado será un tren de pulsos de 64 Kbps.

VELOCIDAD = 8000 muestras/seg x 8 bits/muestra
VELOCIDAD = 64 Kbps

Ya tomadas las muestras será necesario cuantificarlas, la ***cuantificación*** es el método por el cual se asigna un valor de un número finito de combinaciones a una muestra de una señal analógica en función de su valor de amplitud. El número posible de combinaciones estará dado por el tamaño de la palabra binaria que se usará para codificar el valor muestreado.

Ahora será necesario asignar un código a cada valor de esta cuantificación, el proceso de ***codificación*** consiste en asignar un grupo de bits para representar el valor de la muestra en forma binaria.

Existe una técnica que nos permite intercalar en el tiempo muestras de diferentes señales a fin de transmitir la información de todas ellas en serie y sobre un mismo canal sin necesidad de tender un par de cobre por cada línea que haya. En PCM se utiliza el multiplexaje por división en tiempo (TDM: Time Division Multiplexing), que consiste en intercalar en el tiempo muestras de diferentes señales (canales) a fin de transmitir la información de todas ellas en serie y sobre un mismo canal. La velocidad de cada canal es de 64 Kbps, por lo que la velocidad del tren resultante será la suma de cada una de las velocidades de los canales que forman el tren. La norma europea define un tren o patrón que consta de 30 canales de información, uno de sincronía y uno de señalización, para formar la trama básica conocida como *E1* con una velocidad de 2.048 Mbps.

En la trama E1, a cada canal se le asigna una ranura de tiempo, numeradas del 0 al 31. La ranura o time slot 0 se usa para sincronización y alineación de trama, el time slot 16 se usa para señalización, el resto de time slots se usan para transportar la información de voz.

- **Señalización**

La señalización, es el protocolo que se usa para establecer o terminar una conexión entre equipos de comunicaciones. Los tipos de señales existentes en la telefonía son:

- *Señales de línea*. Sirven para indicar los distintos estados del circuito de abonado. Se realiza mediante cambios de impedancia.

- *Señales de registro*. Se utilizan para enviar a la central el número del abonado al que se desea llamar o para activación de servicios en centrales digitales.

- *Señales acústicas*. Sirven para informar a los abonados (A y B) del estado de sus solicitudes al sistema. Por ejemplo, tono de ocupado, timbrado de campana, etc.

Entre las centrales telefónicas existen dos tipos de señalización: señalización por canal asociado CAS y señalización por canal común CCS.

- En la ***señalización por canal asociado CAS*** la información de señalización es transmitida junto con la información de voz y el protocolo más usado actualmente es el R2, el cual trabaja con la filosofía en la que el lado que envía la información debe de recibir una confirmación del otro lado para poder continuar. Estas señales pueden ser para indicar que sea colgado de algún lado de la transmisión y así se libere el circuito, para indicar que alguno de los abonados ya ha contestado, etc. El sistema digital R2, utiliza el canal 16 para la señalización de línea.

- ***Señalización por canal común CCS***. En este tipo de protocolo la señalización se transmite por un circuito dedicado únicamente a este fin. El SS7 es una plataforma que proporciona un sistema de señalización por canal común.

La señalización SS7 consta básicamente de los siguientes elementos:

- *Puntos de Señalización* (SP). Central telefónica que realiza las funciones de conmutación y

acceso a la red inteligente. Puede además incluir las funciones de STP y SCP.

- *Punto de Transferencia de Señalización* (STP). Se encarga de conmutar y enrutar los mensajes de señalización a su destino.

- *Punto de Control de Servicio* SCP. El SCP (Service Control Point). Efectúa las funciones de control para los servicios de la red. Por ejemplo, bases de datos de acceso remoto.

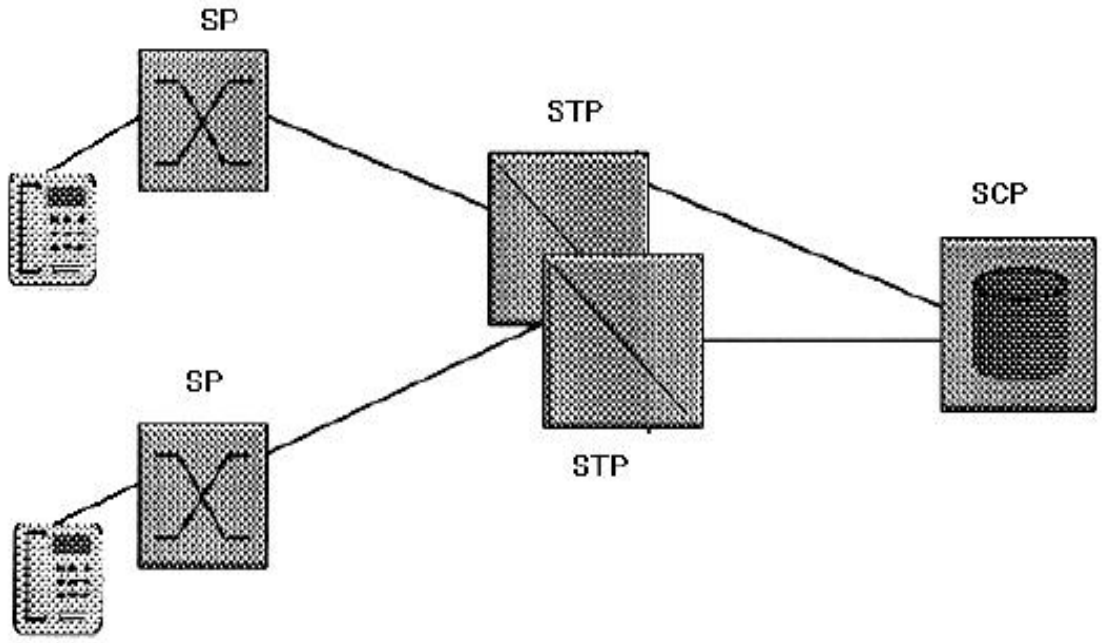



Fig.6.4 Elementos básicos de señalización SS7

Con respecto al modelo OSI la señalización SS7 define lo que es MTP (Message Transfer Part) el cual efectúa las funciones de transferencia de información a través de la red de señalización. SS7 está dividido en 3 capaz, la primera de ellas es la MTP1 que equivaldría a la capa 1 de OSI, y es la encargada de definir las características físicas y eléctricas de los enlaces de señalización. El enlace de señalización es una trayectoria de transmisión bidireccional de dos canales de datos operando en direcciones opuestas y a la misma velocidad. La MTP2 equivalente a la capa 2 de OSI, en este nivel se llevan a cabo las funciones que aseguran la confiabilidad de la transmisión de los mensajes de señalización. La MTP3 equivalente a la capa 3 de OSI este nivel se encarga del enrutamiento de los mensajes y la administración de la red de señalización, Efectúa funciones de discriminación, distribución y ruteo de los mensajes de señalización, así como de administración de tráfico, enlaces y rutas.

Por último es importante mencionar que existen redes que son consideradas 100% digitales, es decir que todos sus sistemas de interconexión así como los dispositivos de interfaz a usuario son digitales capaces de usar el protocolo Q.931. Sus centrales de conmutación deben usar señalización SS7; estas redes se conocen como Red Digital de Servicios Integrados ISDN por sus siglas en ingles. Existen dos tipos de interfaces en dichas redes BRI y PRI; la interfaz tipo BRI (Basic Rate Interface) se usa en aplicaciones de bajo trafico como hogares, mientras que la interfaz tipo PRI (Primary Rate Interface), se usa para en aplicaciones de alto tráfico.

# MÓDULO VII

# TELEFONÍA CELULAR

En este módulo se estudió las redes móviles de telefonía celular, el avance tecnológico que ha tenido dicha red en sus diferentes generaciones, así como los dispositivos que la conforman.

## ➢ Métodos de Acceso al medio aéreo

El recurso que permite que la telefonía móvil exista son las señales radioeléctricas, las cuales viajan por el aire en una gama de frecuencias siendo éstas un recurso finito; debido a esto se han desarrollado técnicas que nos permiten que varios usuarios puedan compartir el mismo recurso a la vez.

Al utilizar el medio inalámbrico, tenemos dos formas de lograr transmisiones entre dos estaciones:

1. Multiplexado en el tiempo (TDD, *Time Division Duplex*). Esto es, durante un intervalo determinado A transmite y B recibe. En el siguiente intervalo, es B quien transmite y A quien recibe.

2. Multiplexado en la frecuencia (FDD, *Frequency Division Duplex*). En este esquema, A utiliza una banda de frecuencia para transmitir hacia B, mientras que B utiliza una banda diferente para enviar mensajes a A.

De lo anterior surge el concepto de acceso múltiple, el cual consiste en que uno o más usuarios puedan accesar al medio al mismo tiempo. La técnica más antigua consiste en utilizar múltiples bandas de frecuencias para múltiples usuarios, lo que es conocido como ***FDMA*** (Frequency Division Multiple Access). FDMA se caracteriza por requerir del uso de las llamadas bandas de guarda, lo cual es el espacio no utilizado entre dos bandas, y que tiene por objeto evitar interferencia por canal adyacente. Implementar la separación de los canales requiere la implementación de filtros analógicos. Si la cantidad de canales aumenta, también crecerá el tamaño del circuito utilizado para modular/demodular, junto con su costo económico y su consumo de potencia. Entre más angosta sea la banda a aislar, más costoso, tecnológica y económicamente hablando, será implementar el filtro que la separe. Entre más se segmente el espectro, también mayor será el desperdicio de frecuencias por el uso de bandas de guarda. Si la banda de frecuencias destinada a cada canal es angosta, también se obtendrá una tasa de transmisión reducida.

Al popularizarse el uso de la digitalización de medios, como lo fue el uso de PCM, ADPCM y otros esquemas de voz digital, la digitalización de textos e imágenes, al mismo tiempo que fueron desarrolladas técnicas de modulación digital (PSK, QPSK, QAM, entre otras), se concibió la idea de que varios usuarios o aplicaciones pudieran hacer uso del mismo canal (banda de frecuencia), alternando para ello en diferentes intervalos de tiempo. Éste es el principio básico del multiplexaje por división de tiempo, o TDMA (Time Division Multiple Access).

Al usar ***TDMA***, es posible multiplexar varios usuarios dentro de la misma banda de frecuencias, lo que evita el uso de bandas de guarda, y aumenta la eficiencia de uso del espectro, se reduce el tamaño del circuito resultante y su costo. Existen, por supuesto, algunos problemas con el uso de TDMA, entre ellos podemos mencionar la alta potencia necesaria para alcanzar una radiobase desde un móvil, y la necesidad de sincronizar todas las estaciones con respecto a una base de tiempo maestra, lo que implica tener pequeños relojes en cada uno de los transmisores. TDMA es más segura que su contraparte analógica FDMA, puesto que facilita el uso de técnicas digitales de encripción. Al ser fácilmente manipulable, la trama de bits destinada a cada usuario facilita

también la inserción de señalización dentro de banda. En la figura 7.1 se muestra esquemáticamente la diferencia entre este tipo de multiplexajes.

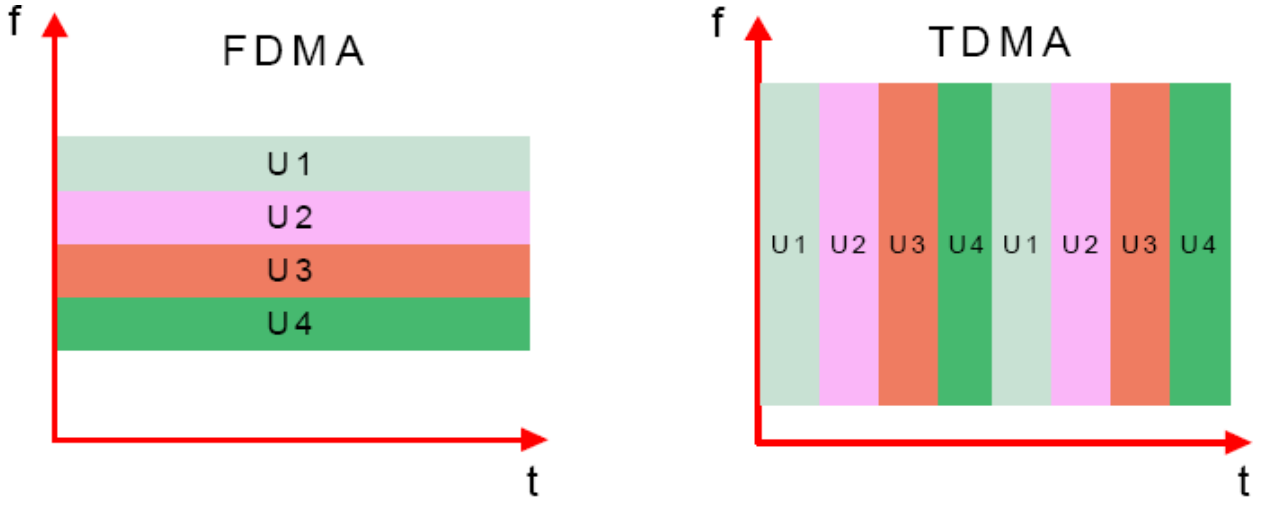



Fig. 7.1 Diferencia entre FDMA y TDMA

De la misma manera existe ***CDMA*** (Code Dividon Multiple Access) que es un sistema estándar de interfaz área que implica el uso de técnicas digitales para la transmisión de información, es usada para sistemas de tercera generación y usa la técnica DSSS la cual se verá más adelante. El principio de operación de CDMA se basa en que la potencia recibida de cada uno de los emisores es igual todo el tiempo. CDMA usa una tecnología de espectro ensanchado, es decir la información se extiende sobre un ancho de banda mucho mayor que el original, conteniendo una señal (código) que lo identifica. Los canales de tráfico en CDMA se definen con dos parámetros: una portadora de RF y una secuencia PN (código único por usuario).

- **Técnicas de acceso al medio en banda ancha**

Como una forma más de insertar múltiples usuarios en un solo canal de radio, llegamos a las técnicas de acceso en banda ancha, llamadas así por utilizar bandas de frecuencia considerablemente más anchas que sus antecesores FDMA y TDMA. Se denominan también espectro disperso, con dos principales variantes: espectro disperso por salto de frecuencia (*Frequency Hoping Spread Spectrum*, FHSS), y espectro disperso de secuencia *directa (Direct Sequence Spread Spectrum*, DSSS).

El ***FHSS*** se llama así porque un solo canal de usuario utiliza varias portadoras para transmitir, "brincando" de una frecuencia a otra, siguiendo una secuencia conocida sólo por el transmisor y el receptor, los cuales deben estar sincronizados entre sí, de modo que siempre se conozca la siguiente frecuencia a sintonizar y el intervalo de tiempo que se deberá permanecer en ella.

Al saltar de una frecuencia a otra, se logran ciertas ventajas:

1) Hay una mayor resistencia al ruido e interferencia, puesto que si tal problema existe en una frecuencia en particular, sólo la porción de información transmitida en esa frecuencia será afectada.
2) La seguridad de la información enviada es mayor que al transmitir por una sola frecuencia todo el tiempo porque, si por un lado es difícil sintonizar la frecuencia en la que se transmite al mismo tiempo que el emisor, por otro lado el tiempo que se logra decodificar es tan poco que la información capturada es poco coherente sin el contexto adecuado.

***DSSS***. Las técnicas de *secuencia directa* tienen con respecto a las técnicas de salto de frecuencia una diferencia fundamental: no existen múltiples portadoras, sino una sola frecuencia portadora, donde, además, todas las estaciones transmiten al mismo tiempo en un aparente caos que para un receptor sin la capacidad para decodificar la información aparece simplemente como ruido blanco. En estos sistemas, las unidades de información digital en banda base son multiplicadas por una secuencia pseudo-aleatoria PN (pseudo-noise) producida por un generador de códigos pseudoaleatorios, donde cada único código proveniente de este generador y se conoce con el nombre de chip. Para cada bit de banda base, un número mucho mayor de chips es generado a la salida de esta operación (normalmente, la relación de los primeros a los segundos es 1:64, y en ocasiones mayor). Estas secuencias son asignadas a cada estación transmisora por una autoridad central, donde cada secuencia es lo suficientemente ortogonal con respectos a las demás secuencias asignadas, de manera que al intentar decodificar una secuencia dada entre las demás sea distinguible aunque se transmita utilizando la misma frecuencia portadora. Esto es posible debido a que la correlación de una señal con su secuencia originadora arroja un número mucho mayor que la correlación con cualquiera de las demás señales presentes.

- **Componentes de la red telefonía celular**

Una red de telefonía celular consta básicamente de los componentes que se muestran en la figura:

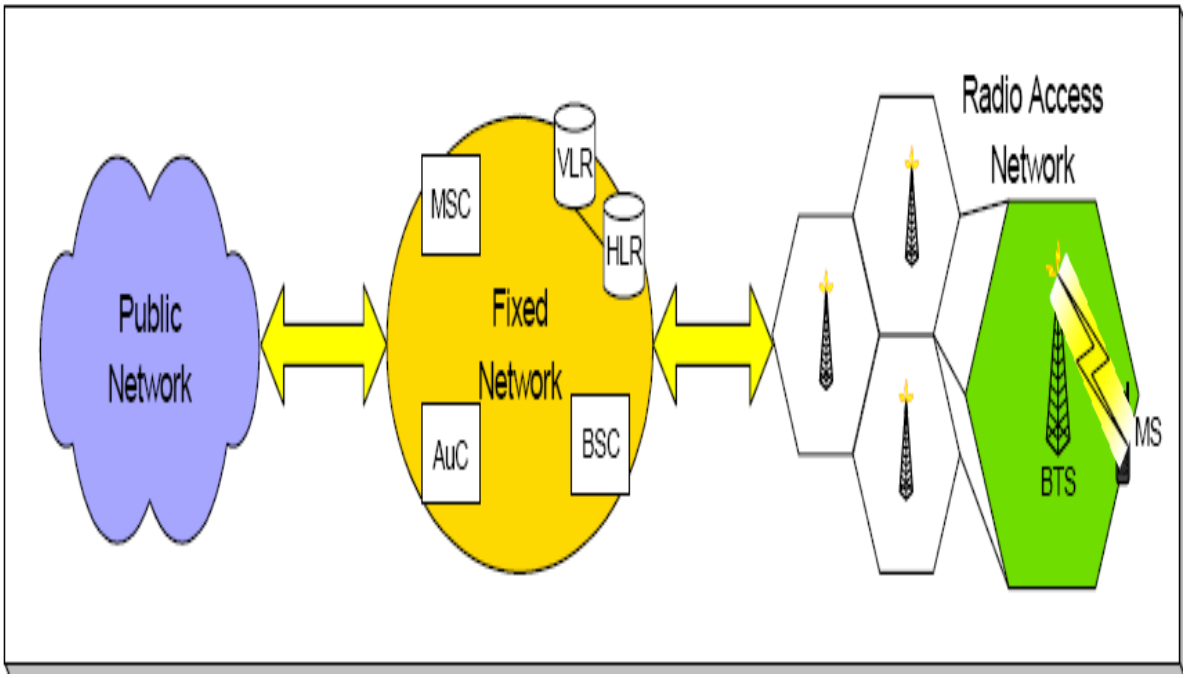



Fig. 7.2 Componentes de una red de telefonía celular

- **RAN**. Red de Acceso por Radio (Radio Access Network). Hace posible la conectividad utilizando alguna tecnología de acceso múltiple inalámbrico (FDMA, TDMA, CDMA, u otra). Estas tecnologías de acceso, junto con los protocolos que las regulan, reciben el nombre genérico de interfaz aérea (air interface).

- **Células**. Con el objeto de maximizar el rehusó de frecuencias y al mismo tiempo incrementar el número total de suscriptores por unidad de área, los sistemas celulares extienden su área de cobertura por medio de radiobases, las cuales están calculadas para cubrir cierta cantidad de

terreno con cierto número de canales (capacidad de llamadas simultáneas). Las radiobases quedan dispuestas de forma semi-ordenada sobre el terreno en un patrón geométrico, de manera que se cubra la mayor área posible, permitiendo que un usuario móvil pueda desplazarse dentro de dicha área de cobertura, sin dejar de acceder al servicio. El término *celular* surgió de la similitud en forma que tiene un patrón de cobertura, en forma de hexágonos contiguos, asemejándose al patrón que sigue el tejido de los seres vivos.

- **Red Fija o FN** (Fixed Network). Es la infraestructura que hace posible la conmutación de llamadas, el correcto enrutamiento de las mismas, el apropiado registro de uso, facturación, entre otras, dentro de la red fija encontramos los siguientes elementos:

- *MSC* (Mobile Switching Center). Es una central de conmutación de circuitos telefónicos. Su función es conectar y enrutar llamadas internas, llamadas entrantes y llamadas salientes.

- *HLR* (Home Location Register). Es una base de datos donde se almacena toda información relacionada con los usuarios, como es su número telefónico, números de serie electrónicos de los aparatos telefónicos, perfil de usuario, servicios a que tiene acceso, etc. En esta base de datos se registran usuarios locales.

- *VLR* (Visitor Location Register). Es una base de datos dinámica, que registra a todos aquellos usuarios que se encuentran visitando el sistema, es decir, que están adscritos en otro sistema, pero que tiene derecho a utilizar los servicios del sistema local, debido a la facilidad de *roaming*.

- *AuC* (Authentication Center). Es un programa que valida la entrada de los usuarios al sistema, consultando las bases de datos HLR y VLR, y verificando que tengan derecho al uso del sistema y sus servicios.

- *BSC* (Base Station Controller). Este elemento de red aparece hasta la segunda generación de redes celulares (GSM), y su función es tomar control de algunas funciones que originalmente pertenecían al MSC, como son: realizar búsqueda (paging) de usuarios por zona, coordinar el handoff entre una célula y otra, y conmutar llamadas localmente.

- **Funcionamiento de la telefonía celular**

Cuando un móvil se desplaza dentro del área de cobertura de un proveedor de servicio, manteniendo una llamada activa y a medida que se desplaza de una célula a otra, se hace necesario que el sistema celular coordine la provisión del servicio entre diferentes células, de modo que el usuario pueda seguir recibiendo el servicio de forma transparente e ininterrumpida. La operación en la que el sistema coordina esta asignación de servicio de una célula a otra, a medida que el usuario se mueve en la frontera entre una célula y otra, recibe el nombre de handoff, o handover. Cuando un móvil inicia una conversación la célula que en ese momento lo ha "adoptado" da recursos para que la conversación se lleve a cabo; se utiliza un canal de tráfico bidireccional y se mantienen lazos entre la radiobase y el móvil por medio de señales en uno o varios canales de control. Al aproximarse a la frontera entre dos (o inclusive tres o cuatro) células, el sistema debe indicar a la radiobase que en ese momento transporta el tráfico del usuario de liberar el canal de tráfico, e instruir a la radiobase que le recibe de asignar canales de tráfico y control, para dar continuidad a la conversación.

Las radiobases y los elementos de red que residen en las mismas, carecen de la inteligencia para coordinar la acción del handoff. Se hace necesario que un tercer elemento, que tenga acceso a la información de la localización del móvil, así como de la asignación de frecuencias en cada una de las células, tome la decisión del "salto" de una célula a otra. En las redes de primera generación (FDMA), era directamente el MSC el encargado de realizar esta función. A partir de las

redes de segunda generación, aparase la figura del BSC, entre cuyas funciones está la de coordinar los handoffs en su respectiva zona de influencia. Por lo general un BSC coordina los handoffs entre varias decenas de células.

Al realizarse el cambio de una célula a otra, el sistema deberá desasignar el canal de usuario que se utilizaba en la célula origen, y asignar un nuevo canal de usuario en la célula destino. La decisión del momento más propicio para realizar el cambio la toma el sistema utilizando mediciones recientes de potencia proveniente del móvil en cuestión medida en las radiobases candidatas a recibirlo. En las redes de primera generación, existían receptores especiales dedicados a realizar estas mediciones, y reportarlas al MSC para apoyar la toma de decisiones de handoff. Estas antenas especiales reciben el nombre de locate receivers. El punto crítico donde se realiza la transición de una célula a otra es, precisamente, la frontera entre células, zona en la cual la potencia recibida de las dos o tres radiobases cercanas es la misma, razón por la cual la frontera se denomina también isocontorno de potencia. Existen además, varias modalidades de handoff, dependiendo sobre todo de la tecnología e interfaz aérea utilizadas:

- *Hard handoff*. En redes de primera generación (FDMA) los teléfonos móviles podían sintonizar una sola frecuencia. Por tal razón, para sintonizar la frecuencia de una radiobase destino, debía existir un momento (milisegundos), durante los cuales el móvil “suelta” la frecuencia origen y sintoniza la frecuencia destino.

- *Soft handoff*. Este procedimiento, utilizado en redes de tecnología digital (TDMA, CDMA), permite al móvil sintonizar un nuevo canal de tráfico, sin “soltar” el canal de tráfico origen. Esta posibilidad aumenta grandemente la calidad del handoff, y disminuye el riesgo de una transición imperfecta o fallida.

- *Softer handoff*. Utilizado en tecnologías CDMA y Spread Spectrum, permite handoffs incluso entre sectores de la misma célula, y sectores de células vecinas.

Como ya se ha mencionado el sistema de telefonía celular basa su funcionamiento en el rehusó de frecuencias a través de un grupo de células, es decir una frecuencia es rehusada a una cierta distancia de la otra, permitiendo que de esta manera no existan interferencia entre las frecuencias de las células. Sin embargo debido al aumento de usuarios en ciertas zonas se ha tenido que recurrir a lo que se denomina como sectorización de células, que equivale a una partición del área de cobertura en tres, cuatro, o hasta seis sectores, es un recurso que permite aumentar la capacidad de tráfico de una célula de forma muy puntual.

Una célula también puede ser particionada como un círculo interno, alrededor de la radiobase, y un círculo más externo hasta la frontera de la célula, de forma que puede decirse que existe una célula “interna” y otra célula “externa”. Otra variante son las microcelulas las cuales las cuales se utilizan para zonas muy pequeñas como lo pueden ser un edificio.

Por último se debe de mencionar que la red de telefonía celular como ya se ha visto con anterioridad requerirá de una conexión con la telefonía fija, a partir de los sistemas de segunda generación, se utiliza la señalización por canal común (CCS), y la serie de protocolos SS7, para los procedimientos de paso de tráfico entre todos los operadores de telefonía móvil entre sí, y hacia los demás operadores. Así mismo, se utiliza para señalizar el paso de tráfico entre el MSC el BTS, y entre MSCs.

IS-41 es un estándar americano, utilizado ampliamente hoy en día. Mediante él, se permite el paso de llamadas entre redes de distinta tecnología y entre diferentes proveedores de servicio. Gracias a este protocolo, MSCs de diferentes proveedores de servicio intercambian información de usuarios por demanda.

- **Generaciones de sistemas celulares**

Ahora que ya se ha mencionado los fundamentos que permiten que la red de telefonía celular exista se mencionarán las principales características de las diferentes generaciones de telefonía celular.

*1era GENERACIÓN*

Como se ya se ha mencionado antes esta generación está caracterizada por tener un acceso al canal totalmente analógico, su modulación es FM, no cuenta con ningún tipo de seguridad y el MSC es el principal componente que permite la facturación registro de usuario y coordina el handoff. Entre los sistemas más usados en esta generación está el AMPS. Esta generación sufre de problemas de seguridad ya que es fácil para un receptor no autorizado decodificar la señal ilegalmente.

*2da GENERACIÓN*

Usa una codificación de digital de voz de forma encriptada, su modulación es completamente digital, utiliza canales dedicados para la señalización. Introduce el concepto de BSC, estandariza de esta manera la interfaz entre el BSC y el MSC, utiliza la FSSH y DSSS. Es en esta generación que surge el concepto de roming automático y el sistema GSM y GPRS.

- GSM (Global System Mobile), propone servicios digitales a nivel de red, trabaja en la banda de 1.8 a 2.0 GHz., posee la funcionalidad llamada on-the-air-privacy que hace imposible el espionaje telefónico ya que cada fabricante compromete a mantener en secreto el algoritmo criptográfico. En el sistema GSM existen dos tipos de servicios: Teleservices (telefonía) y Data Services (IP, X25). En la figura 7.2 se muestra la red GSM.

- GPRS (General Packet Radio Service), es un subconjunto de la interfaz área del GSM dedicado especialmente a la transmisión de datos hacia un MS por lo cual a la radio base se le añade una unidad llamada PCU (Packet Control Unit) que provee una ruta alterna para datos así como una modificación al BTS. Se le adicionan dos elementos el GGSN (Gateway GPRS Support Node) y el SGSN (Service GPRS Support Node). Existen actualizaciones en GSM para la transmisión de datos a alta velocidad entre los cuales podemos mencionar EDGE, UMTS y HSDPA.

*3era generación (CDMA)*

La tercera generación utiliza modulación CDMA; una llamada CDMA empieza con una transmisión a 9600 bits por segundo. Entonces la señal es ensanchada para ser transmitida a 1.23 Mbps aproximadamente. El ensanchamiento implica que un código digital se aplica a la señal generada. Posteriormente la señal es transmitida junto con el resto de señales generadas por otros usuarios, usando el mismo ancho de banda. Las señales de los distintos usuarios se separan haciendo uso de los códigos distintivos y se devuelven las distintas llamadas a una velocidad de 9600 bps. La tasa de transmisión por usuario cambia en tiempo real. Varía de 9600bps cuando el usuario habla, a 1200bps cuando hay silencio.

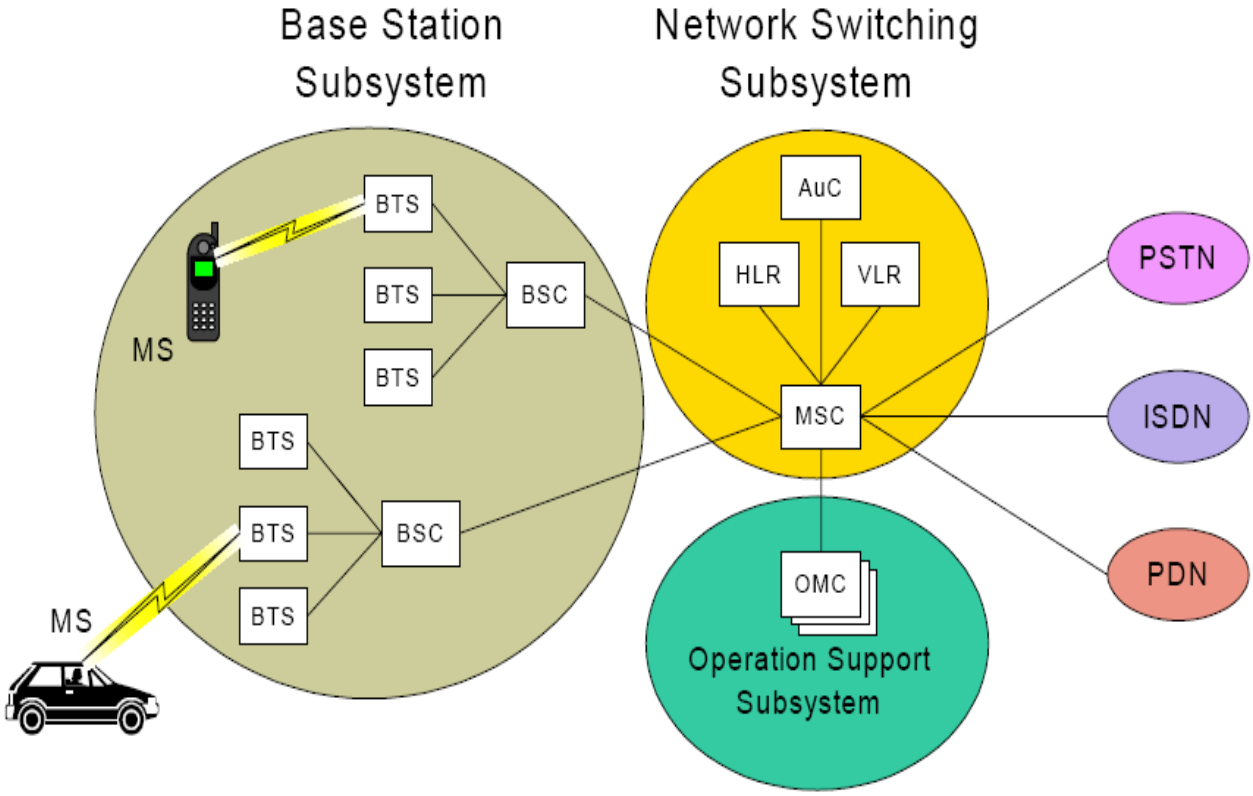



Fig. 7.2 Red GSM

Como parte del procedimiento inicial de reconocimiento entre la radiobase y el MS, se intercambian llaves pública (ESN publica del MS) y privada (MIN del suscriptor), lo que asegura la confidencialidad de la conversación al ser transmitida por el aire. Dado que cada celda utiliza la misma banda de frecuencias, se elimina por completo la necesidad de hacer planeación de frecuencia.

CDMA cuenta con algunas variantes entre las cuales se encuentra la CDMAx1 EV-DO (Evolution Data-Only) que se caracteriza por permitir tasas superiores a 1 Mbps, separa voz y datos en dos portadoras diferentes, puede tener una capacidad de enlace de datos de bajada de hasta 2.4 Mbps; aunque hay otras variantes de CDMA que lo que permite es aumentar el ancho de banda en los canales de voz y datos transmitiendo éstas en una sola portadora optimizando así el uso del espectro esta variante es llamada CDMA2000 1xEV-DV (Evolution-data and voice). Otra variante es el CDMA 2000 3x (o Multicarrier CDMA, MC CDMA) el cual utiliza 3 portadoras de 1.25 MHz para un ancho de banda total de 5MHz, las múltiples portadoras son utilizadas sólo en el enlace de bajada para incrementar la capacidad de transmisión de datos, en el enlace de subida se utiliza una sola portadora.

La tercera generación está caracterizada por ser una red puramente de conmutación de paquetes, mayores ancho de banda con respecto a 2G, servicios multimedia de voz, datos y video, cobertura universal así como terminales universales, establece QoS y servicios interactivos. Se pretende que por un solo medio de transmisión sea posible transportar datos y voz, lo que también se busca sea posible en las redes de datos ethernet actuales a través de la telefonía sobre IP la cual se menciona en el módulo 8 que a continuación se presenta.

# MÓDULO VIII

# VOZ POR IP

Hoy en día la tendencia en las telecomunicaciones es la unificación en una sola red de servicios de voz y datos, se pretende que se utilice la infraestructura de la redes de datos para poder transmitir por medio de ella nuestra voz. En este módulo se estudiaron las características que conforman una red de telefonía IP.

## ➢ Protocolos básicos de la telefonía IP

Primeramente definamos lo que es telefonía IP; ***telefonía IP*** es una aplicación de voz sobre IP y en la cual se llevan servicios básicos de telefonía tradicional como transferencia de llamada, conferencia, sígueme, llamada en espera, grupos de trabajo, retención de llamada, etc.

En un principio la idea de basarnos en la redes de datos existentes sobre TCP/IP es buena, sin embargo existen algunos inconvenientes en esto, primeramente los protocolos usados en la redes de datos no pueden ser utilizados en la redes de voz, debido a que protocolos como TCP posee características que no permitirían un buen desempeño en la transmisión de voz en tiempo real, características como lo son la comprobación de llegada de paquetes, que no es un protocolo que permite multicast, que es orientado a conexión y debido a la retransmisión de paquetes es probable que surjan problemas de delay en una transmisión. Ante esto se podría proponer usar otro tipo de protocolo por ejemplo UDP, sin embrago tiene desventajas ya que UDP no realiza ningún tipo de comprobación en la llegada de paquetes por lo cual no se tendría la seguridad de que realmente ha llegado la información a su destino, no provee mecanismos de sincronización ni control de flujo o congestión. La solución a este problema es extender el uso de UDP, adicionando cierta información de control a los datos y utilizando UDP para distribuir la información de control y de voz. Ésta es la forma en la que el protocolo ***RTP*** (Realtime Transport Protocol) funciona en la arquitectura de TCP/IP.

El protocolo RTP está definido como un protocolo que provee servicios de entrega end-to-end para datos con características de tiempo real, tales como audio y video interactivos, por lo que este protocolo puede ser utilizado por las aplicaciones de VoIP.

La especificación de RTP define dos protocolos separados. El primero RTP, su función es transferir información de tiempo real (voz). El segundo RTCP (RTP Control Protocol), provee información acerca de los participantes en la sesión (control), en redes TCP/IP comúnmente funciona sobre UDP.

RTP envían suficiente información a la aplicación para que esté segura en que orden poner los paquetes para reproducirlos, además provee información acerca de la calidad de la recepción, para que así la aplicación pueda utilizarla para realizar ajustes locales.

La IETF (Internet Engineering Task Force) es un grupo global en el que participan especialistas y el cual se dedica al desarrollo de estándares sobre Internet, entre los cuales se encuentran H323, SIP, MGCP y MEGACO para redes de voz sobre IP.

El estándar H.323 proporciona los fundamentos de audio, video y comunicaciones de datos a través de las redes basadas en IP, dirige el control de llamada, administra multimedia y el ancho de banda, así como las interfaces entre LAN´s y otras redes. H 323 no garantiza la calidad de servicio (QoS). H.323 es parte de una gran serie de estándares de comunicaciones que habilitan videoconferencia a través de redes conocidas como H.32X, tales series incluye H.320 y H.324, las cuales dirigen las llamadas hacia la ISDN y la red pública.

<table>
<tr><th colspan="2">Video</th><th colspan="2">Audio</th><th colspan="3">Control</th><th>Datos</th></tr>
<tr><td colspan="2">H.261<br>H.263<br><br>Codecs de video</td><td colspan="2">G.711<br>G.722<br>G.723<br>G.729<br><br>Codecs de audio</td><td rowspan="2">H.225<br><br>Terminal a Señalización Del Gatekeeper</td><td rowspan="2">Q.931<br>Señalización De Llamada</td><td rowspan="2">H.245<br>Canal de control</td><td rowspan="2">T.120<br>Terminal para Compartir datos</td></tr>
<tr><td>RTP</td><td>RTCP</td><td>RTP</td><td>RTCP</td></tr>
</table>

Fig.8.1 Cuadro de protocolos presentes en la telefonía IP

- **Componentes de una red de telefonía IP**

El estándar H.323 define cuatro componentes de básicos de comunicación: *Terminales, Gateways, Gatekeepers y Multipoint Control*

1. Terminales. Son puntos finales sobre la LAN, todos estos puntos deben soportar el estándar H.245, el cual se emplea para negociar el uso del canal y las capacidades. Se requieren de otros tres componentes, Q.931, RAS y RTP/RTCP

2. Gateway. Es opcional en la conferencia H.323, proporciona muchos servicios, el más común es la conversión entre los puntos finales de H.323 y otros tipos de terminales, además establece el enlace entre las terminales analógicas de la red PSTN y el enlace con terminales remotas bajo el estándar H.320 basadas en ISDN. Permite a dispositivos H.323 comunicarse con sistemas no H.323.

   Del lado de la red H.323 (comunicación con las terminales), un gateway corre señalización de control H.245, para intercambio de capacidades, señalización de llamada H.225 para inicio y terminación de llamada y H.225 RAS (Registration, Admissions, and Status) para registrarse con el Gatekeeper. Del lado de la PSTN, el Gateway corre protocolos propios de esta red como ISDN y SS7, el Gateway traduce estos protocolos de un modo transparente a su correspondiente parte del lado de la red que no es H.323 y viceversa. Los Gateways deben traducir entre CODECs de audio y video Sin embargo el Gateway no es requerido para comunicaciones entre dos terminales dentro de la red H.323.

3. Gatekeeper. Es el componente más importante de la red H.323. Actúa como el punto central de todas las llamadas en una zona y proporciona el control de servicios para registrar los puntos terminales. El Gatekeeper tiene dos funciones principales de control, la primera traslada la dirección de red de las terminales y gateways a IP e IPX lo cual es realizado con la especificación RAS. La segunda es el manejo del ancho de banda.

Un gatekeeper es un componente opcional, cuando está presente todas la terminales, gateways y MCUs se debe registrar a él. El Gatekeeper puede autorizar el acceso a la LAN en base a la disponibilidad de ancho de banda o autorización de las llamadas. Un gatekeeper puede ser configurado para limitar el ancho de banda o permitir sólo cierta cantidad de llamadas simultáneas. La especificación RAS es la encargada de la función de administración de ancho de banda realizada por el Gatekeeper.

El gatekeeper puede negar el realizar más conexiones una vez que ha sido alcanzado el ancho de banda máximo, de esta forma se puede especificar el número máximo de conferencias simultaneas, el ancho de banda restante permanece para las demás transmisiones en la red. Una característica opcional de un gatekeeper es la de enrutar llamadas, cuando la llamada es enrutada a través de gatekeeper, éste permite un control más efectivo y se tiene más información de la llamada lo cual puede ser utilizada para tarificar llamadas o re-enrutar llamadas hacia otro sistema cuando el usuario destino es inalcanzable.El Gatekeeper provee además servicios importantes como direccionamiento, autorización y autentificación de terminales y Gateways además de generación de usuarios.

4. Multipoint Control Units (MCU). Bajo H.323 consiste en un Controlador Multipunto (MC). El MC maneja las negociaciones H.245 entre todas las terminales para determinar las capacidades comunes de audio y video, además soporta conferencias entre tres o más puntos finales. Los participantes envían su información de control hacia la MC, de tal forma que la información sobre las capacidades soportadas por cada punto final puedan ser negociadas.

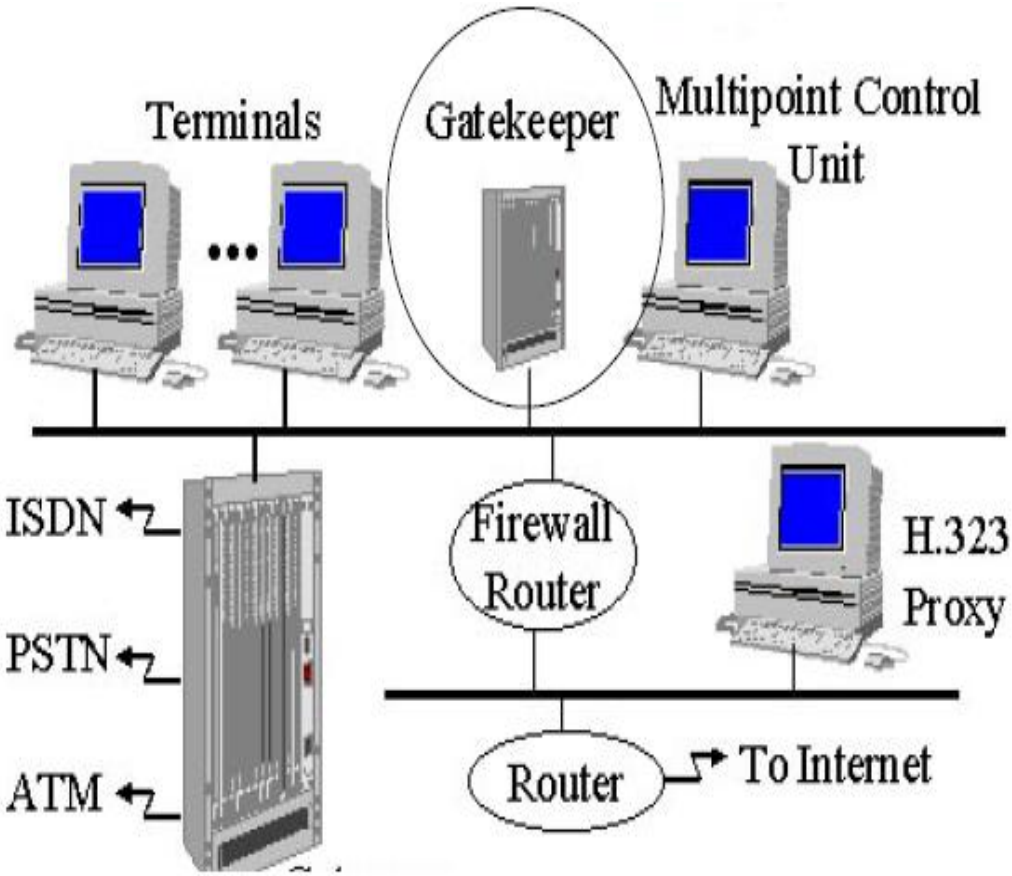



Fig. 8.2 Componentes de una red de telefonía IP

- **Protocolo SIP**

SIP (RFC 2543) es un protocolo basado en texto y es cliente–servidor. Proporciona los mecanismos necesarios para que los sistemas de usuario final y servidores proxy puedan dar sus diferentes servicios como los son: seguimiento de llamada, número de identificación, movilidad, capacidades de negociación entre terminales, transferencia de llamadas, mensajes instantáneos y control de dispositivos de red. SIP maneja señalización de llamada, localización de usuario y registro básico, tarificación y QoS.

Con SIP los usuarios tienen la capacidad de moverse a otras localidades y recibir las características de telefonía desde cualquier localidad remota vía el registro remoto. SIP contiene un punto de establecimiento punto a punto y conferencias multipunto, así como simples llamadas en punto final de señalización a través del servidor proxy. La mayoría de las características de telefonía son soportadas por este protocolo.

En SIP existen dos tipos o modos de servidores de red definidos:

1. Redirect server. El redirect server, es en el cual el usuario puede mandar un requerimiento de invitación de llamada a otra persona. Este redirect server entonces buscará por las posibles localizaciones del usuario llamado y enviará la correspondiente SIP-URL de regreso a quien llama. Basado en esta información, el que llama podrá entonces intentar contactar a otro usuario directamente.

2. Proxy server. Es el servidor que provee servicios de: a) Seguridad, con políticas de control de admisión, enfatiza a quien puede llamar y de quién puede marcar y eventualmente informa mediante reportes de uso. b) Servidores que implementan los servicios como llamadas perdidas, reenvío, proyección, etc. c) Ruteo: Encuentra el lugar a donde debe ser dirigida la llamada.

SIP puede ser utilizado para invitar participantes en ambos tipos de sesiones unicast y multicast y el iniciador de la invitación no tiene forzosamente que participar en la sesión.

En SIP se cuenta con el ENUM (E.164[2] Número Mapping) el cual es el encargado de resolver las llamadas en diferentes dominios y el ruteo basado en número telefónico, esto debido a que hoy en día cada fabricante emplea sus propias implementaciones de direccionamiento incluyendo tablas de ruteo para la traslación de lo marcado. ENUM consiste de una arquitectura basada en DNS y un protocolo que mapea los números SIP a los números URL dentro de un registro. Estos registros definen los servicios que son asociados con un número en particular, incluyendo fax, correo electrónico, mensajes instantáneos, páginas web personales, etc.

Al igual que el correo electrónico que utiliza URL´s las direcciones SIP utilizan el formato de datos, por ejemplo:

sip: jiri@iptel.org
sip: voicemail@iptel.org? Sujeto=dirección
sip:sales@hotel.xy; geo.position:=48.54_123.84_120

- **Protocolo MGCP (Media Gateway Control Protocol)**

MGCP nace de Internet Protocol Device Control (IPDC) y Signal Gateway Control Protocol (SGCP). IPDC es un conjunto de protocolos que pueden desempeñar el control de conexión,

[2] E.164 es el nombre de la normativa que define el plan de numeración telefónica internacional que administra la Unión Internacional de Telecomunicaciones (UIT).

control de media, y señalización del transporte entre circuitos conmutados e Internet. SGCP es un protocolo basado en UDP y diseñado en el concepto de direccionamiento de red que combina voz y datos en una red IP.

El MGCP es, en esencia, un protocolo maestro/esclavo, donde se espera que los gateways ejecuten comandos enviados por el MGC. El maestro es el MGC ('softswitch' o 'call agent') y el esclavo es el MGW (que puede ser un GW de VoIP, un DSLAM, un router MPLS, un teléfono IP). El Protocolo de Control de Media Gateway (MGCP) es usado para controlar los gateways de telefonía desde los elementos de control de llamadas externos llamados Media Gateways Controllers (MGC) o Gatekeepers.

MGCP asume una arquitectura de control de llamada, donde la inteligencia del control de la llamada está fuera de los gateways y manejada por un elemento de control de llamada externo. El MGCP asume que estos elementos de control de llamadas o MGC, se sincronizarán entre sí para enviar comandos coherentemente a los gateways que están bajo su control.

Lo que se propuso con MGCP fue sacar el control de la señalización del propio gateway (GW), llevándolo al MGC que se encargará del control de los media gateways'(MGW). En MGCP se puede decir que se ha separado la inteligencia (las funciones de control) de los datos.

- **Protocolo Megaco/H.248**

Se especifica en el RFC 3015. El protocolo H.248 o Megaco permite la conmutación de llamadas de voz, fax y multimedia entre la red PSTN y las redes IP de siguiente generación. El protocolo Megaco, que tiene su origen en el protocolo MGCP proporciona un control centralizado de las comunicaciones y servicios multimedia a través de redes basadas en IP. Megaco está adquiriendo solidez en el mercado porque permite una mayor escalabilidad que H.323, y da respuesta a las necesidades técnicas y a las funciones de conferencia multimedia que se pasaron por alto en el protocolo MGCP. Funcionalmente, Megaco es un protocolo de señalización utilizado entre los elementos de una arquitectura distribuida que incluye media gateway y controladores de media gateway (conocidos a menudo como softswitches, gatekeeper o call server)

Megaco y MGCP son protocolos que operan como maestro-esclavo, modo de requerimiento-respuesta, y notificación de eventos. Megaco está basado y considerado similar a http, soporta multimedia, usa terminación y los conceptos de contexto para manejar, llamadas y definir su estado.

H.248 es el resultado de la cooperación entre la ITU y el IETF. Antes de lograr esta cooperación existían varios protocolos similares compitiendo entre sí, principalmente MGCP (la combinación de SGCP e IPDC) y MDCP. H.248 se considera un protocolo complementario a H.323 y SIP, ya que un Media Gateway Controller (MGC), controlará varios Media Gateways utilizando H.248, pero será capaz de comunicarse con otro MGC utilizando H.323 o SIP.

Como vemos sean desarrollado diversos protocolos que buscan que las redes de datos y voz converjan en una sola; la implementación de redes de voz IP implica el cambio de equipos de red que permitan un control de tráfico y calidad de servicio entre otras cosas, lo cual se traduce en costos para las empresas que a su vez provoca que dicha convergencia vaya todavía a paso lento en su implementación.

# MÓDULO IX

# MICROONDAS Y SATÉLITES

Este módulo se divide en dos partes, en la primera se da un panorama general de la forma en cómo se llevan a cabo los enlaces inalámbricos a gran escala por medio de microondas, en la segunda parte se estudiaron a las redes de satélites, cuales son sus sistemas y componentes principales.

## 1.- MICROONDAS

- **Fundamentos de la redes de microondas**

Hoy en día las redes de microondas son una de la formas que permiten enlazar ciudades o localidades las cuales se encuentran distantes entre sí, esto gracias a su costo relativamente bajo y su fácil instalación, para poder entender como es que esto se lleva a cabo es necesario definir algunos conceptos que hacen posible que existen las redes de microondas.

Cualquier transmisión tanto de radio como de televisión se hace a través de las denominadas Ondas Electromagnéticas. Este tipo de ondas se caracterizan por que están formadas, como su nombre indica por la conjunción de un campo eléctrico y otro magnético. La unión de estos campos es la que permite que este tipo de ondas se pueda transmitir por el espacio independientemente de cuál sea su frecuencia a la velocidad de la luz; a la particularidad que tiene este tipo de ondas de viajar por el espacio es a lo que se le denomina técnicamente como propagación de las ondas electromagnéticas.

***Onda Electromagnética***. Son ondas producidas por la oscilación o la aceleración de una carga eléctrica. La radiación electromagnética se puede ordenar en un espectro que se extiende desde ondas de frecuencias muy elevadas (longitudes de onda pequeñas) hasta frecuencias muy bajas (longitudes de onda altas). Las ondas de radio tienen una longitud de onda que puede ser desde miles de metros hasta 0.3 metros, para las microondas van desde 0.3 metros hasta 1 milimetro.

La luz visible es sólo una pequeña parte del espectro electromagnético. Por orden creciente de longitudes de onda (orden decreciente de frecuencias), se han ordenado en una escala denominada espectro electromagnético. Se denomina espectro electromagnético al conjunto de ondas que van desde las ondas con mayor longitud como las ondas de radio, hasta los que tienen menor longitud como los rayos Gamma.

Una onda electromagnética se define con tres parámetros:

- *FRECUENCIA*.- Define el número de ondas que se transmiten por segundo.

- *VELOCIDAD*.- Las ondas electromagnéticas no necesitan un medio material para propagarse; pueden atravesar el espacio desplazándose en el vacío a una velocidad aproximada de 300.000 km/s a la que se denomina con la letra *c*.

- *LONGITUD DE ONDA*: Es el resultado de dividir la velocidad de propagación (velocidad de la luz) por la frecuencia.

- **Las microondas**

Las microondas son las ondas electromagnéticas que comprende el rango de frecuencias entre 300 Mhz. y 300 Ghz. y entre 30 cm. y 1 cm. El rango de las microondas incluye las bandas de:

- UHF (ultra-high frecuency 0.3—3 Ghz).
- SHF (super-high frecuency 3—30 Ghz ).
- EHF (extremely high frecuency 30—300 Ghz).

Las microondas pueden ser generadas de varias maneras, generalmente son producidas por dos tipos de dispositivos:

- *Dispositivos de estado sólido.* Los dispositivos de estado sólido para microondas están basados en semiconductores de SILICIO O ARSENURIO DE GALIO, e incluyen transistores de efecto de campo (FET), transistores de unión bipolar (BJT), diodos GUNN y DIODOS MPATT.

- *Dispositivos basados en tubos de vacío*. Son dispositivos que trabajan bajo la influencia de campos eléctricos y magnéticos entre los que se incluyen el magnetrón, el klystron, el TWT. El magnetrón es usado en el horno de microondas a una frecuencia de 2.45 Ghz. rotando las partículas de agua.

La propagación de Microondas depende de diversos factores como los son:

- *Zona de Fresnel* (60%). Es el volumen de espacio entre emisor y receptor RF (radio frecuencia) de manera que el desfase entre las ondas en dicho volumen no supere los 180º. Fresnel definió una zona que hay que tener en cuenta además de tener, visibilidad directa entre antenas. Realmente definió una serie de zonas. La zona 1 contribuye positivamente a la propagación de la onda, la segunda negativamente, la tercera positivamente, la cuarta negativamente, y así sucesivamente.

- *Difracción* (Loss). Es un fenómeno que consiste en la dispersión y curveado aparente de las ondas cuando encuentran un obstáculo.

- *Factor K*. Es un índice de radio efectivo de la tierra el cual ha sido desarrollado para que estadísticamente se describan los efectos de refracción de las ondas electromagnéticas en el medio debido a que la tierra no es totalmente plana.

- *Reflexión* (Multitrayectoria). Es el fenómeno que se da en una onda cuando ésta golpea algún tipo de material y éste no absorbe la energía de la onda provocando que ésta rebote.

- *Terreno y Obstrucciones*. Es causado por la presencia de obstáculos naturales como lo pueden ser árboles, o presencia de grandes lagos. En las ciudades es causado por la presencia de grandes construcciones.

- *Interferencia*. Puede ser causada por diversos factores como lo son las señales que son adyacentes en frecuencia a la señal deseada y que son producidas por la imperfección de los filtros en los receptores. También puede haber interferencia que surja en el receptor debido a la transmisión de otras señales de otros transmisores en la misma frecuencia.

## 1. Componentes básicos de un sistema de microondas

Un sistema de microondas consta de manera general de tres componentes los cuales se muestran en la siguiente figura.

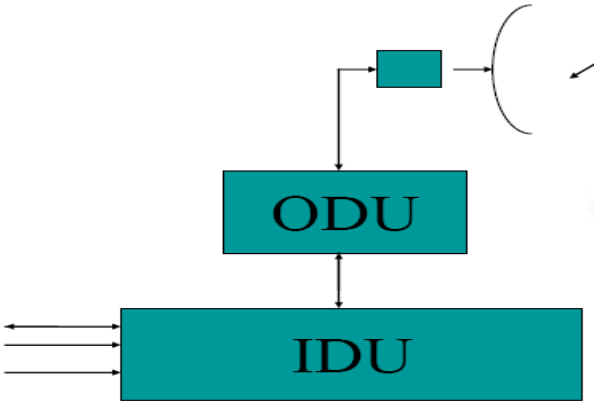



Fig. 9.1 Componentes de un radio de microondas

- **La unidad Indoor** o unidad interior cuenta con los siguientes componentes:

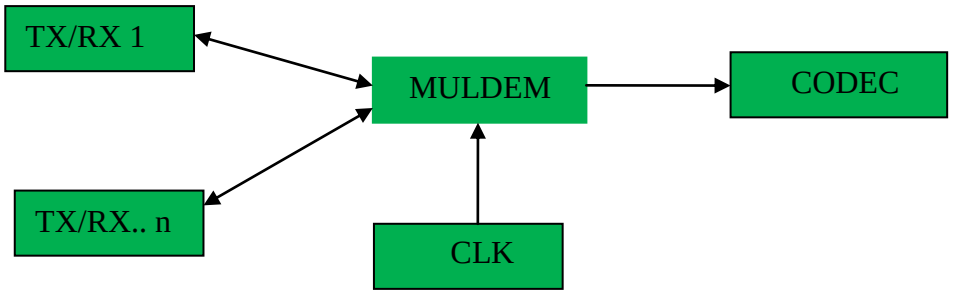
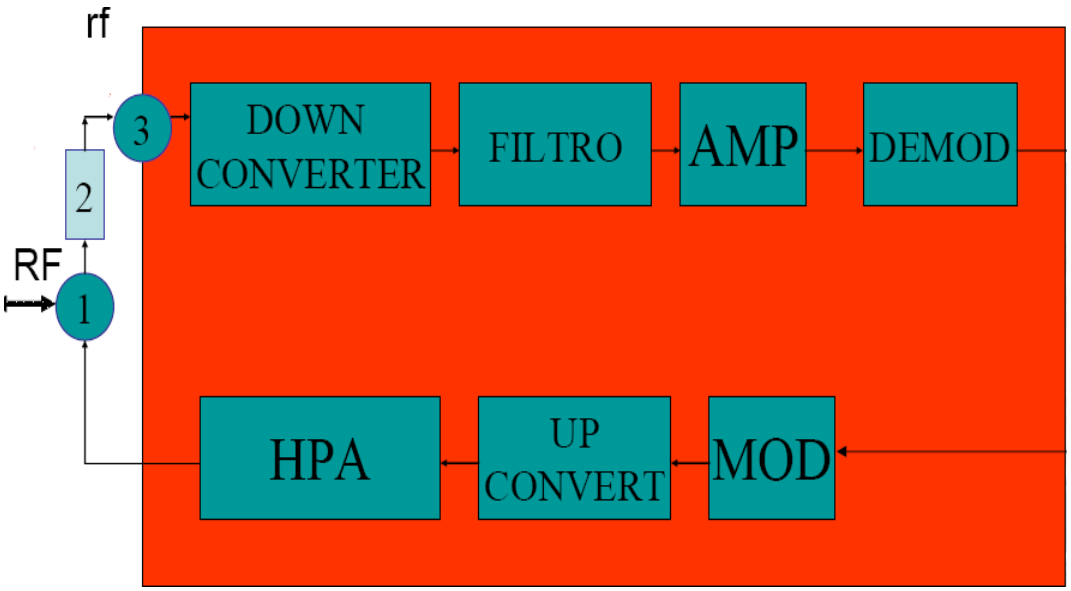



Fig. 9.2 Componentes principales de la unidad IDU

- *MULDEM*.- Es el componente encargado de multiplexar y demultiplexar los diversos afluentes de alguna cadena binaria.
- *CODEC*.- Es el encargado de convertir datos de analógico a digital y viceversa de digital a analógico.
- *TX/RX*.- Es el componente que transmitirá o recibirá la señal.

- **Unidad ODU** es la unidad que se encuentra en el exterior y estará conectado con la antena cuenta con los siguientes componentes.




1.-Circulador

2.-Filtro de línea

3.-Aislador

Fig.9.3 Componentes principales de la unidad ODU

- *Circulador*.- Es un dispositivo de 3 puertos que permite el flujo de la señal de rf a través de un puerto bloqueando el flujo a través del otro puerto.
- *Filtro de linea*.- Limita los productos de intermodulación, determina el ancho de banda para la sintonización del radio.
- *Aislador*.- Usado para prevenir la trayectoria de retorno de la señal de rf.
- *Down Converter.*- Baja la señal de rf a fi (frecuencia intermedia) típicamente 70 Mhz. algunos radios bajan la señal de rf efectuando una conversión intermedia.
- *Mezclador*.- la aplicación primaria de un mezclador es la combinación de una señal de entrada y una de referencia para obtener una sola señal de salida, idealmente la salida de un mezclador sólo contendrá las frecuencias de salida deseada frf+flo y frf-flo donde frf es la señal de rf y flo es la señal de oscilador local.
- *Filtro Saw*.- este dispositivo es básicamente un transductor el cual transforma las señales electromagnéticas a señales acústicas.
- *HPA*.-Es un amplificador que proporciona la potencia necesaria para poder enviar la señal al aire.
- *Up Converter*.- Es el encargado junto con el MOD de modular la señal que será enviada a la antena.

➢ **Antenas**

Las antenas para sistemas de microondas pueden ser divididas como:

- *Sistemas de Radiación Directa.*- enfocan el haz radiante usando un alimentador para iluminar una superficie curva reflejante. Las antenas parabólicas son un ejemplo típico.

- *Sistemas Periscopicos.*- estas antenas poseen un reflector parabólico que se coloca cerca del equipo de radio, con frecuencia en el techo de alguna caseta repetidora.

- *Sistemas Repetidores Pasivos*.- se refiere a un sistema usado para redirigir las señales de microondas, como un repetidor pero sin usar equipo de radio activo.

Toda antena posee las siguientes características técnicas:

- *Ganancia.* Es una característica de la antena que se define como la relación de la máxima intensidad en una dirección dada y la máxima radiación para un radiador.

- *Reciprocidad*. Este término se refiere al hecho que todas las propiedades de las antenas son las mismas tanto en la transmisión como en la recepción.

- *Patrón de radiación*. Son representaciones gráficas de la potencia relativa radiada por una antena en todas direcciones y pueden ser una representación polar ó rectangular.

- *Acoplamiento back to back*. Es la fracción de potencia expresada en dB (decibel) recibida por una segunda antena localizada exactamente detrás de la antena de transmisión.

- *Acoplamiento lateral.* Es la fracción de potencia expresada en dB recibida por una segunda antena localizada adyacente a la antena de transmisión y apuntando en la misma dirección.

- *Polarización*. Es la característica de las antenas para operar en una polarización vertical u horizontal y otras operar en polarización doble simultáneamente.

- *Ancho de banda*. Se refiere al rango de frecuencia en el cual la antena puede operar.

- *Operación duplex. S*e refiere a la capacidad de una antena de transmitir y recibir 2 ó más frecuencias simultáneamente.

- *Pérdidas de retorno.* Es una medida de la potencia relativa de reflexiones debido al desacoplamiento de impedancia.

- *Campo cercano y campo lejano*. El campo cercano se refiere a la región relativamente cercana a una antena en la cual el patrón de radiación es formado. A esta área se le denomina la región de Fresnel el campo lejano también llamado la región Fraunhofer es donde la intensidad varia con el ángulo y distancia. La línea divisoria entre el campo cercano y el campo lejano es conocida como la distancia del campo lejano y es una función del diámetro de la antena y de la frecuencia de operación y puede ser aproximada por: $Df = (2B^2)/\lambda$.

- *Envolvente del patrón de radiación.* Representa el máximo valor de la potencia transmitida o recibida en cualquier azimuth. Las envolventes del patrón de radiación son construidas para cada polarización y en polarización cruzada.

Las Antenas usadas tienen 2 grados de libertad:

- *Elevación.* Elevación: Ángulo entre el eje del haz de la antena y el plano horizontal.

- *Azimuth.* Es el Ángulo entre el plano vertical que contiene el eje del haz de la antena y la dirección del norte geográfico del lugar, medido en la dirección de las manecillas del reloj.

Para que un enlace esté perfectamente alineado los ejes centrales de la elevación y azimuth de las 2 antenas deben coincidir, esto garantizará el mejor nivel de Rx en ambos Radios.

- **Aspectos a considerar en el diseño de un enlace de microondas**

A manera de resumen de las características que conforman un enlace microondas se mencionaran los aspectos que debemos tomar en cuenta al momento de diseñar un enlace por medio de un sistema de microondas. Dichos aspectos se pueden dividir en dos, por una parte los referentes al estudio del medio en el cual se hará el enlace, entre los cuales podemos destacar:

1. Línea de vista entre puntos
2. Cercanía con la fuente de información
3. Posibilidad de uso de edificios como torres
4. Presencia de interferencias
5. Facilidades de alimentación y espacio
6. Accesibilidad
7. Considerar la curvatura de la tierra, factor “K”
8. Salvar la altura de la primera zona de fresnel
9. Considerar la existencia de vegetación y su crecimiento
10. Calcular la altura de las torres requeridas
11. Una vez que se tienen los obstáculos ubicados, se debe de conocer la altura de cada uno sobre el nivel medio del mar.
12. La altura de cada obstáculo se debe incrementar para considerar los efectos de la modificación de la curvatura de la tierra, las zonas de fresnel y la vegetación.
13. Con las alturas incrementadas, se traza una línea recta que sea capaz de unir ambos extremos pero salvando todos los obstáculos.
14. Si la línea recta no es horizontal, se tienen entonces ángulos de elevación y de bajada en los extremos. Se debe de jugar con estos ángulos para minimizar el tamaño de las torres en los dos extremos.

Otras de las características que se deben tomar en cuenta son las técnicas las cuales determinaran la calidad del enlace, dentro de éstos se encuentran:

1. Parámetros técnicos de los radios de microondas
2. Frecuencia de Operación
3. Potencia de Tx
4. Estabilidad de Frecuencia
5. Sensibilidad del Receptor
6. Ganancia del Sistema
7. Tiempo medio entre fallas
8. Margen de dispersión
9. Relación Portadora Ruido

## 2.- SATÉLITES

Un satélite es un cuerpo que gira alrededor de otro de masa preponderante y cuyo movimiento está principalmente determinado, de modo permanente, por la fuerza de atracción de este último, se clasifican en dos tipos, naturales y artificiales, estos últimos a su vez son clasificados respecto a su órbita y su aplicación.

Con respecto a su órbita se clasifican en:

- *Satélites de Órbita Baja*. Estos satélites tienen una altitud sobre el nivel del mar de entre 250 a 1,500 Km., tienen como ventaja que poseen poco retraso en las comunicaciones requieren baja potencia, se usan comúnmente en aplicaciones de comunicación móvil y observación de

la tierra.

- *Satélites de Órbita Polar*. Su altitud sobre el nivel del mar es de 500 a 800 Km, sobre eje polar, al rotar alrededor de la tierra puede observar cualquier región del planeta, es usado comúnmente para aplicaciones de clima y navegación.

- *Satélites de Órbita Elíptica*. Tiene una altitud sobre el nivel del mar en perigeo de 200 a 1,000 Km. y en apogeo de 39,000 Km., son comúnmente usados para servicios de comunicación.

- *Satélites de Órbita Geoestacionaria*. Tienen una altitud sobre el nivel del mar de 35,790 Km. sobre el plano ecuatorial. Por rotar a la misma velocidad de la tierra, el satélite se percibe como un punto fijo en el espacio. Se utiliza comúnmente en aplicaciones como servicios de comunicación fijos y móviles, clima y navegación (GPS).

Un sistema de comunicación satelital consta básicamente de un ***segmento espacial*** el cual consta del satélite y su estación o centro de control, y ***segmento terrestre*** que es el conjunto de estaciones terrenas (antenas y equipos de comunicación asociados) que están ubicadas dentro del área de cobertura del satélite, con capacidad de transmitir y/o recibir la información requerida por los usuarios del sistema en forma de señales de radiofrecuencia. Pueden encontrarse en tierra firme o en vehículos de transportación terrestre, aérea o marítima.

En cualquier estación terrena podemos encontrar, al menos, una de las siguientes secciones:

- **La Cadena Ascendente** que consta de los equipos que procesan las señales para su transmisión al satélite como lo son: El Modulador que genera una portadora en frecuencia intermedia (FI) modulada analógica o digitalmente, el Convertidor de Subida (Upconverter) que sintoniza la portadora de FI a la frecuencia requerida de transmisión, dentro del rango del enlace ascendente correspondiente a la banda de operación y el Amplificador de Alta potencia (HPA: High Power Amplifier) que proporciona a la portadora de RF la potencia que, aunada a la ganancia de transmisión de la antena, le imprimen el nivel adecuado para llegar al satélite.

- **La Cadena Descendente** es la que consta de los equipos que procesan las señales recibidas del satélite. Cuenta con un Amplificador de Bajo Nivel de Ruido (LNA: Low Noise Amplifier) que amplifica las señales recibidas por la antena, con un mínimo de ruido y distorsión, un convertidor de Bajada (Downconverter) que sintoniza la frecuencia de la portadora deseada y la traslada al rango de Frecuencia Intermedia (FI) y un demodulador que extrae la información contenida en la portadora de FI.

- **Componentes de un satélite**

Son dos los tipos de satélites que se encuentran en el espacio el primero de ellos fue el satélite de estabilización por giro, el cual ya está en desuso siendo reemplazado por el estabilizado por tres ejes en la figura se muestra estos dos tipos de satélites.

El satélite cuenta con dos secciones principales la carga útil (payload) y la plataforma o bus. La primera consta del equipo de comunicaciones que permite realizar el enlace entre las estaciones terrenas ubicadas dentro de su área de servicio, es la parte rentable del satélite. La segunda consta de la estructura y equipamiento necesario para que el satélite pueda operar adecuadamente en el espacio.

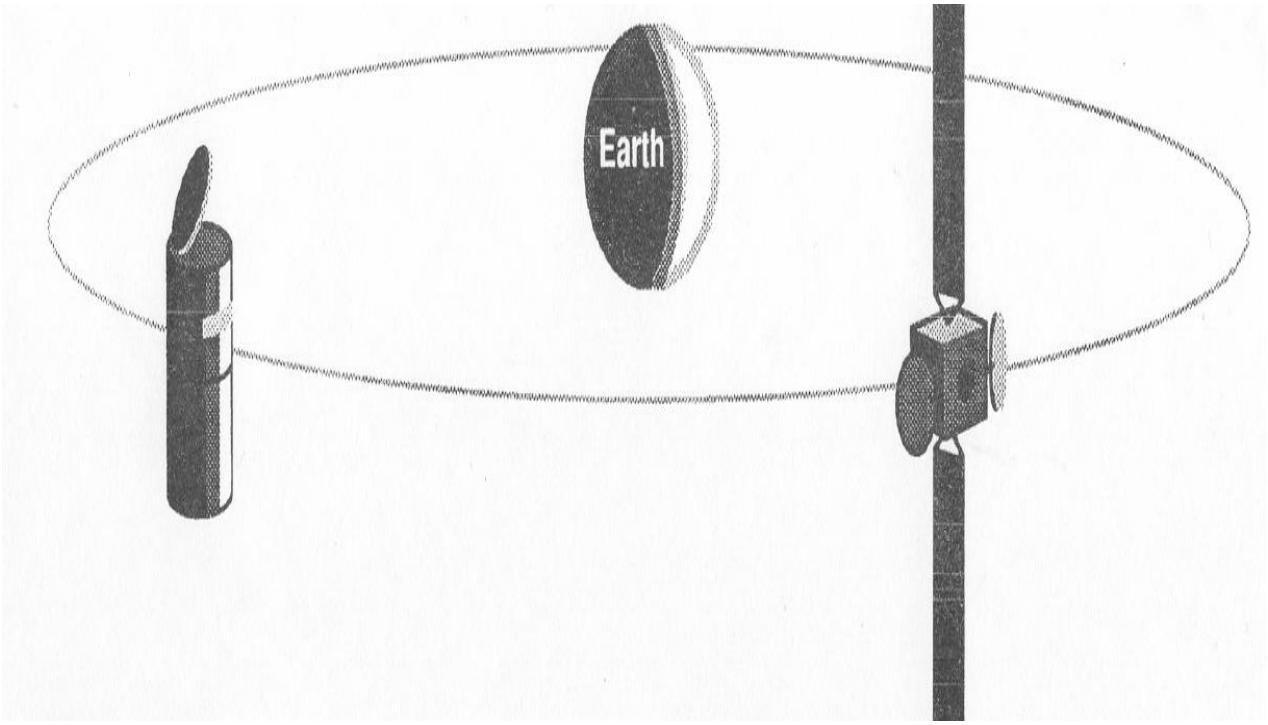



Fig. 9.4 Tipos de satélites, a la izquierda el estabilizado por giro
a la derecha el estabilizado por 3 ejes

La sección de payload está conformada por los siguientes elementos:

- **Subsistema de Antenas**. Reciben desde y transmiten hacia la tierra las señales de radiofrecuencia de los usuarios en las bandas de operación ( C, Ku, L, etc.) y polarizaciones ( V, H, RHCP, LHCP, etc.) para las que fue diseñado el satélite.

- **Canales o Transpondedores**. Son los elementos del subsistema de comunicaciones del satélite, conectados entre la antena receptora y transmisora, que se encargan de procesar las señales de los usuarios para su retransmisión a la tierra. Existen dos tipos de Transpondedores:

1. *Repetidores Convencionales* (“Bent Pipe”) que son los que no modifican las características de las señales transmitidas desde tierra.
2. *Transpondedor regenerativo*, el cual modifica las características de las señales transmitidas desde tierra, permite realizar cambios en las señales, como tipo de modulación o velocidad de información, entre las desventajas de ésto se encuentran que aumenta la complejidad del transpondedor así como la demanda de corriente por las unidades adicionales requeridas y por consiguiente el costo del satélite y del lanzamiento

Dentro de la sección de bus se encuentran los siguientes sistemas:

- **Subsistema de Potencia Eléctrica**. Proporciona energía eléctrica para la operación continua y eficiente de todos los subsistemas del satélite. Su fuente primaria de generación de energía es un conjunto de celdas solares (colocadas en la superficie del cuerpo cilíndrico o en arreglos planos), empleadas en operación bajo luz solar. Su fuente secundaria son baterías recargables,empleadas durante el lanzamiento y operación sin luz solar (eclipses).

- **Subsistema de Telemetría, Comando y Rango**. Permite realizar un enlace entre el satélite y su Centro de Control para realizar las funciones de Telemetría (envío de información del estado

de los subsistemas), de control, de rango (medición entre la estación de control y el satélite para conocer su posición exacta.

- **Subsistema de propulsión**. Mediante una serie de impulsores estratégicamente colocados en el cuerpo del satélite, permite aplicar fuerzas controladas para efectos de control de su posición u orientación. Se emplea para colocar el satélite en la órbita geoestacionaria realizar correcciones a la órbita del satélite o sacar al satélite de la órbita. geoestacionaria, una vez concluida su vida útil.

- **Subsistema de Control de Orientación**. Se emplea para mantener el correcto apuntamiento de las antenas del satélite hacia su área de cobertura y mantener continuamente orientados los paneles solares hacia el sol.

- **Subsistema de Control Térmico**. Regula la temperatura al interior del satélite.

- **Subsistema de Estructura**. Proporciona a los demás subsistemas el soporte, la estabilidad y la resistencia mecánica requerida en cada etapa de la misión.

De esta forma conociendo los diversos sistemas con los cuenta un satélite de comunicaciones nos damos cuenta de la complejidad de dichos equipos que a lo largo del tiempo han ayudado a acortar aún más distancias entre los países brindando servicios como los son televisión, telefonía, internet, telegrafía entre otras.

# MÓDULO X

# REDES INALÁMBRICAS

Hoy en día las redes inalámbricas se han popularizado de manera importante ocasionando que esta tecnología sea cada vez más barata y accesible al usuario. La implementación de una red inalámbrica se puede llevar a cabo sin tener que invertir grandes cantidades de dinero dependiendo de la cobertura que se desee tener. En este módulo se verán los elementos que componen una red inálambrica.

## ➢ Conceptos Básicos de las redes inalámbricas

Una red inalámbrica consta básicamente de los siguientes componentes:

- *El medio*. Es el aire en donde se viaja la señal así como la infraestructura cableada. El medio se encuentra en las siguientes capas:

  - Core Layer o BackBone. Es la infraestructura base del sistema inalámbrico.
  - Distribution Layer. Es la encargada de transmitir información del Core Layer a las entidades donde se conectan los usuarios.
  - Access Layer. Es el encargado de mantener al usuario en todo momento conectado al sistema.

- *Antenas*. Las antenas pertenecen al Access Layer.

- *Estaciones Móviles*. Son los dispositivos que permiten la interconexión con la interfaz área, pertenece al Access Layer.

- *Servicios o Servidores*. No son utilizados como dispositivos móviles pero son considerados parte de la redes inalámbricas, se localizan en la capa de Distribution Layer.

- *Punto de Acceso o Estación Base*. Es el dispositivo que posee una tarjeta de red para el medio cableado y un radio para la interfaz área. La tarjeta de red pertenece a la Distribución Layer y el radio a Access Layer. Es el encargado de recibir la información de los diferentes dispositivos cliente para su centralización o bien para su encaminamiento, se puede configurar a su vez en los siguientes modos:

  - Modo Raiz. Es el modo en el cual el punto de acceso (acces point) da servicio en un área determinada.
  - Modo Repetidor. Es el modo en el cual el access point da servicio en un área determinada y a su vez está interconectado hacia otro access point el cual dará servicio en otra área.
  - Modo Puente. Es el modo que permite crear puentes entre redes de tipo alámbricas e inalámbricas.

A su vez las redes inalámbricas se clasifican básicamente en 3 categorías:

- *Las Redes PAN* (Personal Área Networks). Trabaja bajo el estándar 802.15 también conocido como bluetooth, fue desarrollado por la IEEE, alcanza velocidades de 1Mbit/s con un promedio de 10 metros de alcance.

- *Redes WAN* (Wide Area Network) 802.20. Son todas aquellas redes que se pueden comunicar en distintas ciudades e incluso distintos países, acaparan desde 100 hasta 10,000 Km. de distancia aproximadamente, GSM y GPRS son ejemplo de estas redes.

- *Redes MAN* (Metropolitan Area Network) 802.16. Se le denomina como WI-MAX, cubren distintos sitios dentro de una misma localidad como lo es una ciudad, su distancia de cobertura es considerada de 1 hasta 10 kilómetros; este estándar podrá ser usado en frecuencias desde los 2 Ghz hasta los 11 Ghz.

- *Redes LAN* (Local Area Network) o WLAN. Son las redes más populares, los estándares más importantes en el mercado actual son: 802.11a con modulación OFDM a una velocidad de transmisión de 52 Mbps en la frecuencia de 5 GHz, 802.11b con DSSS a una velocidad de 11 Mbps en la frecuencia de 2.4 Ghz y 802.11g con DSSS a una velocidad de 52 Mbps en frecuencia de 2.4 Ghz.

Las WLAN ocupan principalmente 2 topologías o también conocidas como modos de funcionamiento o tipos de operación:

- Stand Alone (Ad-HOC). Es una red que consiste en un grupo de computadoras o clientes móviles que se comunican directamente unas con las otras, este tipo de red realiza una comunicación punto a punto. Los equipos que se quieren enlazar requieren de un dispositivo cliente configurado de igual manera en cada uno de los equipos, “SSID” (Service Set Identifier).

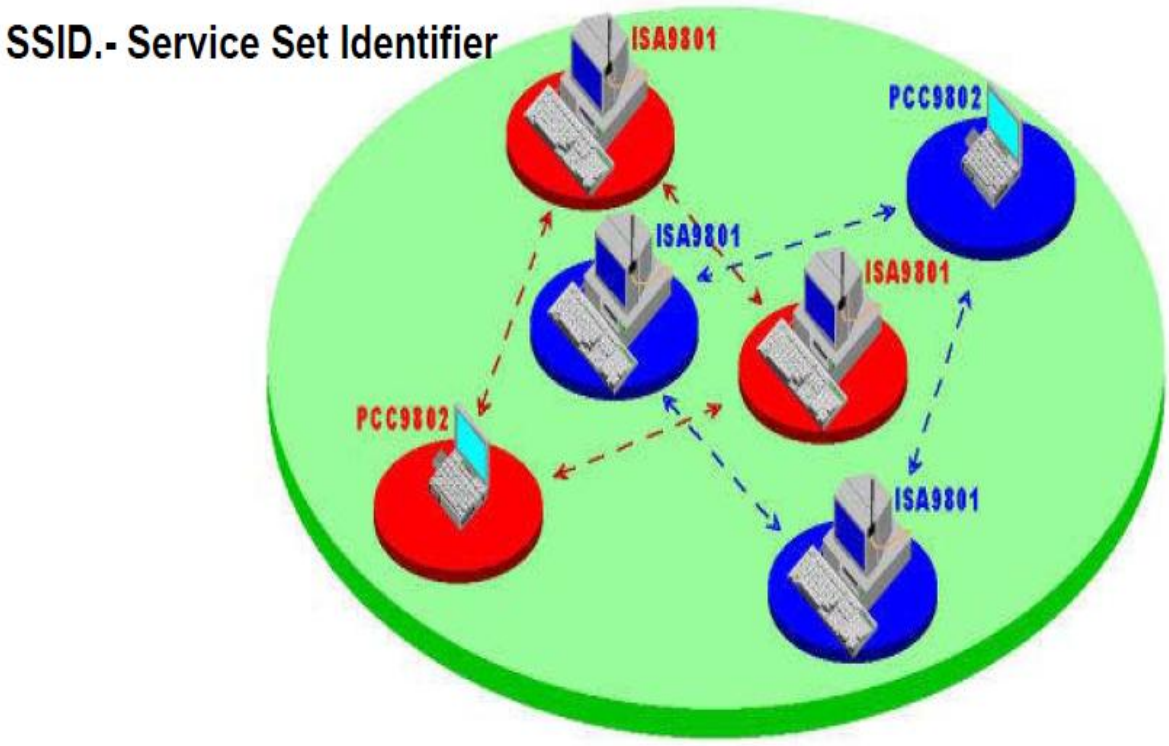



Fig.10.1 Esquema de red Stan Alone

- Infrastructure (Wired) BSSs. Ésta es la forma de trabajo en los que se utilizan los llamados Puntos de Acceso (Access Point), permiten trabajar con las distintas redes, dejando el trabajo de canalizar los datos al punto de acceso reduciendo así el 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. Esta forma de

funcionamiento es mejor que AD HOC, ya que con AD HOC los paquetes de información son enviados al aire con menos posibilidades de que lleguen a su destino.

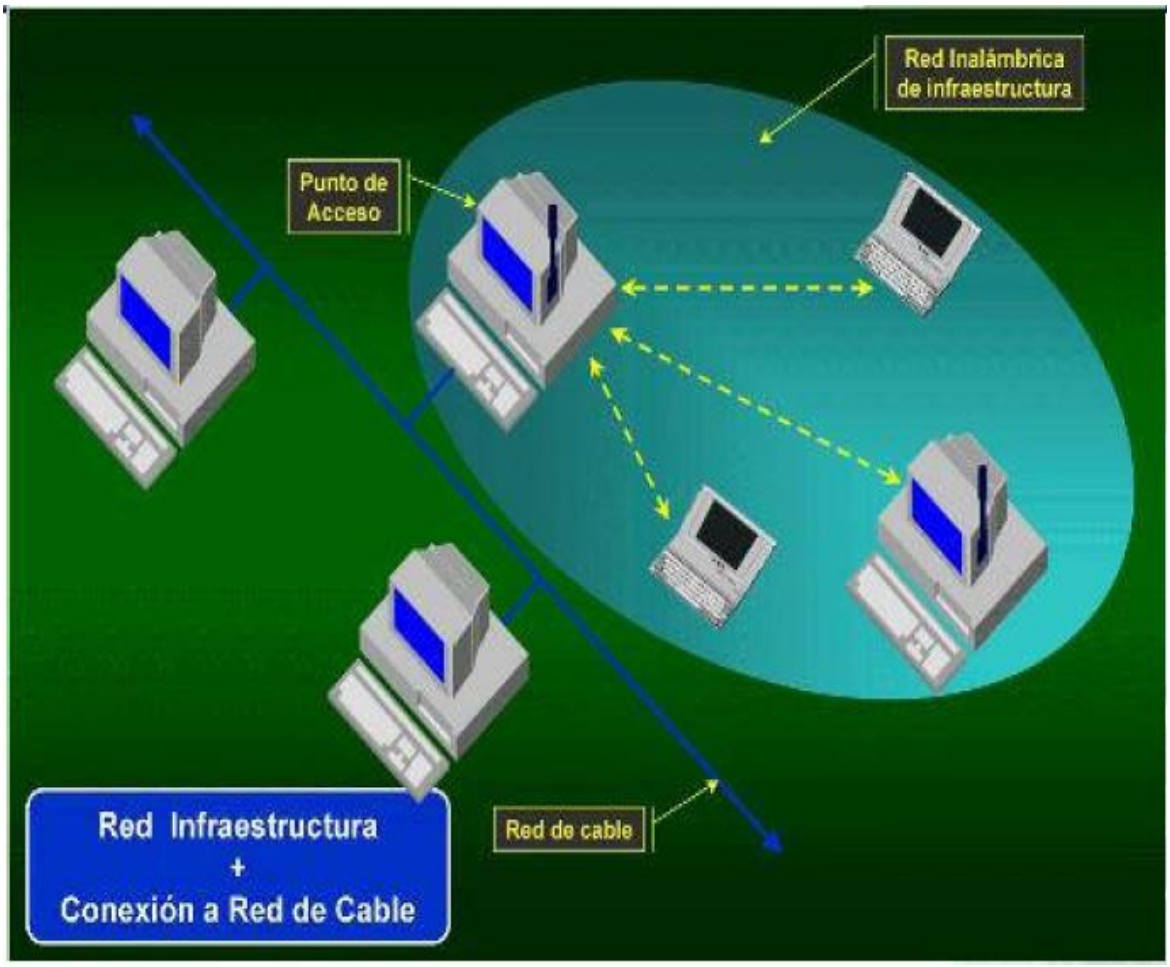



Fig. 10.2 Esquema de red Infrastructure

- **Técnicas de acceso múltiple al medio**

La transmisión de la información inalámbrica se realiza por medio de diversos canales de frecuencias cada uno de los canales es referenciado por su frecuencia central, cada canal contiene o transfiere información por arriba y debajo de esa frecuencia central. El ancho de banda del canal depende del esquema de modulación y sobre todo de la información que contiene el canal, si la información es más precisa mayor es el ancho de banda del canal.

Debido a la diversidad de señales existentes en el medio así como su utilización en diversas aplicaciones es la implementación de técnicas que hagan posible que por un solo canal se puedan transmitir más de una portadora (señal), entre las técnicas más utilizadas encontramos:

- FDMA: Frequency Division Multiple Access, 30 KHz. por canal, modulación FM, 1 y 3 watts.

- TDMA: Time Division Multiple Access, 30 KHz. por canal, 3 servicios por canal, modulación PSK, 600 miliwatts de potencia.

- CDMA: Code Division Multiple Access. No tiene canales se utiliza todo el espectro, una comunicación se identifica por un código y dominio digital, es decir ruido único para

distinguirlas unas de otras. El código es transmitido por un canal por separado con saltos cada 0.4s., por lo cual es necesario la sincronizar los saltos.

De esta forma se logra tener una reutilización de frecuencias útiles para así poder brindar acceso múltiple a la red a varios usuarios a la vez. En la figura 10.3 se muestra esquemáticamente la diferencia entre estas técnicas de modulación.

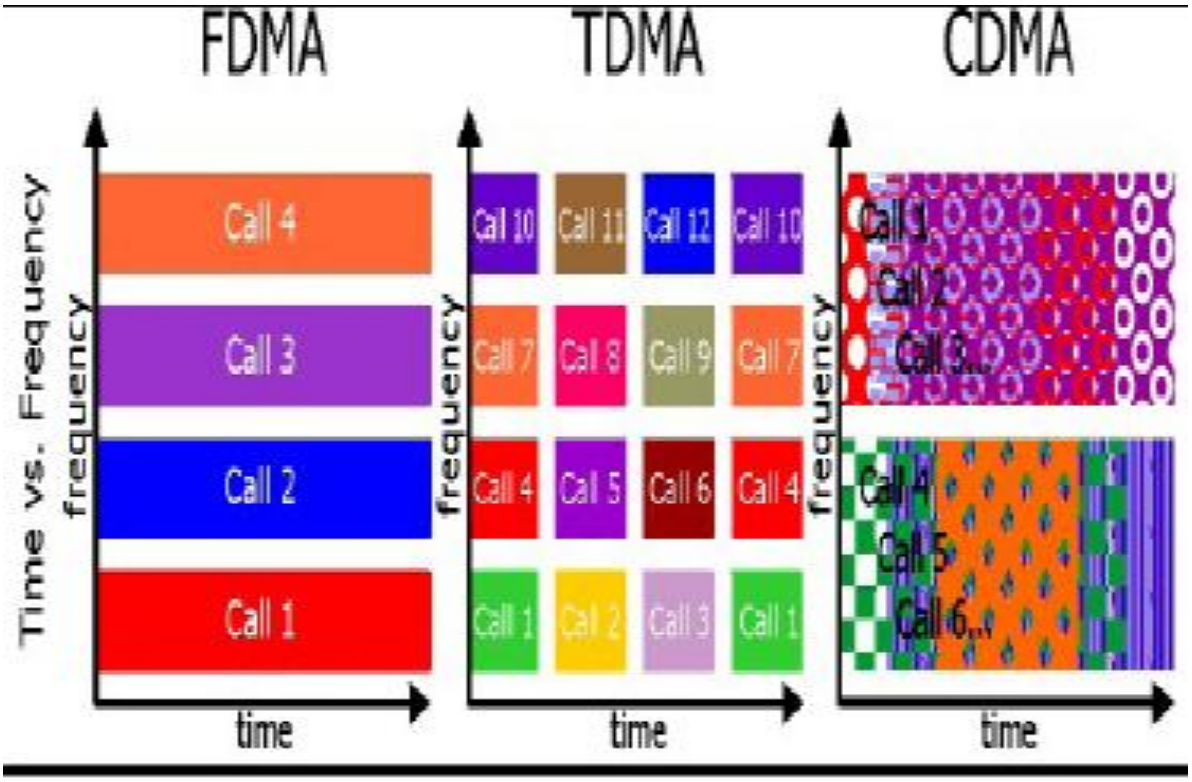



Fig. 10.3 Diversos métodos de acceso al medio representado por llamadas

- **Tecnología de Espectro Amplio (SS)**

Espectro Amplio es una técnica de codificación para la transmisión de señales digitales, diseñado para evitar interferencias o intercepción de las señales. Se caracteriza por su ancho de banda amplio y su baja potencia pico, es el sucesor de comunicaciones de banda angosta. Una señal en espectro amplio se usa cuando el ancho de banda es más amplio que lo requerido para enviar información.

La señal de espectro amplio es una señal parecida al ruido lo cual es una ventaja ya que el ruido es difícil de detectar, interceptar y modular sin el equipo apropiado, además el ruido no tiene crestas en su espectro que muestren información coherente.

La interferencia o modificación intencional de una señal es más difícil de realizar sobre una comunicación SS que una de banda angosta.

Por su parte la banda angosta se caracteriza por que más potencia es requerida para enviar una transmisión, cuando se utiliza una rango de frecuencias más pequeño su potencia debe ser mayor que el nivel del ruido, también llamado como ruido de pisó, para así asegurar una recepción libre de errores; otra de las desventajas que tiene la banda angosta es que sufre de interferencia y/o modificación de la señal debido a la presencia de señales no deseadas. Una portadora de banda angosta transfiere la misma cantidad de información que con espectro amplio pero con un rango

de frecuencia más grande. Los receptores de espectro angosto verán a una señal SS como si fuera ruido, no podrán demodularla o interpretarla.

Entre las tecnologías que hacen uso de la técnica de espectro amplio se encuentran:

WLAN 802.11 Wi-Fi
WPAN 802.15 bluetooth
WWAN 802.16 antenas semidirigidas

*TIPOS DE ESPECTRO AMPLIO*

Principalmente se utilizan dos tipos:

− **FHSS** (Frequency Hopping Spread Spectrum). Es la técnica que utiliza la agilidad de cambiar de frecuencia abruptamente dentro de la banda de radio, utiliza la frecuencia de 2.4 GHz. ISM (Industrial, Scientific, Medical) y una banda de 83.5 MHz. La señal portadora cambia de frecuencia, o salta (hops), de acuerdo a una secuencia seudo aleatoria llamada PN o Pseudo Noise.

El PN es una lista de frecuencias a la cual la portadora brinca en un intervalo de tiempo especificado, antes de repetir el patrón de la secuencia de nuevo

La portadora se mantendrá en cierta frecuencia por un tiempo especificado llamado “dwell time” el cual toma 400ms. en un periodo de 30 segundos por portadora en un solo recorrido de las frecuencias y 200ms. en un periodo de 30 segundos por portadora en dos recorridos de las frecuencias.

El tiempo que toma para saltar a otra frecuencia se llama Hop Time el cual se mide en microsegundos (200 a 300 microsegundos en 802.11 y 500-600 microsegundos en Bluetooth).

Cuando la lista de la secuencia (PN) se ha agotado se repite la secuencia de frecuencias, tanto el receptor como el transmisor deben estar sincronizados.

En un principio FHSS emitía a 1 Watt y tenía que recorrer 75 de los 79 canales o frecuencias, actualmente son 15 canales con una potencia de 125mW.

− **DSSS** (Direct Sequence Spread Spectrum). Es la técnica de enviar información donde el transmisor y receptor trabajan en frecuencias con una amplitud de 22MHz., el hecho de tener una cantidad amplia de canales permite transferir información a una taza de transferencia alta.

DSSS combina la señal de información con una secuencia de bits mejor conocida como “chipping code o ganancia de procesamiento”, una alta ganancia de procesamiento implica mayor resistencia a la interferencia.

En DSSS cada canal es una banda de frecuencias contigua de 22 MHz. de ancho con una señal de 1 MHZ. como portadora. El canal 1 abarca de 2.401GHz a 2.423 GHz. es decir “.412 GHz. ±11MHz.”, el canal 2 de 2.406GHz. a 2.429 GHz. es decir “.41 GHz ±11MHz”.

Distintos sistemas con DSSS que transmitan en canales traslapados en el mismo espacio físico causaran interferencia entre ellos

Debido a que los canales de 22MHz. que no se enciman tienen un espaciado de canalización de 3 MHz existe una referencia de 3 y 2 canales que no se interfieren. Por tal motivo existe una

posible coexistencia de 3 sistemas con DSSS en un mismo espacio en los canales 2 ,6 y 11. En la figura 10.2 se muestra de manera esquemática la distribución de los canales en el sistema DSSS.

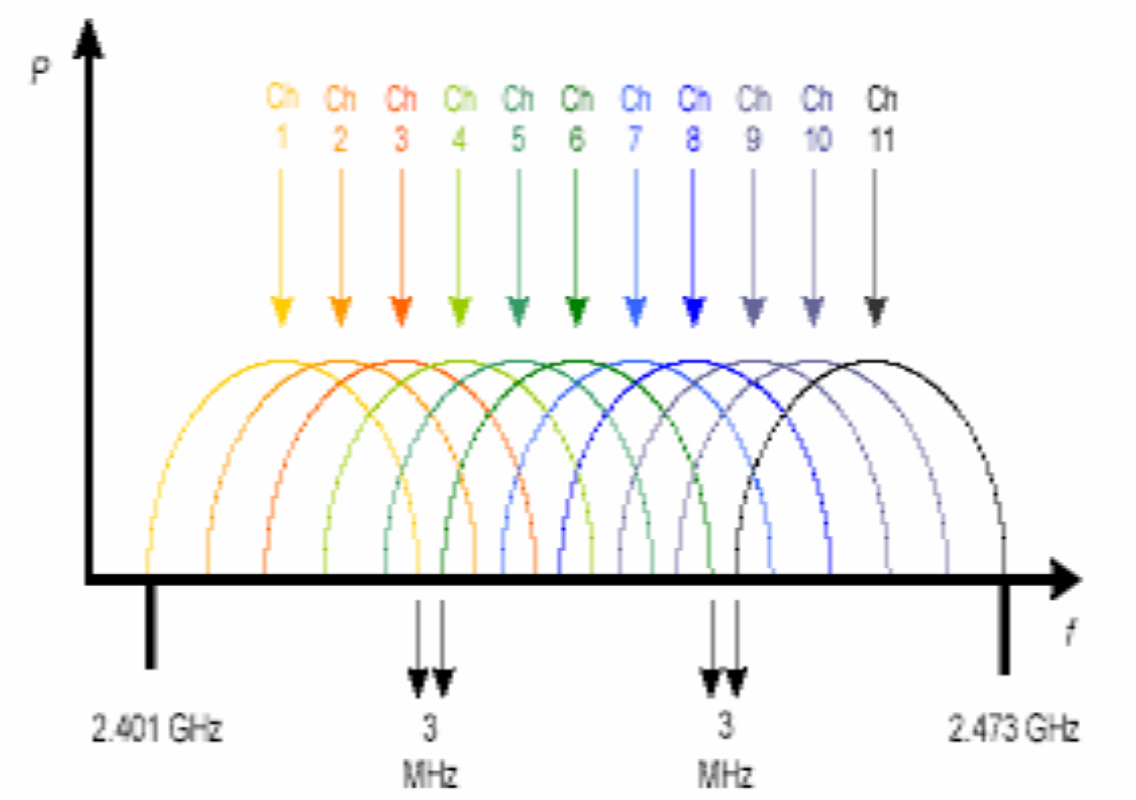



Fig.10.4 Distribución de canales del sistema DSSS.

- **Seguridad en las redes 802.11**

Una red que trabaja bajo protocolo el protocolo 802.11 ofrece los siguientes servicios de seguridad:

− *Autenticación*. Se distinguen dos métodos de autenticación:

- *Open System Authentication* (OSA). Es el método en el cual no se requiere algún tipo de encriptación para la transmisión de datos, lo que quiere decir que el texto viaja en claro. Con tan sólo configurar el SSID se podrá tener acceso a la red.

- *Shared Key Authentication* (SKA). Es el método en el cual la encriptación es requerida, las estaciones deben ser configuradas con algún tipo de algoritmo o llave de encriptación. Por ejemplo el uso de la clave WEP.

− *Control de Acceso*. Puede estar definido por las siguientes técnicas:

- *SSID*. Sin cifrado, sin confidencialidad es el nombre de la red que se indica tanto en el dispositivo Access Point como en los clientes al conocerlo se podrá acceder a la red sin mayor esfuerzo. Un dispositivo inalámbrico viene configurado de fábrica con un SSID, la

manera en que se configura es con una clave alfanumérica. No se cifra en las tramas de control por lo cual existen programas que pueden obtener de manera sencilla el SSID.

- *Dirección MAC*. Este método se basa en direcciones MAC que poseen los dispositivos clientes, una lista selectiva en donde sólo se dejara entrar a la red a los clientes que se encuentren registrados en ella. Las capas MAC están formadas por 12 caracteres alfanuméricos y tampoco se cifra al transmitirse. Utiliza autenticación OSA, SKA

- *WEP* (Wired Equivalent Privacy). Con este sistema se codifican o se cifran todos los datos enviados entre los distintos dispositivos inalámbricos, se puede habilitar o deshabilitar y especificar una clave para el cifrado de la información ya sea a 64 o 128 bits; entre mayor numero de bits, mayor será el nivel de seguridad, pero vuelve a la red con un menor rendimiento, la clave wep debe de ser configurada en cada uno de los equipos que pertenezcan a la red.

- *WPA* (Wireless Protected Access) (EAP/ 802.1x). Fue desarrollado por Wi-Fi Alliance basado en el draft 3 de IEEE 802.11i, utiliza un servidor de autenticación definido en el estándar IEEE 802.1X.

  IEEE 802.1X utiliza dos modos: Con un Servidor de Autenticación, el cual se utiliza en ambiente empresarial o institucional por lo cual es más seguro y PSK "pre-shared key", donde todos los clientes comparten una misma frase de 8 a 63 caracteres ASCII o 64 dígitos hexadecimal (256 bits), SOHO (personal mode). Las etiquetas o elementos de información son distintas en WPA y WPA2.

- *Temporal Key Integrity Protocol* (TKIP). Es un conjunto de algoritmos alrededor de WEP, diseñados para lograr una mejor seguridad en hardware con WEP.

  TKIP añade 4 principales mejoras a WEP. Añade una función adicional que mezcla la llave por paquete para evitar los ataques que hacen uso de la debilidad de generación de llaves, un nuevo proceso en la secuencia de generación de Vectores de Inicialización (IV) para evitar ataques de réplica, un nuevo mensaje de integridad, una función criptográfica message integrity check (MIC) para detectar modificaciones de bits y alteraciones de fuente y destino y una extensión del espacio del IV, para eliminar la reutilización de llaves (re-key).

- **Protocolo IEEE 802.15 (Bluetooth)**

Opera en ISM 2.4GHz utiliza 79 canales, en la frecuencia de 2.402 hasta 2.480 GHz, con una potencia de 1mW. a 100mW., generalmente alcanza una distancia nominal de 10 m., pero si se regula la potencia puede llegar hasta los 100m. La tasa de transferencia de datos es de 1Mbps, utiliza paquetes y transmisión de switcheo de circuitos

Una característica esencial para su desarrollo fue el de implementar todo en un chip CMOS para reducir costos, consumo de potencia y tamaño para dispositivos portátiles.

IEEE 802.15 utiliza la técnica de acceso o interfaz área de FHSS (Frequency Hop Spread Spectrum) con una banda completa de 79 canales de 1MHz. cada uno, cada canal se divide en slots o ranuras de tiempo de 625 microsegundos y tiene una taza de salto efectivo de 1600 saltos por segundo.

El Bluetooth es una de las redes que ha ganado popularidad ya que se encuentra en la mayoría de los dispositivos móviles, y tiene un costo bajo, permite el envió de archivos pequeños en poco tiempo; así las redes inalámbricas cobran importancia logrando que los usuarios tengan acceso a ellas sin tener que invertir grandes cantidades de dinero.

## MÓDULO XI

## SEGURIDAD EN REDES

En este módulo se estudió un aspecto fundamental que hoy en día se busca pueda poseer toda red de datos y en la cual se invierten cantidades importantes de recursos financieros, la seguridad. Se pretende garantizar que los sistemas puedan transportar la información sin que ésta sea modificada o reemplazada durante su transporte y que pueda llegar integra a su destino final.

La seguridad informática surge después de que se ha visto que es posible llevar a cabo el robo de información en los sistemas informáticos; el robo de información así como la alteración de ella se ha utilizado para realizar grandes fraudes, usurpar funciones, o robar la identidad de alguna persona o empresa, lo cual se ha traducido en grandes pérdidas.

### ➢ Tipos de ataques informáticos

El robo de información se puede realizar de varias formas algunas de la cuales se deben a las vulnerabilidades de los sistemas, otros hacen uso de la confianza e ignorancia que el usuario tiene acerca de los sistemas informáticos; entre las técnicas más utilizadas para el robo de información tenemos:

- **URL falsos o maliciosos**. Es el ataque que consiste en falsificar o hacer pequeñas variaciones en direcciones URL legítimas, engañando de esta manera al usuario haciéndole creer que está ingresando a una página web legitima cuando no es así, por lo que el atacante adquirirá los datos que el usuario ingrese en dicha página.

- **Cross site scripting**. Son los ataques que permiten ejecutar código de "scripting", como VBScript o JavaScript en las páginas que algún usuario visita, no percatándose de la ejecución del mismo.

- **Sesiones preestablecidas**. Para seguir a los usuarios de una aplicación y administrar los recursos mediante autenticación se usan identificadores de sesión tales como: cokies, campos ocultos, campos que forman parte del URL. Con esto el atacante usa una página legitima pero inserta un identificador de sesión al que vigila hasta que aparezca una página restringida.

- **Ataques encubiertos**. Consiste en suplantar el contenido original de una página, o que existan marcos escondidos en ejecución adquiriendo así algún tipo de información.

- **Obtención de datos del usuario**. Consiste en obtener registros de lo que está tecleando el usuario o capturar de flujos de clicks.

- **Vulnerabilidades de los clientes**. Es el ataque el cual se logra debido a que el usuario permite la ejecución de programas los cuales hacen uso de recursos del sistema como lo pueden ser memoria o que exploran el sistema de archivos de los mismos.

- **Hombre en medio**. Un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

- **DoS** (denegación de servicio). Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por consumo del ancho de banda excesivo de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Se genera mediante la

saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no dé abasto a la cantidad de usuarios.

Sin embargo los ataques informáticos también se pueden llevar a cabo a nivel de red local, por lo cual se hace necesario establecer políticas de vigilancia de los paquetes, haciendo de esta manera necesario la implantación de un ente vigilante de los paquetes que será el encargado de aceptar conexiones únicamente de ciertas direcciones IP, aceptar conexiones únicamente de intervalos de direcciones IP, aceptar conexiones únicamente de computadoras con ciertos nombres y usuarios autorizados, rechazar conexiones fuera de horas permitidas, registrar la actividad de servicios seleccionados cuando las conexiones son aceptadas o rechazadas. Este ente también será el encargado de aislar nuestra red local del mundo de exterior de las redes (internet).

Cada computadora o dispositivo conectado a internet tendrá una dirección única o un nombre único, se vuelve necesario la identificación de alguna máquina por medio de un nombre y no sólo por su IP ya que el usuario encuentra difícil recordar direcciones numéricas que nombres comunes. El servidor encargado de traducir la dirección IP asignada a una máquina por un nombre se le conoce como DNS (Domain Name System). Existe un problema más de seguridad en este tipo de servicios de resolución de nombres, un atacante puede recurrir a sustituir la dirección real de un servidor por otra en donde se encuentra un servidor malicioso, así el usuario estaría entregando información importante a un servidor que no es el real, esto se logra suplantando el nombre de la computadora real por otra, haciendo creer al usuario que está en el sistema correcto.

Por otra parte la inseguridad de las redes no sólo se da a nivel de usuario ya que pueden existir ataques o robos de información que hacen uso de algunas vulnerabilidades que existen en los equipos de red, o de los protocolos que usan algunas aplicaciones para su funcionamiento. Se podría mencionar por ejemplo el uso de aplicaciones como Telnet en el cual toda la información que viaja por la red va en claro permitiendo que alguna persona que coloque un sniffer obtenga datos de los sistemas como podrían ser contraseñas o nombres de usuario. Otro ejemplo de protocolo usado en los equipos red en el cual se han encontrado vulnerabilidades de seguridad es el SNMP el cual se mencionará a continuación.

- **Protocolo SNMP (Simple Network Management Protocol)**

El SNMP es el protocolo que permite supervisar, analizar y comunicar información de estado entre una gran variedad de hosts, pudiendo detectar problemas y proporcionar mensajes de estados. Se utiliza para monitorear los dispositivos adjuntados a una red, supervisando el desempeño de la red, buscar y resolver problemas.

SNMP consiste de un conjunto de estándares para la administración de redes, incluyendo un protocolo de capa de aplicación, un esquema de base de datos y un conjunto de objetos de datos. El SNMP consiste básicamente de 3 elementos:

- **Agente**. Es una entidad SNMP en algún dispositivo: servidor, router, firewall, switch, etc., que tiene información almacenada en un MIB. Provee la interface entre el manager y el dispositivo físico administrado, actúa como servidor, y se ejecuta en cualquier dispositivo de red que tenga soporte para SNMP.

- **Manager**. Es un cliente en la red que accede al MIB del agente para obtener información. El Manager provee la interfaz entre el usuario administrador de red y el manager del sistema, administra dispositivos de red y se ejecuta en PCs (sistemas Windows y/o Unix).

- **MIB**. Es un grupo de variables asociadas con algún dispositivo de red, donde se almacena información del objeto administrado. El Manager y el Agente utilizan el protocolo Management Information Base (MIB) y un conjunto relativamente pequeño de comandos para intercambiar información.

El protocolo SNMP consta de los siguientes mensajes básicos:

- GetRequest. Utilizado por el manager para obtener información de variables específicas.

- GetNextRequest. Utilizado por el manager para obtener la siguiente información del objeto administrado.

- GetBulk. Utilizado por el manager para obtener un grupo de variables.

- SetRequest. Utilizado por el manager para realizar cambios a un valor de alguna variable en específico.

- GetResponse. Utilizado por el agente para enviar la información pedida por el manager.

- TRAP. Es utilizado por el agente para enviar mensajes “espontáneos” al manager para notificar eventos importantes. Existen algunos mensajes Traps disponibles para ser mandados a la estación de monitoreo:

    -coldStart
    -warmStart
    -linkDown
    -linkUp
    -authenticationFailure
    -egpNeighborloss
    -enterpriseSpecific

Los mensajes GetNext y GetBulk son utilizados cuando Manager no conoce el MIB del Agente. Esto es importante, ya que esto permite al Manager revisar la base de datos del MIB entera sin previo conocimiento. A esto se le conoce como MIB walk

La mayoría de firewalls, routers y servidores guardan sus estadísticas operacionales en Identificadores de Objeto (OIDs). Los OIDs consisten en números separados por puntos decimales (1.3.6.1.4.1). El MIB asocia a cada OID una etiqueta legible (por ejemplo dpsRTUAState1) y otros parámetros relacionados con el objeto. Por lo que el MIB sirve como un diccionario de datos o “code book” que es utilizado para ensamblar e interpretar los mensajes de SNMP.

Cuando un SNMP manager quiere “saber” el valor de un objeto, tal como el estado de un punto de alarma, el nombre del sistema o cualquier otra característica, ensamblará un paquete GET que incluya el OID de cada objeto de interés. El elemento recibe la petición y busca cada OID en su “code book” (MIB). Si el OID es encontrado, es ensamblado un paquete de respuesta y enviado con el valor actual del objeto. Si el OID no es encontrado, es enviada una respuesta especial de error que identifica que el objeto no es administrado.

Cuando un elemento envía un paquete TRAP, incluye su OID e información del valor (bindings) para clarificar el evento. Los managers pueden utilizar los “bindings” para correlacionar y manejar los eventos. También generalmente despliegan las etiquetas legibles para facilitar al usuario administrador de red el entendimiento y realización de la decisión a tomar.

Como medida de seguridad se ha implementado password de SNMP el cual tanto los managers como los agentes deben de conocer perteneciendo de esta manera a una misma comunidad y así poder realizar peticiones especificas; existen varios tipos de comunidad entre los cuales se encuentran:

- Comunidad Read Only o "get", que sólo provee acceso para ver las estadísticas y parámetros del sistema.
- La comunidad Read Write o “set”, que permite hacer cambios en los valores de sistema.

Hoy en día la versión más reciente del protocolo SNMP es la 3 la cual cubre aspectos de seguridad, provee mayores capacidades de configuración remota que sus predecesores. El acceso no está limitado a una sola comunidad, es introducido nombres de usuario y contraseñas. Las vistas de los OIDs está basado por usuario. Soporta cifrado de transferencia de datos y también provee detección de errores de transmisión.

El protocolo SNMP provee además los siguientes aspectos de seguridad:

- **User-Based Security Model (USM)**. El cual Provee los servicios de Autenticación y Confidencialidad. Para el servicio de Autenticación implementa los protocolos HMAC-MD5-96 y HMAC-SHA-96. Para el servicio de Confidencialidad implementa el protocolo DES (Data Encryption Standard) en modo CBC (Cipher Block Chaining). USM fue diseñado principalmente para protegerse de las modificaciones de la información, enmascaramiento, modificación de la cadena del mensaje y divulgación; no protege contra ataques de denegación de servicio (DoS) o análisis de tráfico.

- **View-Based Access Control Model (VACM)**. Determina si es permitido el acceso a un objeto administrado en el MIB local del Agente, define la política de control de acceso para el agente; hace posible la configuración remota.

Sin embargo el protocolo SNMP tiene diversas vulnerabilidades de seguridad, por ejemplo la comunidad Read Only es colocado por default con la palabra "public“, lo que ocasiona que cualquier usuario, autorizado o no, puede identificar la información de configuración de los dispositivos (esto es valioso para un posterior ataque informático). La comunidad Read Write es colocado por default con la palabra “private”, lo que también ocasiona que cualquier usuario, autorizado o no, pueda cambiar los valores de configuración, además que la comunidad o contraseña viaja en claro por la red.

Típicamente la mayoría de los ataques, utilizando el protocolo SNMP, están enfocados a denegación de servicio.

- **Herramientas para el fortalecimiento de la seguridad**

El primer intento por proporcionar seguridad a los sistemas surge con la implementación de contraseñas y usuarios, de esta forma, ninguna persona que no sepa la contraseña indicada no podrá ingresar al sistema. Sin embargo esto no significa que no sea posible llevar a cabo el robo de información ya que cualquier persona que posea dicha contraseña podrá ingresar al sistema simulando ser el usuario original.

*SNORT*

Snort es un sniffer de paquetes y un detector de intrusos basado en red, implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.

Permite guardar en un archivo los logs para su posterior análisis de los paquetes capturados. Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se logea. Así se sabe cuándo, de dónde y cómo se produjo el ataque.

Snort tiene una base de datos de ataques que se está actualizando constantemente y a la cual se puede añadir o actualizar a través de Internet. Los usuarios pueden crear 'firmas' basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo de firmas de Snort, para que así todos los usuarios de Snort se puedan beneficiar.

*FIREWALL*

Es un dispositivo o software diseñado para bloquear el acceso no autorizado. El firewall está diseñado para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes host de una red en base a un conjunto de normas y otros criterios. Se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. Funciona a nivel de red (nivel 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino, etc. A menudo en este tipo de firewalls se permiten filtrados según campos de nivel de transporte (nivel 4) como el puerto origen y destino, o a nivel de enlace de datos (nivel 2) como la dirección MAC. Un firewall puede trabajar en los siguientes modos de funcionamiento:

- *Filtro de paquetes*. Se ve en cada paquete que entre o salga de la red y acepta o rechaza basándose en reglas definidas por el usuario. El filtrado de paquetes es bastante eficaz y transparente a los usuarios.

- *Aplicación de pasarela*. Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet.

- *Servidor proxy*. Intercepta todos los mensajes que entran y salen de la red. El servidor proxy oculta de manera eficaz las verdaderas direcciones de red. Trabaja en el nivel de aplicación (nivel 7), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Se pueden realizar filtrados según la URL a la que se desea ingresar.

*FIRMA DIGITAL*

Una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. La firma digital no implica que el mensaje esté encriptado, es decir, que éste no pueda ser leído por otras personas.

El firmante genera mediante una función matemática una huella digital del mensaje. Esta huella digital se encripta con la clave privada del firmante, y el resultado es lo que se denomina firma digital la cual se enviará adjunta al mensaje original. De esta manera el firmante va a estar adjuntando al documento una marca que es única para ese documento y que sólo él es capaz de producir.

El receptor del mensaje podrá comprobar que el mensaje no fue modificado desde su creación y que el firmante es quién dice serlo; en primer término generará la huella digital del mensaje recibido, luego desencriptará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice serlo.

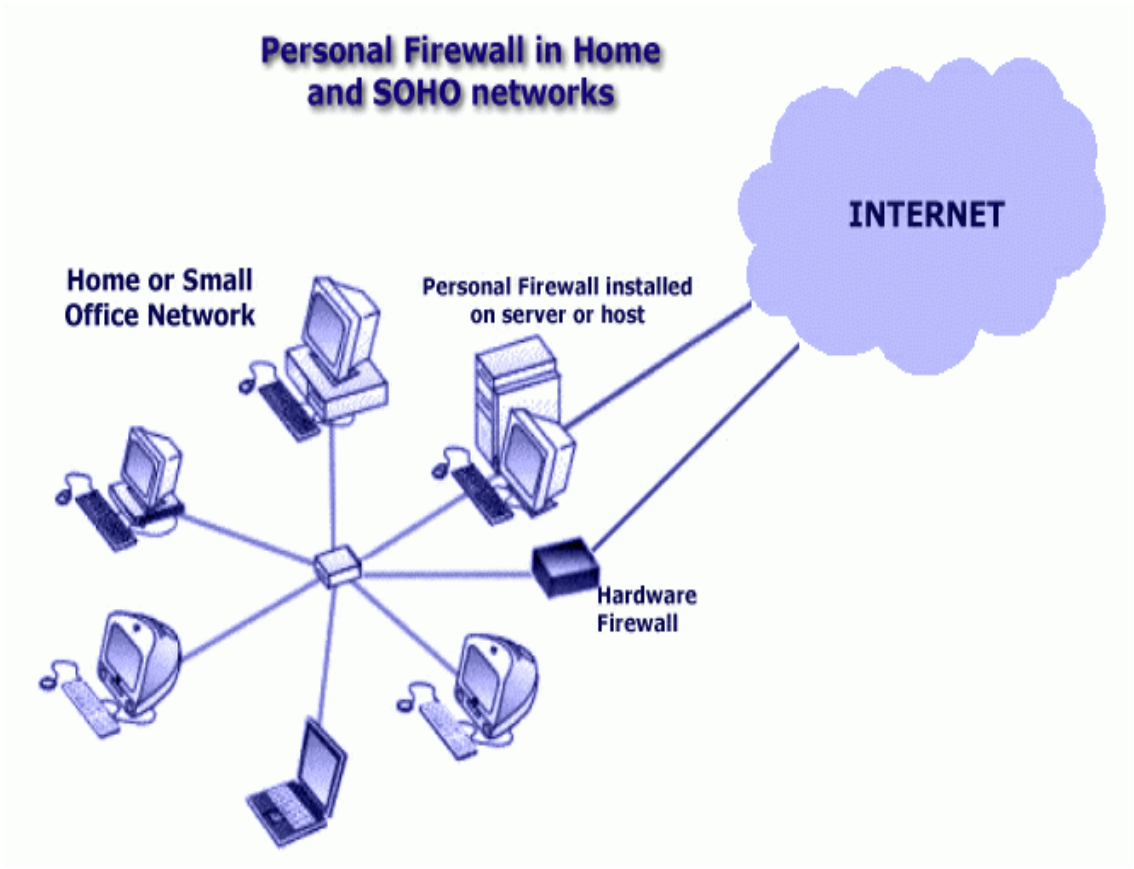



Fig.11.1 Red LAN conectada hacia internet a través de un firewall

*CERTIFICADO DIGITAL*

Un Certificado Digital es el equivalente electrónico a un documento de identidad. El Certificado Digital asocia una clave criptográfica a una identidad, de tal forma que ésta quede fehacientemente ligada a los documentos electrónicos sobre la que se aplica. Un Certificado sirve para: autentificar la identidad del usuario de forma electrónica ante terceros, firmar digitalmente de forma que se garantice la integridad de los datos trasmitidos y su procedencia y cifrar datos para que sólo el destinatario del documento pueda acceder a su contenido. Además que garantiza: la identidad del emisor y del receptor de la información (autentificación de las partes), que el mensaje no ha sido manipulado durante el envío (integridad de la transacción), que sólo el emisor y receptor vean la información (confidencialidad) y que el titular de un mensaje no pueda negar que efectivamente lo firmó.

*SSL(Secure Sockets Layer)*

Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP. Se ubica en la pila OSI entre los niveles de transporte (TCP/IP) y de aplicación (donde se encuentran los protocolos HTTP para Web, FTP para transferencia de ficheros, SMTP para correo electrónico, Telnet para conexión a máquinas remotas, etc.). SSL proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, que puede elegirse entre DES, triple-DES, RC2, RC4 o IDEA, y cifrando la clave de sesión de los algoritmos anteriores mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por

un atacante en una transacción dada, no sirva para descifrar futuras transacciones. MD5 o SHA se pueden usar como algoritmos de resumen digital (hash). Esta posibilidad de elegir entre tan amplia variedad de algoritmos dota a SSL de una gran flexibilidad criptográfica.

Con el protocolo SSL durante la conexión el cliente y el servidor intercambian una serie de mensajes para negociar las mejoras de seguridad.

Como podemos ver son varias las técnicas, procesos y protocolos que se han desarrollado para lograr que los sistemas informáticos sean seguros, sin embargo no podemos decir que exista un sistema 100% seguro, un sistema que se diga que es seguro tendrá que estar aislado de la interacción con el humano y con los demás sistemas ya que es el hombre quien crea los sistemas y él es quien los vuelve inseguros explorando las vulnerabilidades en los procesos y programación de dichos sistemas.

# CAPÍTULO 2

# PROYECTO

## Mejora de la Infraestructura de Telecomunicaciones en Edificio Administrativo de la Universidad Autónoma de la Ciudad de México

- **Planteamiento del problema**

La Universidad Autónoma de la Ciudad de México debido a su crecimiento y expansión ha tenido la necesidad de ampliar su infraestructura informática, ya que cada día son más usuarios los que realizan consultas a diversos programas y servicios que se encuentran instalados en los servidores de la misma universidad.

La UACM cuenta con un edificio administrativo en el cual se encuentran diversas áreas como lo son recursos humanos, finanzas, etc., las cuales realizan de manera continua consultas a bases de datos, aplicaciones y a la página web de la universidad en donde a su vez se tiene acceso a otras aplicaciones como listados de alumnos, consulta de historiales académicos, horarios, etc.

Actualmente la interconexión entre sus equipos de computo se realiza por medio de switchs de red de capa 2, los cuales se encuentran instalados en el site principal (MDF) y en dos IDFS, proporcionando servicio de red a 353 nodos activos entre impresoras, PC y servidores. Los switch no son administrables, la velocidad por puerto no es mayor a los 100 Mbps, provocando que existan problemas de congestionamiento, lo que trae como consecuencia que el envío de archivos entre computadoras así como las consultas a base de datos y aplicaciones de los servidores internos de la universidad sea lenta, aún cuando las interfaces que red de cada unas de las PC soportan una velocidad de 1 Gbps. Otros de los problemas que existen es la perdida de paquetes que se ve reflejada a través del comando ping que se hace entre las maquinas de la red local.

Debido al limitado ancho de banda que existe en las interfaces de los switch no es posible realizar más de 8 consultas simultaneas a los programas que se encuentran corriendo en los servidores, siendo esto un número muy reducido, ya que por ejemplo en el área de finanzas se requiere que tengan acceso al sistema 19 personas lo cual rebasa la capacidad del equipo actualmente instalado.

El equipo de red con el que cuenta la universidad no permite algún tipo de segmentación, por lo que todos los host comparten un mismo dominio. Sólo se tiene un segmento y una sola clase de direccionamiento IP en la red interna, lo cual ha provocado un problema de administración para el personal de sistemas, ya que no se logra identificar con base a la dirección IP el lugar en donde se encuentra localizada alguna computadora, esto debido a que en la asignación de direcciones IP no se siguió algún tipo de norma o diferenciación de IP con respecto a las diferentes áreas, así mismo la secuencia de estas direcciones se realizo conforme se habilitaban computadoras nuevas quedando regadas dichas direcciones en todo el edificio.

Debido a la problemática que se ha planteado anteriormente es necesario hacer un cambio en la infraestructura de equipos de red (switch) por un nuevo equipo que permita mejorar los servicios de ésta.

- **Objetivo**

La siguiente propuesta de cambio de equipo de red tiene como objetivo hacer una mejora en la red de la UACM que permita obtener un aumento en la velocidad en transferencia de archivos entre computadoras, aumento en la velocidad de las consultas a sus bases de datos y a servidores internos. Así mismo lograr una disminución de paquetes perdidos.

- **Audiencia**

La siguiente propuesta va dirigida hacia el personal que se encuentran en el área de sistemas como lo son el administrador de red, de soporte técnico y de comunicaciones, ya que es necesario tener un conocimiento técnico del funcionamiento de los diversos componentes de una red de datos, así como los protocolos y normas existentes en las redes Ethernet. Será el personal de sistemas el que determinará el tipo de direccionamiento que se configurará en la red interna.

Con el cambio de switch que se propone resultarían beneficiados el personal de sistemas ya que se lograría tener una mejor administración de la red, teniendo un control del direccionamiento IP, asignación de direcciones, recursos compartidos como lo son impresoras o carpetas, maquinas conectadas a la red, usuarios y privilegios que éstos pueden tener, lo cual conduce a su vez a prestar un mejor servicio que beneficiará a las personas de las diferentes áreas administrativas que actualmente hacen uso de los servicios de la red.

- **Ingeniería y diseño detallado**

*Ingeniería de tráfico*

En los sistemas de telecomunicaciones, tráfico es un término que se utiliza para referirse al flujo de información a través de la red. El hecho de que exista tráfico implica necesariamente uso de los recursos de la red.

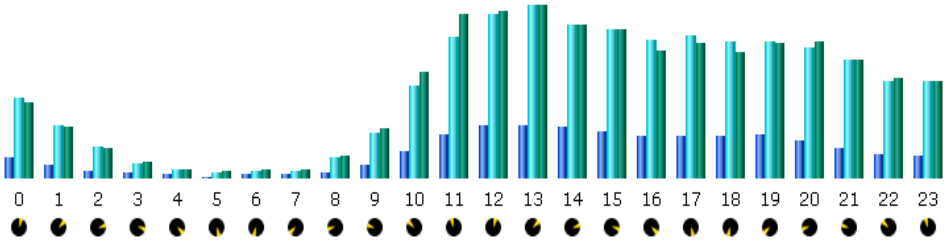
La teoría de tráfico es la descripción matemática del flujo de información en una red de telecomunicaciones. La ingeniería de tráfico es la ciencia que apoya el diseño de redes de telecomunicaciones de manera que cumplan con los requerimientos de calidad de servicio de los usuarios.

Se decidió tomar como base para realizar un análisis de la carga de trafico que existe en la red interna las consultas que se realizan al servidor web con el que cuenta la institución, esto debido a que desde ahí es posible ingresar a diversas aplicaciones particulares de las áreas como los son, listados, consultas de nóminas, base de datos del personal, información de los alumnos, etc. Por lo cual es un referente importante para diagnosticar el tráfico que a diario se encuentra en la red.

Los datos de las consultas que a diario se hacen al sistema han sido tomados de una aplicación llamada Awstats que se encuentran instalada en el mismo, estos datos fueron tomados en diciembre del año 2008, en la cual se ilustran las consultas realizadas durante ese mes; tomaremos en consideración el tráfico generado durante la hora con más afluencia de visitantes, con base a la grafica observamos que en la hora pico se generan 3.52 GB. de tráfico.

3.52 GB = 28835.84 Mb = 28.16 Gb

Visitas por Horas




| Visitas por Horas | Páginas | Solicitudes | Tráfico | Visitas por Horas | Páginas | Solicitudes | Tráfico |
|---|---|---|---|---|---|---|---|
| 00 | 14327 | 56038 | 1.53 GB | 12 | 37217 | 115531 | 3.43 GB |
| 01 | 9326 | 37176 | 1.03 GB | 13 | 37370 | 121326 | 3.52 GB |
| 02 | 5353 | 21572 | 634.22 MB | 14 | 35267 | 108176 | 3.15 GB |
| 03 | 2841 | 9943 | 348.08 MB | 15 | 32491 | 104517 | 3.03 GB |
| 04 | 1740 | 6188 | 198.46 MB | 16 | 28708 | 98168 | 2.60 GB |
| 05 | 1325 | 3763 | 124.07 MB | 17 | 29627 | 100570 | 2.77 GB |
| 06 | 1349 | 4357 | 199.36 MB | 18 | 29629 | 96658 | 2.57 GB |
| 07 | 1618 | 5213 | 172.84 MB | 19 | 29668 | 96833 | 2.78 GB |
| 08 | 3815 | 14518 | 457.61 MB | 20 | 26149 | 91919 | 2.78 GB |
| 09 | 8280 | 31287 | 1023.47 MB | 21 | 20794 | 82714 | 2.42 GB |
| 10 | 18395 | 64853 | 2.16 GB | 22 | 17136 | 68591 | 2.06 GB |
| 11 | 30861 | 98518 | 3.33 GB | 23 | 15813 | 68044 | 1.99 GB |

Por lo que por cada hora tenemos un tráfico o tasa de arribo de eventos (λ) de:

$$\lambda = 28.16 \text{ Gb tráfico/hora}$$

Según los datos arrojados en la siguiente tabla el promedio de tiempo que los usuarios hacen consultas a la página es de 354s. es decir 5.9 minutos.

Duración de las visitas

| Número de visitas: 40377 - Media: 354 s | Número de visitas | Porcentaje |
|---|---|---|
| 0s-30s | 25533 | 63.2 % |
| 30s-2mn | 3201 | 7.9 % |
| 2mn-5mn | 3003 | 7.4 % |
| 5mn-15mn | 3927 | 9.7 % |
| 15mn-30mn | 2141 | 5.3 % |
| 30mn-1h | 1614 | 3.9 % |
| 1h+ | 958 | 2.3 % |

Por lo que la duración promedio del evento (tm) o tiempo promedio de ocupación es de:

$$tm = 5.9 \text{ minutos/evento}$$
$$tm = 5.9 \text{ minutos/evento}) / (60 \text{ minutos/hora})$$
$$tm = 0.0983 \text{ horas/evento}$$

Con base a lo anterior la intensidad de tráfico (A) actual será de:

$$A = \lambda * tm = (28.16 \text{ trafico/hora}) \times (.0983 \text{ horas/evento})$$
$$A = 2.76 \text{ E (Erlang}^{1}\text{)}$$

Por otra parte se sabe que la aplicación a la cual ingresan de manera recurrente varios usuarios a la vez desde el servidor web requiere de un total de 1.7 MB para su consulta lo que equivale a 13.6 Mb por lo que tan sólo se permiten 8 conexiones simultaneas en la infraestructura actual de un ancho de banda de 100 Mb, aún teniendo en el servidor interfaces de red de 1 Gb. A esta aplicación en particular se requiere que tengan acceso un total de 20 personas del área de finanzas, lo que quiere decir que sólo un 40% puede ingresar a la aplicación al mismo tiempo; se desea que por lo menos 19 de ellas puedan hacer uso del sistema, es decir que el 95 % puedan estar haciendo uso de la aplicación de manera simultánea.

En este caso el número de usuarios que hacen uso del sistema actualmente es de 8 por lo que N=8 y P=60%. P es el grado de servicio que este caso es el porcentaje de usuarios que no pueden ingresar al sistema.

Para lograr el propósito de que el 95% de los usuarios puedan consultar la aplicación al mismo tiempo se debe modificar el valor de P con los usuarios que ingresarán al sistema por lo que:

$$P = 95\ \% = 0.95$$

Con base a la tabla de Erlang B tenemos que:

Para

$$P = 0.95 \qquad N = 8$$

Por lo que:

$$8 \times 13.6 = 108.8 \text{ Mb}$$

Por lo que se necesitan 109 Mb adicionales de ancho de banda en los puertos del switch a los 100 Mb que brinda actualmente para lograr que 19 personas puedan ingresar al sistema de manera simultánea.

Por lo anterior se concluye que con la infraestructura actual no permite dicho número de conexiones y es necesario aumentar el ancho de banda para lograr este número de conexiones y más.

- **Enfoque**

La presente propuesta ofrece una solución técnica al problema descrito anteriormente, para tal motivo se propone un equipo de red moderno que cubra las necesidades que actualmente tiene la universidad en su infraestructura de red.

El aspecto principal que se ha tomado en cuenta para la propuesta de instalación de Core Switch ha sido en gran medida el técnico ya que el modelo y marca que se proponen cubren de manera importante la problemática que se encuentra en la red actualmente instalada en la universidad; sin embargo el aspecto financiero aunque no es el principal eje que se sigue para proponer este Core Switch no se ha dejado de lado ya que el Core Switch y switch de la marca que se propone instalar no son de elevado costo, ofreciendo las mismas funcionalidades de otros equipos como lo pueden ser Cisco.

[1] Erlang es una unidad de medida de intensidad de tráfico

- **Alcance**.

La presente propuesta de mejora de la infraestructura de red de la universidad contempla la instalación de un Core Switch así como de 6 Switch multicapa, su configuración, programación y puesta en marcha de los mismos. Se programarán la creación de segmentos de red (vlans), direccionamiento ip de las mismas y la programación de rutas estáticas.

El área de sistemas tendrá que brindar las facilidades necesarias para la instalación del Core Switch y de los switch; facilidades como lo son espacio en racks, la instalación de tierras físicas, remate a panel de la fibra óptica, conexión de corriente regulada para los equipos y conexión a UPS. Así mismo deberá proporcionar para la conexión de fibra a panel los "jumpers" necesarios dependiendo del nivel de redundancia que se desea tener. En esta propuesta no se contempla ningún tipo de instalación de cableado extra para ampliar la red.

Se brindará un mantenimiento preventivo por 2 años al equipo instalado, así mismo se garantiza una reconfiguración o cambios en la programación de los equipos por el mismo periodo de tiempo.

Con lo que respecta a la garantía del equipo ésta no será válida si el daño o falla ha sido causada por descarga eléctrica o por mal aterrizaje a tierra de los equipos, o por sobrecalentamiento debido a la falta de aire acondicionado.

En la instalación así como la programación del equipo no se prevé ninguna configuración para VoIP.

- **Conceptualización y modelado**.

El proyecto se enfoca al cambio de equipo de red (switch) ofreciéndole un equipo de red moderno con posibilidad de crecimiento. Se propone que por medio de este equipo se pueda segmentar la red existente en por lo menos un segmento por área ya que de esta manera se tendrían por cada segmento no más de 50 equipos los cuales no generan grandes cantidades de tráfico y por consiguiente congestionamiento; este tráfico sólo sería visible entre los host conectados en ese segmento de red. La segmentación se llevaría a cabo por medio de la creación de vlans en los diferentes switch. El direccionamiento para el segmento de red que se utilizaría en las vlans el área de sistemas lo debe proporcionar así como mascaras y gateways.

Como ya se ha mencionado el edificio consta de diez pisos no incluyendo la planta baja en la cual se encuentra el MDF que es donde se instalará un switch principal llamado Core Switch el cual será el encargado de administrar todos los segmentos de red creados además de permitir la interfaz entre la LAN y la WAN o algún servidor proxy, NAT, firewall, etc.

El Core Switch proporcionaría el servicio de red a los pisos 1, 2 y 3 del edificio e inclusive a planta baja debido a que la infraestructura del cableado actual así lo permite. Para tal propósito será necesario que el Core Switch cuente con 3 tarjetas de puertos de cobre, cada uno con 48 puertos debido a que actualmente se brindan un total de 101 servicios de red en este MDF, quedando 43 puertos libres para la habilitación futura de servicios. Así mismo se instalarán dos tarjetas de procesamiento MSM para poder brindar redundancia en CPU del Core Switch. Estas tarjetas a su vez cuentan con los puertos SFP que permitirían la conexión de la fibra óptica, por lo cual será necesario contar con 4 minigibics SX, ya que se ha expresado que se desea redundancia entre las interfaces de interconexión de los switch.

Se contempla una programación en el Core Switch de 16 vlans, 13 de los diferentes áreas que se encuentran en el edificio, una para servidores internos, una para la interfaz hacia la WAN y una más de administración.

En el Core Switch como se ha mencionado se programaran las siguientes 4 vlans: certificación, recursos humanos, servicios generales, recursos materiales, servidores y WAN, las cuales tendrán puertos de cobre activos; las restantes 9 vlans, serán creadas, sin embargo éstas no tendrán puertos de cobre asociados tan sólo estarán dadas de alta en el puerto de fibra respectivo que permita que éstas sean accesibles desde el IDF en el cual den servicio.

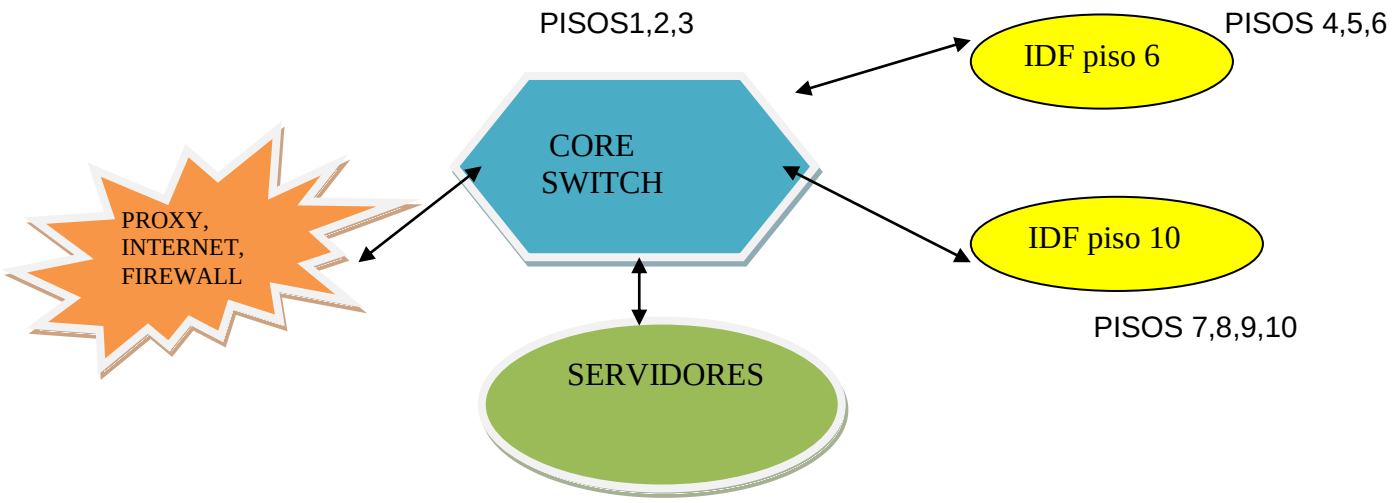
La conexión entre el Core Switch y los IDF se realizará por medio de fibra óptica por lo cual ya se deberá de contar con el tendido de la misma en el backbone para dicho fin.

Por lo que respecta a los IDF se propone instalar 3 switch de 48 puertos en cada uno, tanto en el IDF del piso 6 como en el IDF del piso 10 del edificio. Estos switch se colocarían en "stack" que es la tecnología de interconexión de estos switch; el stack del piso 6 daría servicio de red a los pisos 4, 5 y 6 y se conectaría como ya se mencionó al MDF por medio del tendido de fibra óptica. En estos pisos se encuentran 5 áreas administrativas por lo cual se contempla que en el switch 1 del stack le fueran programado 2 vlans, que darían servicio al área de finanzas y sistemas que en conjunto no rebasan más de 48 nodos activos siendo un total de 38. El switch 2 daría servicio al piso 5 programando de igual forma 2 vlans para dos áreas que se encuentran ahí, con un total de 40 nodos activos. En el tercer switch se programaría sólo una vlan que daría servicio a una área que se encuentra en el piso 6. Para la instalación de este stack se debe contemplar la compra 3 cables de estaqueo así como los "jumpers" de fibra y 2 minigibics SX.

El stack del piso 10 proporcionaría servicio de red a los pisos 7, 8 ,9 y 10, se programaría una vlan para cada piso, debido a que en cada uno de estos pisos sólo existe un área. Cada switch atenderá un segmento de red es decir un piso, debido a que en el piso 10 no se encuentran muchas máquinas conectadas el switch número 3 del stack sería programado con dos segmentos, el segmento del piso 9 que sólo tiene conectadas 26 maquinas y el antes mencionado piso 10 con sólo 12 maquinas conectadas. Al igual que el IDF de piso 6 se debe de contar con los cables de estaqueo y "jumpers" de fibra para la conexión hacia el panel, así como 2 minigibics para la conexión de fibra.

Para el acceso a la administración de los equipos antes mencionados se dejará configurado con el protocolo SSH v2, que es un módulo extra que será cargado en los equipos que se instalarán en la red, de esta manera se brindara seguridad en el acceso a la administración del equipo. El acceso vía Telnet será deshabilitado para dicho fin.

Diagrama esquemático de la interconexión de la red



- **Descripción de interfaces y subsistemas**

El Core Switch que se propone es el Black Diamond 8810 de marca Extreme con un chasis de 10 slots; que contaría con 3 tarjetas de 48 puertos Ethernet 10-100-1000 BASE-T RJ45, con funcionalidades de PoE, de esta manera se podría dar servicio a un total de 144 maquinas.

Será necesario contar con una tarjeta extra tipo MSM G8X ya que ésta permitirá la redundancia en CPU del Core Switch, estas tarjetas cuentan con 8 puertos SFP, para las conexiones de fibra óptica es necesario considerar la instalación de interfaces de fibra minigibics. Se colocan 2 tarjetas adicionales debido a que se desea redundancia entre sus conexiones de backbone por lo cual se deben considerar la instalación de un total de 4 minigibics dos para la fibra que va hacia el IDF de piso 6 y dos más hacia el piso 10.

Este Core Switch son non-blocking en todos sus puertos, por lo que se garantiza una alta disponibilidad en cada uno de ellos. Cuenta con una amplia gama de funcionalidades en la capa 2 a 4 que son totalmente compatibles con IPv4 e IPv6.

Cada uno de los procesos del core se ejecuta de manera independiente al sistema operativo, por lo que aumenta la integridad del sistema protegiéndolo de ataques como lo son la negación de servicio (DOS). Es un sistema en el cual cada proceso puede ser reiniciado de manera independiente uno del otro sin que esto signifique parar el sistema; permite además que diferentes tipos de módulos puedan ser agregados de manera independiente. Cuenta con el Ethernet Automatic Protection Switching (EAPS) que ofrece un tiempo de recuperación mucho menor que STP y rapid STP de unos 50 milisegundos en todos sus puertos. El BlackDiamond soporta Spanning Tree (802.1D), VLAN Spanning Tree (PVST+), Rapid Spanning Tree (802.1w) y Multiple Instances de Spanning Tree (802.1s). Cuenta con la funcionalidad de Link Agregation que es una funcionalidad que permite la agregación en una sola línea lógica de hasta 8 puertos físicos logrando con esto tener hasta 80 Gbps de ancho de banda. Como ya se ha mencionado es un equipo el cual ya está diseñado para la convergencia hacia VoIP.

Con lo que respecta a los equipos que se instalaran en lo IDF se proponen los switch Summit X450e de 48 puertos el cual utiliza la misma tecnología de hardware non-blocking, de alto rendimiento, que es el mismo utilizado en los BlackDiamond 8800. Brinda gigabit de alta densidad más 10 puertos Gigabit Ethernet en formato compacto 1RU, que admiten una amplia gama de funcionalidades de Capa 2 a Capa 4 en cada puerto. Se proveen fuentes de alimentación redundantes opcionales con cada switch para contar con protección contra descargas eléctricas. Admite la recuperación de procesos y mejoras en las aplicaciones sin la necesidad de reiniciar el sistema.

El switch brinda funcionalidades de calidad de servicio (QoS) y capacidades de administración de tráfico, el tiempo de latencia es minimizada.

Es un switch Gigabit Ethernet con Interfaces 10/100/1000BASE-T de 48 puertos más 4 puertos SFP; tiene una fuente de alimentación interna de CA y CC y ofrece la opción para una fuente de alimentación redundante externa de CA y CC. Con 10 Gigabit Ethernet doble opcional. Proporciona una agregación de alto rendimiento para las aplicaciones de red empresarial, HPCC y Ethernet de portadora. Ofrece conmutación de Capa 2/Capa 3 a velocidad de red alámbrica para todos los puertos con prestaciones de calidad de servicio (QoS) y seguridad, como listas de control de acceso (ACL) basadas en hardware.

Este tipo de switch ofrece doble apilado para proporcionar interfaces de alta velocidad de 40 Gbps de ancho de banda de apilamiento. Los stack están diseñados para apoyar la convergencia de servicios tales como VoIP y vídeo por su alta disponibilidad, se pueden apilar hasta ocho unidades.

Al igual que el core switch cada uno de los proceso que maneja el Summit es independiente por lo cual se pueden reiniciar en cualquier momento sin que el sistema se pare.

Cuenta con la funcionalidad de Link Aggregation (802.3ad) que permite la conexión física de hasta ocho enlaces en una sola conexión lógica, de hasta 20 gigabits por segundo (Gbps) de ancho de banda con conexión redundante.
Al igual que el Core Switch cuenta con capacidades avanzadas de enrutamiento proporcionando enrutamiento estático RIP, OSPF y el BGP con la licencia extra se obtienen características como los son:

• Completo OSPF de una mayor extensibilidad
• BGP interinstitucional
• Transmisión con IPv6 de hardware OSPFv3
• Túneles IPv6, IPv6 a IPv4 traducción, e IPv6 multicast

- **Cálculo de disponibilidad**

Se pretende que el equipo que se desea adquirir pueda contar con el estándar de disponibilidad, es decir con 99.999 % de disponibilidad, con base a datos obtenidos en diversas páginas de internet acerca de los productos que se proponen instalar tenemos lo siguiente:

MTBF del Summit X450a es de 141,005 horas

Los switch como tal cuentan con un único MTBF ya que es considerado como un solo sistema, por lo que lo podremos considerar como tal. En el presente proyecto los swtich y la falla que puedan experimentar éstos no perjudicarán en nada al funcionamiento del Core Switch así como del stack instalados en los IDF.

En caso de presentar alguna falla el equipo, éste sería detectado en un tiempo no mayor a media hora, el tiempo que se tomaría para verificar el tipo de falla sería de media hora; en caso de que la falla requiera de algún cambio de componentes o tarjetas o inclusive el cambio del equipo éste tardaría 24 horas en llegar a sitio debido a que se tendrían que importar dichas piezas. Teniendo las refacciones el tiempo de cambio y en su caso de programación debe de ser de un máximo de 45 minutos.

MTBF = 141,005 horas;
MTTR = 0.5 +.5 + 24+45 = 25.45 horas
D = MTBF / (MTBF + MTTR) = 141,005 / (141,005 + 25.45) = 99.981 %

Si el cliente deseará aumentar el porcentaje de disponibilidad se deberá considerar un aumento en el presupuesto debido a que el tiempo de traslado de refacciones se puede minimizar con un tiempo de respuesta de 6 horas.

Por lo que respecta al Core Switch éste es considerado como un sistema en el cual intervienen principalmente el número y tipo de tarjetas instaladas, en el caso del presente proyecto se tiene que tomar en cuenta la tarjeta de procesamiento central MSM y el número de fuentes instaladas. Consultando en la página del fabricante se tiene que éste ofrece un MTBF para la tarjeta MSM de 124768 horas y garantiza un MTBF de 166408 horas si se tienen instaladas en el Core Switch 6 fuentes de poder.

Al igual que con los switch Summit los tiempos de detección de fallas así como de reparación de las mismas son iguales, es decir media hora para detectar la falla, se tomaría igualmente media hora para verificar el tipo de falla, 24 horas en caso de requerir cambio de alguna refacción y 45 minutos para la sustitución de las mismas.

De esta manera se tienen los siguientes cálculos:

Para la tarjeta MSM

MTFB = 124678 horas
MTTR = 0.5 +.5 + 24+45 = 25.45 horas
D = MTBF / (MTBF + MTTR) = 124678 / (124678 + 25.45) = 99.97 %

Para las fuentes de poder

MTFB = 166408 horas
MTTR = 0.5 +.5 + 24+45 = 25.45 horas
D = MTBF / (MTBF + MTTR) = 166408 / (166408 + 25.45) = 99.98 %

Tomando en cuenta que se trata de un sistema en serie tenemos que la disponibilidad total es:

D = .9997 * .9998 = 99.95 % Total del sistema

Al igual que como en el caso del Summit si se deseara tener un nivel de disponibilidad mayor habría un aumento en el presupuesto debido a que el tiempo de traslado de las refacciones sería minimizado.

- **Pruebas, certificación y aceptación.**

Después de terminada la instalación de los diferentes stack se tomaría en periodo de prueba de 1 mes en el cual se realizarían modificaciones a la programación de los mismos, creación de nuevas rutas, nuevas vlans o cambio de direccionamiento. Durante este periodo se monitorearían el estado de los switchs es decir que éstos no presenten fallas a nivel de software y hardware, de ser así se procedería al cambio total del equipo. Así mismo durante este periodo de tiempo se llevaría a cabo la habilitación de nodos si así se requiere con configuraciones especiales como lo es MAC-LOCK o limit learning para que se determine que configuración cubre sus necesidades y así poder brindar un control más efectivo de las máquinas que se conectarían a la red.

El tiempo de transferencia de un archivo de una maquina a otra debe disminuir, se propone que se hagan pruebas entre diferentes equipos localizados en diferentes vlans para determinar el tiempo en el cual se lleva a cabo la transferencia de los archivos; así mismo se habrá de notar una mayor rapidez al momento de mandar a imprimir cualquier documento de cualquier número de páginas en las impresoras localizadas en red.

Se propone que el área de sistemas realice mediciones de pérdida de paquetes por medio del comando ping en el cual se mostraría el tiempo que tarda de llegar los paquetes hacia la máquina, el promedio de tiempo es de 5 ms. con un tamaño de paquetes de 32 bits.

Se realizarán pruebas de redundancia entre la interconexión de los switch, estas pruebas consistirían en deshabilitar alguna de las dos fibras que alimenta a cada uno de los IDF por lo que no debería haber en ningún momento perdida de servicio de red interna y hacia internet, de esta manera comprobaríamos que la configuración haya sido programada de manera adecuada; se podría dejar un ping de manera permanente entre dos máquinas que estén localizadas en diversas vlan´s y notar que no haya en ningún momento perdida de paquetes, tal vez si un aumento de tiempo pero que no podrá ser mayor a los 15 ms.

Con respecto a la consulta de base de datos, los usuarios tendrán que realizar diversas pruebas de consulta, éstas tendrán que tener un tiempo de respuesta menor que el registrado antes de la realización del presente proyecto siempre y cuando la aplicación así como el servidor cumplan con

los requerimientos para dicho fin, de igual manera el número de usuarios debe aumentar y el tiempo que se tarda el servicio en hacer la consulta debe ser el mismo.

Se propone también la colocación de un sniffer en la red interna para verificar el tráfico saliente de cada subred y comprobar que sólo salgan peticiones a internet y servidores internos y que en ningún momento las solicitudes sean entre equipos de una misma vlan o alguna otra vlan.

Con lo que respecta a la compartición de carpetas, todas las peticiones que los usuarios hagan se deben de realizar sólo desde el segmento de red en el cual se encuentran las máquinas que comparten dicho recurso no deben existir conexiones a dichas carpetas desde otras vlans siempre y cuando se establezcan los permisos adecuados para dicho fin.

Se propone así mismo realizar transmisiones de video entre las diversas maquinas de los diferentes pisos con una calidad de video aceptable, por lo que no debe de haber en ningún momento retraso en la señal ni pausas.

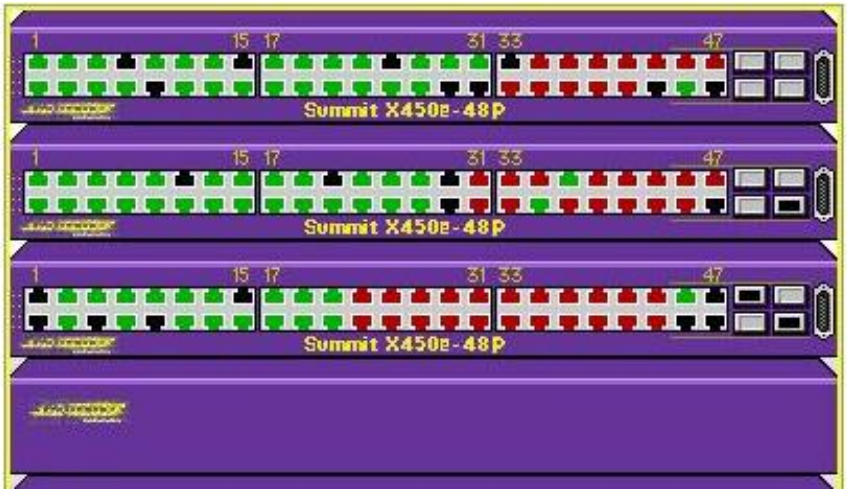
Éstas son la pruebas que se proponen para determinar que el cambio de infraestructura de la red ha cumplido con los establecido en los objetivos del mismo, sin embargo el cliente podrá realizar otro tipo de pruebas siempre y cuando la falla en alguna de ellas sea atribuible al equipo de red instalado.

- **Evaluación y aceptación**

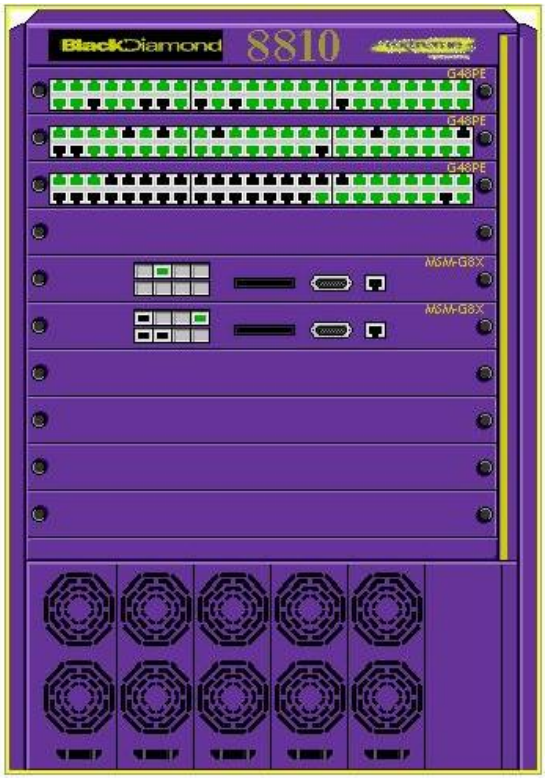
Habiendo realizado las pruebas anteriores y las propias del cliente en las cuales se demuestre que hay una disminución de paquetes perdidos, aumento de velocidad en transferencia de archivos, aumento en la velocidad de las consultas a sus bases de datos y a servidores internos; se entregarán todas las pantallas de pings, se preguntará a los usuarios de la red si están satisfechos con el cambio y como es que notan la velocidad de consultas.

El personal de sistemas será el encargado de determinar si se ha cumplido con lo establecido, estando satisfecho del resultado de todas ellas se procederá hacer la entrega de las memorias técnicas de todos los equipos así como de archivos de configuraciones y respaldos de los mismos. Con lo cual se dará por terminado la etapa de instalación y puesta en marcha de los equipos pasando de esta manera a la etapa de mantenimiento preventivo por 2 años.

Esquema de instalación en stack de los switch de los IDF



Esquema de la instalación del core switch en el MDF



# Conclusiones

Por medio de los conocimientos adquiridos durante el diplomado Integral en Telecomunicaciones fue posible hacer una propuesta de instalación de un Core Switch en la Universidad Autónoma de la Ciudad de México. Dicha propuesta se pudo llevar a cabo en la realidad por lo que se logro instalar dicho equipo en la universidad y cubrir de manera exitosa los requerimientos para su instalación; así mismo la realización de la propuesta aunque no se contemplaba ninguna otra instalación de tipo VoIP permitió dar el primer paso para la migración de telefonía convencional a telefonía IP.

Gracias a este diplomado pude ampliar mis conocimientos en el área de las telecomunicaciones, me actualicé de información acerca de las nuevas tecnologías existentes en la redes de voz y datos; a nivel laboral me fue de gran ayuda ya que al mismo tiempo que tomaba el diplomado se decidió hacer la migración de telefonía convencional a telefonía IP en mi centro de trabajo; por lo que tuve la oportunidad de asentar en la práctica todas las bases teóricas aprendidas en el diplomado, especialmente en los módulos de telefonía, voz IP, y microondas. Así puede participar de manera activa en la instalación de esta tecnología entendiendo cada unos de los procesos que se llevaron a cabo en la misma.

En términos generales el diplomado es muy bueno, sin embargo considero que su costo es un poco elevado y no se cubre en algunos módulos de manera integra el conocimiento que se dice se va adquirir.