**Universidad de San Carlos de Guatemala**
**Facultad de Ingeniería**
**Escuela de Ingeniería en Ciencias y Sistemas**

# FUNDAMENTOS PARA TRANSMITIR DATOS DE UNA RED TELEFÓNICA HACIA UNA RED DE DATOS EN FORMA SEGURA

**EDDY WILFREDO GUARÁN BAEZA**

**ASESORADO POR: ING. PEDRO DAVID TZOC Y TZOC**

**GUATEMALA, AGOSTO DE 2005**

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA


FACULTAD DE INGENIERÍA

# FUNDAMENTOS PARA TRANSMITIR DATOS DE UNA RED TELEFÓNICA HACIA UNA RED DE DATOS EN FORMA SEGURA

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

**EDDY WILFREDO GUARÁN BAEZA**
ASESORADO POR: ING. PEDRO DAVID TZOC Y TZOC

AL CONFERÍRSELE EL TÍTULO DE
**INGENIERO EN CIENCIAS Y SISTEMAS**

GUATEMALA, AGOSTO DE 2005

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA


## NÓMINA DE JUNTA DIRECTIVA

| | |
|---|---|
| DECANO | Ing. Murphy Olympo Paiz Recinos |
| VOCAL I | Vacante |
| VOCAL II | Lic. Amahán Sánchez Álvarez |
| VOCAL III | Ing. Julio David Galicia Celada |
| VOCAL IV | Br. Kenneth Issur Estrada Ruiz |
| VOCAL V | Br. Elisa Yazminda Vides Leiva |
| SECRETARIO | Ing. Marcia Ivonne Véliz Vargas |

## TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

| | |
|---|---|
| DECANO | Ing. Sydney Alexander Samuels Milson |
| EXAMINADOR | Ing. Ricardo Morales |
| EXAMINADOR | Ing. Virginia Tala Ayerdi |
| EXAMINADOR | Ing. Edgar Santos |
| SECRETARIO | Ing. Pedro Antonio Aguilar Polanco |

**HONORABLE TRIBUNAL EXAMINADOR**

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

# FUNDAMENTOS PARA TRANSMITIR DATOS DE UNA RED TELEFÓNICA HACIA UNA RED DE DATOS EN FORMA SEGURA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha julio de 2004.

Eddy Wilfredo Guarán Baeza

# DEDICATORIA

**A Dios**

A ti Padre Santo por darme el don de la vida y ser mí guía en todo momento, te dedico este logro.

**A mis padres**

Isabel Guarán y Aura Floridalma por todo el esfuerzo, comprensión, amor y dedicación que me han brindado y por los valores y principios que me inculcaron con su ejemplo,  a ustedes en especial les dedico este triunfo.

**A mis hermanos**

Luis Adolfo, Mario Javier, Mynor Estuardo y Rita Mariela por la amistad y el apoyo que siempre me han dado.

**A mis abuelos**

Por todo el amor y consejos que me han regalado.

Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala 2 de agosto de 2005

**Ingeniero Carlos Azurdia**
**Coordinador del Área de Trabajos de Graduación**
**Escuela de Ciencias y Sistemas**

Respetable Ingeniero Azurdia:

De manera cordial me permito saludarle y a la vez manifestarle mi apoyo sobre el trabajo de graduación que fue desarrollado por el estudiante Eddy Wilfredo Guarán Baeza, en el tema de Fundamentos para transmitir datos de una red telefónica hacia una red de datos en forma segura.

Manifiesto que tuve a la vista el trabajo de graduación antes mencionado y considero que cumple con los requisitos requeridos por la Facultad de Ingeniería, por lo cual apoyo el mismo.

Sin otro particular por el momento

Atentamente,

Ing. Pedro David Tzoc y Tzoc
Colegiado 6220

Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala 17 de febrero de 2005

**Ingeniero**
**Luis Alberto Vettorazzi España**
**Coordinador de la Carrera de Ingeniería en**
**Ciencias y Sistemas**

Respetable Ingeniero Vettorazzi:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **EDDY WILFREDO GUARÁN BAEZA**, titulado: "**FUNDAMENTOS PARA TRANSMITIR DATOS DE UNA RED TELEFÓNICA HACIA UNA RED DE DATOS EN FORMA SEGURA"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme.

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados y
Revisor


El coordinador de la carrera de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, al trabajo de graduación titulado: Fundamentos para transmitir datos de una red telefónica hacia una red de datos en forma segura, presentado por el estudiante universitario Eddy Wilfredo Guarán Baeza, aprueba el presente trabajo y solicita la autorización del mismo.

Ing. Luis Alberto Vettorazzi España
Coordinador
Ingeniería en Ciencias y Sistemas

Guatemala, febrero de 2005

# ÍNDICE GENERAL


Página

**ÍNDICE DE ILUSTRACIONES** IX

**GLOSARIO** XI

**RESUMEN** XVII

**OBJETIVOS** XX

**INTRODUCCIÓN** XXI

**1. FUNDAMENTOS DE LA COMUNICACIÓN** 1

1.1. Concepto de comunicación 1

1.2. Elementos de la comunicación 1

1.3. Comunicación digital 2

1.4. Elementos en la comunicación digital 2

1.5. Telecomunicación 3

**2. TRANSMISIÓN DE INFORMACIÓN** 5

2.1. Características de la transmisión de datos 5

2.1.1. DTE 5

2.1.2. DCE 5

2.1.3. Formas de comunicación 5

2.2. Transmisión de datos entre redes de datos 6

2.2.1. Formas de transmisión 6

2.2.2. Tipos de conexiones 9

2.3. Transmisión de datos entre redes telefónicas 10

2.3.1. Comunicación celular 10

2.3.1.1. Definición y principios de la comunicación móvil 11

2.3.1.2. Componentes de un sistema celular 12

2.3.1.3. Estructura de un sistema celular 13

2.3.2. Tipos de redes telefónicas 15

2.3.2.1. Redes conmutadas 15

2.3.2.2. Redes de difusión 16

2.3.3. Formas de acceso 17

2.3.3.1. FDMA 17

2.3.3.2. TDMA 17

2.3.3.3. CDMA 18

2.3.3.4. GSM 19

**3. REDES FÍSICAS Y REDES LÓGICAS** 23

3.1. Redes de datos 23

3.1.1. Elementos de una red de datos 23

3.1.2. Cableado estructurado 25

3.1.3. Repetidores 26

3.2. Niveles lógicos en las redes de datos 26

3.2.1. Modelo de referencia OSI 27

3.2.2. Modelo de referencia TCP/IP 28

3.3. Redes Telefónicas 29

3.3.1. Elementos de una red telefónica 29

3.3.1.1. Nodos de información 29

3.3.1.2. Enlaces o canales 31

3.3.2. Ruteo para *host* móviles 34

3.3.3. Sistema de radiocomunicaciones móviles 38

3.3.4. Ip móvil 39

**4. SERVICIOS DE RED** 43

4.1. Redes de datos 43

4.1.1. Compartimiento de recursos 44

4.2. Redes telefónicas 44

4.2.1. Servicios básicos 44

4.2.2. Servicios telemáticos 45

4.2.3. Servicios de difusión 46

4.3. RDSI 46

4.3.1. Ventajas de la RDSI 48

4.3.1.1. Velocidad 48

4.3.1.2. Señalización 49

4.3.1.3. Servicios 49

4.3.1.4. Canales y servicios 50

4.4. SONET 51

4.5. SDH 51

4.6. ADSL 52

4.7. Servicios combinados entre redes de datos y redes telefónicas en Guatemala 53

4.7.1. Videotexto 53

4.7.2. Teletexto 54

4.7.3. Correo electrónico 55

4.7.4. Internet 55

**5. SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN** 57

5.1. Asuntos de seguridad 57

5.2. Criptografía 58

5.2.1. Concepto de criptografía 58

5.2.2. Ventajas y uso de la criptografía 59

5.2.3. Algoritmos de encriptamiento para las redes de datos 59

5.2.3.1. Algoritmos simétricos 60

5.2.3.2. Algoritmos asimétricos 60

5.2.4. Algoritmos de encriptamiento para las redes telefónicas 61

5.3. Diseño de la seguridad de la red 62

*5.3.1. Firewall* 62

5.3.2. Estrategias para proteger las conexiones 63

5.3.3. Importancia en la seguridad de la información 64

5.3.4. Gestión de seguridad celular 65

5.4. Vulnerabilidad de las comunicaciones 65

5.4.1. Fuentes de ruido 66

5.4.2. Fuentes de interferencia 68

5.5. Aspectos principales de interferencia de las comunicaciones inalámbricas en la ciudad de Guatemala 68

5.5.1. Tipos de interferencia en sistemas analógicos de telefonía móvil celular en la transmisión de datos 73

5.5.2. Interferencia en sistemas digitales 82

5.6. Mecanismos utilizados por las empresas de telecomunicaciones en Guatemala en la transmisión de datos 86

5.7. Críticas a los aspectos de seguridad en la transmisión de datos y a los servicios que prestan las empresas de telecomunicaciones en Guatemala. 94

5.8. Sugerencias para mejorar la seguridad en la transmisión de datos y los servicios para que las redes telefónicas y las redes de datos sean fuentes más confiables. 97

5.9. Ejemplo de un modelo para incrementar la seguridad en la transmisión de datos de las redes telefónicas a las redes de datos en Guatemala. 99

5.10. Desempeño que realiza la SIT en Guatemala en la seguridad de la transmisión de datos de las redes telefónicas a las redes de datos en cuanto a servicios 109

**CONCLUSIONES** 116

**RECOMENDACIONES** 118

**BIBLIOGRAFÍA** 119

## ÍNDICE DE ILUSTRACIONES

### Figuras


| | | |
|---|---|---|
| 1 | Estructura de un sistema celular TMA | 14 |
| 2 | Elementos de la red GSM | 20 |
| 3 | Modo de conmutación de circuito | 21 |
| 4 | Esquema de ruteo para *host* móviles | 34 |
| 5 | Ruteo de un paquete en un *host* móvil | 37 |
| 6 | Red digital de servicios integrados | 47 |
| 7 | *Firewall* en la red de una empresa | 63 |
| 8 | Forma de interferencia señal /ruido | 66 |
| 9 | Disminución de la señal por la distancia | 70 |
| 10 | Atenuación versus frecuencia | 71 |
| 11 | Desvanecimiento de onda de la señal | 73 |
| 12 | Reducción del tamaño de antenas | 75 |
| 13 | Interferencia de un móvil | 76 |
| 14 | *Drive Test* | 78 |
| 15 | Problemas por fallos de cobertura | 79 |
| 16 | Problema de la diafonía digital | 82 |
| 17 | Supresor de eco para un circuito de dos hilos | 84 |
| 18 | Antena yagi | 85 |
| 19 | Estructura de las tramas | 89 |
| 20 | Utilización del MTSI | 94 |
| 21 | Modelo con incremento de seguridad en una red GSM | 100 |

## Tablas


| | | |
|---|---|---|
| I | Velocidad de transmisión por tipos de cable | 32 |
| II | Reducción de niveles de potencia en los sistemas AMPS | 81 |
| III | Reglas del sistema experto | 108 |

## GLOSARIO

**Abonado** Persona natural o jurídica usuaria, bajo contrato, de una red pública de telecomunicaciones, a la cual tiene derecho a acceder para establecer sus comunicaciones.

**Algoritmo** Conjunto de reglas y procedimientos, expresados mediante datos o símbolos, que describen un estado o una asociación lógica para resolver un problema. Es la condición necesaria para el desempeño de tareas automáticas.

**Algoritmo A3** Algoritmo que se utiliza en el sistema GSM de telefonía móvil para autentificación.

**Algoritmo A5** Algoritmo que se utiliza en el sistema GSM de telefonía móvil para encriptación de la información transmitida.

**Algoritmo A8** Algoritmo que se utiliza en el sistema GSM de telefonía móvil para la generación de la clave de cifrado.

**AMPS (American Mobile Phone System)** Sistema americano de telefonía móvil.

**Atenuación** Disminución del valor eléctrico u óptico recibido de una señal, con respecto a su valor original de emisión.

| | |
|---|---|
| **Canal** | Ruta de transmisión de comunicaciones a través de cualquier clase de medio de transmisión: cable conductor, radio, fibra óptica o de cualquier otro tipo. |
| **CDMA** | Proceso que permite a todos los usuarios transmitir sobre la misma frecuencia al mismo tiempo; cada uno se distingue por su código. |
| **Criptografía** | Técnica de escritura tales que la información esté oculta de intrusos no autorizados. |
| **Conmutación** | Conjunto de operaciones necesarias para unir entre sí los circuitos, para establecer una comunicación temporal entre dos o más estaciones o nodos. |
| **DTE** | Equipo terminal de datos |
| **DCE** | Equipo de terminación del circuito de datos |
| **E1** | Potadora digital de 2.048 Mbps. |
| **Emisor** | Ente que da origen a la información. |
| **Espectro Electromagné-tico** | Es el conjunto de todas las frecuencias de emisión de los cuerpos de la naturaleza. Comprende un amplio rango que va desde ondas cortas (rayos gamma, rayos X), ondas medias o intermedias (luz visible), hasta ondas largas (las radiocomunicaciones actuales). |

| | |
|---|---|
| **GPRS(General Packet Radio Service)** | Red de conmutación de paquetes que está superpuesta a la red GSM. Basado en esta, permite una mayor velocidad de transmisión de datos y posibilita a los terminales estar conectados permanentemente a la red. |
| **GSM** | Sistema celular digital ampliamente usado en todo el mundo. |
| **FDM** | División del flujo de información de entrada, en un número de subflujos que son enviados en canales de radio separados. |
| **Handoff** | Proceso de transferir una unidad móvil de una celda a otra, mientras está en comunicación. |
| **Interfaz** | Punto de una vía de comunicación que permite el intercambio de información entre dos dispositivos o sistemas y para el que se han especificado sus características físicas, eléctricas y el tipo de señales a intercambiar, así como su significado. |
| **Interconexión** | Es la vinculación de recursos físicos y soportes lógicos, incluidas las instalaciones esenciales necesarias, para permitir el interfuncionamiento de las redes y la interoperabilidad de servicios de telecomunicaciones ó de redes de datos. |
| **IP (Internet protocol)** | Protocolo utilizado en Internet. |

| | |
|---|---|
| **ISDN (Integrated service digital network)** | Red digital de servicios integrados |
| **MMS(Multime-dia Messaging Services)** | Servicio de Mensajería Multimedia. Permite transmitir imágenes en movimiento, vídeos, gráficos y sonidos, Junto con el texto de los mensajes. Suponen un gran salto cualitativo respecto al servicio SMS, y es posible gracias a la implantación de las tecnologías GPRS y UMTS. |
| **Modulación** | Modificación de alguno de los parámetros que definen una onda portadora (amplitud, frecuencia, fase), por una señal moduladora que se quiere transmitir (voz, música, datos). |
| **Módem (Modulator/ Demodulator)** | Modulador / Demodulador. Dispositivo electrónico que hace posible que datos digitales sean enviados a través de una facilidad analógica de trasmisión. |
| **MPT (Mobile Protocol Trunking)** | Protocolo del sistema Trunking de telefonía móvil. |
| **MSC (Mobile services Switching Center)** | Central de conmutación de la red GSM |
| **Nodo** | Es el elemento de red, ya sea de acceso o de conmutación, que permite recibir y reenrutar las comunicaciones. |

| | |
|---|---|
| **Operador** | Persona jurídica pública, mixta o privada responsable de la gestión de un servicio de telecomunicaciones en virtud de autorización, licencia o concesión, o por ministerio de la ley. Esta resolución se refiere indistintamente al operador y al concesionario. |
| **PSTN** | Red mundial consistente de cables de cobre y conmutadores en países de todo el mundo, el cual permite llamar a cualquier parte del mundo. |
| **UMTS (universal mobile telecomunica - tions system)** | Sistema universal móvil de telecomunicaciones utilizado en Europa. |
| **TDM (Time Division Multiplex)** | Multiplexando por división de tiempo. |
| **TDMA** | Proceso de dividir el espectro disponible en función del tiempo y dar todo el espectro a un usuario durante un período de tiempo. |
| **Transceptor** | Transmisor y receptor de radio combinados en un único equipo provisto de un sistema de conmutación que le permite trabajar alternativamente en emisión y recepción. |
| **Receptor** | Ente que recibe la información. |

| | |
|---|---|
| **Ruido** | Fluctuación aleatoria de voltaje que obstaculiza la recepción normal de una señal recibida. |
| ***Software*** | Todo el conjunto de programas que un ordenador puede interpretar y que llevan a cabo diferentes funciones de automatización. |
| **SIM (Subcriber Identity Module)** | Módulo de identificación de inscripción |

## RESUMEN

En el presente trabajo se definen los mecanismos para que las redes de datos y las redes telefónicas celulares puedan transmitir datos en forma segura ya que en la actualidad las formas de transmisión de datos por medio de este tipo es característico de las redes tanto telefónicas como redes de datos; en estas se produce un continuo desarrollo y exploración.

Tanto las redes de datos como las redes telefónicas celulares utilizan formas para proteger mejor la información que se maneja dentro de algún tipo de red que por ser pública puede ser accedida por cualquier persona sin tener una especificación total de lo que realiza sobre ella. Este es el caso actual sobre lo que las redes de datos se protegen por medio de mecanismos tales como los cortafuegos (*firewall*) y la encripción de la información utilizada también por las redes telefónicas celulares.

En el primer capítulo se describen los conceptos comunicación, sus componentes tanto en forma natural como a través de medios que involucran la tecnología que va evolucionando para producir comunicación.

En el segundo capítulo se describen las características que tiene la transmisión de los datos en las redes de datos y en las redes telefónicas; describiendo la estructura que hace posible la transmisión de los datos desde estos tipos de redes estos tienen dedicaciones distintas pero en cuanto a estructura presentan similitudes y diferencias. Estos se pueden encontrar en las formas como transmiten la información y por medio de las formas para acceder al medio y estar incorporados en un momento definido.

En el capítulo tres se analizan los componentes que hacen posible a las redes de datos y a las redes telefónicas, por medio de mecanismos móviles por eso se define el sistema de comunicaciones móviles que posibilita la comunicación entre algo que continuamente cambia de lugar y algo que permanece fijo. Así de esta forma definiendo las formas lógicas que hacen posible la intercomunicación entre nodos de un sistema.

En el capítulo cuatro se toman los servicios que se ofrecen por parte de las redes telefónicas y por parte de las redes de datos ya que éstas proveen de servicios de compartir archivos así como de servicios teleinformáticas que involucran a los tipos de redes tratados. Se exponen conceptos de red digital de servicios integrados así como las características que posee esta red que ha surgido como una evolución de las redes telefónicas. Ya que una de las mayores características de las redes de datos y las redes telefónicas celulares es compartir servicios tales como el ingreso a Internet por medio de un teléfono celular.

En el capítulo cinco trata el tema de la seguridad y cómo ésta influye sobre la transmisión de la información en Guatemala. Ya que la información integra se trabaja con mecanismos que involucran la criptografía que usa algoritmos de encripción simétricos y asimétricos para transmitir información sobre las redes de datos, en el caso de las redes telefónicas celulares es realizada por el tipo de transmisión de información ya sea por medio de CDMA o por GSM este es muy utilizado por las empresas de telecomunicaciones de Guatemala.

En este capítulo se investigó cuáles son las formas utilizadas por las empresas guatemaltecas para asegurar que la información transmitida a través de los servicios que ellos prestan es segura, también se anotan observaciones

sobre la seguridad que estas empresas manejan y se les proporciona una sugerencia para incrementar el nivel de seguridad dentro de las red de telecomunicaciones que usa el estándar de las telecomunicaciones GSM.

# OBJETIVOS

## General

- Definir las formas de seguridad por medio de las cuales las redes telefónicas y las redes de datos interactúan en Guatemala para asegurar la integridad de la información que se transmite por ambos medios.

## Específicos

- Identificar las formas seguras en la transmisión de datos tanto en redes de datos como en redes telefónicas.

- Conocer las formas seguras que utilizan las redes de datos y las redes telefónicas para la transmisión de la información.

- Analizar las formas similares que existen entre las transmisiones seguras de las redes de datos y las telefónicas y cuales son las formas con las cuales pueden trabajar ambos tipos de redes.

- Documentar las formas seguras que existen para la transmisión de la información y especialmente aquellas que se pueden aplicar sobre las redes tanto telefónicas como de datos.

# INTRODUCCIÓN

Por la evolución continua del mundo se han venido provocando cambios en diversos aspectos y entre ellos, la comunicación. Esta es una forma de transmitir información de distinta naturaleza y de distintos intereses, por ella.

Las formas de comunicación desde la antigüedad hasta nuestros tiempos han evolucionado continuamente desde medios convencionales como el papel hasta los medios digitales actuales los como los correos electrónicos. Estos son consultados desde cualquier dispositivo digital con acceso a la Internet y entre estos dispositivos los teléfonos celulares que han alcanzado gran difusión porque integran servicios digitales hacia este tipo de dispositivos además del creciente uso de la telefonía celular en nuestro medio se presenta un nicho en el cual las grandes empresas de telefonía están apostando hacia nuevos horizontes de la tecnología en redes que vinculan tanto las redes de datos como las telefónicas.

Los servicios telefónicos están creciendo mediante el uso de los servicios de Internet. Siempre debe cuidarse la funcionalidad y confidencialidad. Por ello es importante la transmisión de los datos de las redes telefónicas hacia las redes de datos en forma segura, y viceversa.

# 1. FUNDAMENTOS DE LA COMUNICACIÓN

## 1.1. Concepto de comunicación

Proceso de transmisión y recepción de ideas, información y mensajes.

## 1.2. Elementos de la comunicación

El tipo de sistema de comunicación más estudiado consta de varios componentes. El primero es una fuente de información (por ejemplo, una persona hablando) que produce un mensaje o información que será transmitida. El segundo es un transmisor (como, por ejemplo, un teléfono y un amplificador, o un micrófono y un transmisor de radio) que convierte el mensaje en señales electrónicas o electromagnéticas. Estas señales son transmitidas a través de un canal o medio, que es el tercer componente, como puede ser un cable o la atmósfera. Este canal es especialmente susceptible a interferencias procedentes de otras fuentes, que distorsionan y degradan la señal. (Algunos ejemplos de interferencias, conocidas como ruido, incluyen la estática en la recepción de radios y teléfonos, y la nieve en la recepción de imágenes televisivas). El cuarto componente es el receptor, como por ejemplo el de radio, que transforma de nuevo la señal recibida en el mensaje original. El último componente es el destinatario, como por ejemplo una persona escuchando el mensaje.

## 1.3. Comunicación digital

Esta comunicación como tal no diverge del concepto original de comunicación ya que el único valor agregado a este tipo de comunicación es el conjunto de mecanismos o dispositivos digitales como lo pueden ser el teléfono, fax, Internet, etcétera. Uno de los grandes avances en las comunicaciones ha sido el uso de señales digitales. En telefonía, la señal se digitaliza al llegar a la central de conmutación. La comunicación entre centrales telefónicas es digital, con lo que se reduce el ruido y la distorsión y se mejora la calidad y la capacidad.

## 1.4. Elementos en la comunicación digital

En este entorno los elementos son los mismos que conforman a la comunicación a diferencia de que desde esta perspectiva se tratan todos los componentes de la comunicación como mecanismos digitales. Entre los componentes se pueden mencionar los siguientes:

**Emisor:** es el medio que abre el proceso, la que cuenta con una gran fuente de información. El emisor ha de tener en cuenta los siguientes aspectos:

- Que su contenido sea comunicable.
- Que pueda interceptar al receptor.
- Que el protocolo se adapte al tipo de receptor.

**Receptor:** es el destinatario del mensaje. Para que la comunicación se lleve a cabo eficazmente, el receptor tendrá que tener una actitud previa de receptividad.

**Contenido:** es el mensaje que se quiere transmitir.

**Código:** son las distintas formas y estilos que tiene el emisor de transmitir el mensaje.

**Canal de transmisión:** es el medio por el cual se canaliza el mensaje codificado.

**Retroalimentación** (*Feedback*): es la variable que va a medir la efectividad del proceso de comunicación. Si el receptor responde es que la comunicación ha sido eficaz. Es en este momento cuando el emisor pasa a receptor y viceversa.

## 1.5. Telecomunicación

Un sistema de telecomunicaciones, consiste en una infraestructura física a través de la cual se transporta información desde la fuente hasta el destino, y con base en esta se ofrecen a los usuarios diversos servicios y sistemas en telecomunicaciones, por lo anterior, en lo sucesivo se le denominará “red de telecomunicaciones” a la infraestructura encargada del transporte de la información.

Para recibir un servicio en materia de telecomunicaciones, el usuario utiliza un equipo terminal mediante el que obtiene entrada a la red por medio de un canal de acceso; hay que puntualizar que cada red de telecomunicaciones tiene distintas características, ya que puede utilizar distintas redes de transporte y acorde con esta será el equipo terminal que el usuario necesitará (en una red telefónica se necesitan aparatos telefónicos, etc.).

La principal razón por la que se han desarrollado las redes de telecomunicaciones es porque el costo de establecer un enlace entre dos usuarios de una red sería sumamente elevado si los diferentes usuarios no

tuvieran su equipo terminal conectado a la misma red. Es mucho mejor el contar con una conexión dedicada para que cada usuario tenga acceso a la red mediante su equipo terminal, pero una vez dentro de la red los mensajes utilizan enlaces que son compartidos con otras comunicaciones de diversos usuarios de la misma red.

# 2. TRANSMISIÓN DE INFORMACIÓN

## 2.1. Características de la transmisión de datos

Para que dos mecanismos puedan comunicarse, entre otras, deben usar la misma técnica de modulación. Conforme a la Electronic Industries Association (EIA) en cada extremo de la línea, la computadora se designa como "equipo terminal de datos" (DTE), y el módem, equipo para comunicaciones de datos" (DCE).

### 2.1.1. DTE

Este es un equipo terminal de datos, este equipo puede ser cualquiera, siempre y cuando sea la mente o el destino de los datos.

### 2.1.2. DCE

Equipo de terminación del circuito de datos. Se encarga de transformar las señales portadoras de la información procedentes del DTE en otras que sean susceptibles de ser enviadas hasta el DTE remoto a través de los medios de comunicación existentes.

### 2.1.3. Formas de comunicación

Sin lugar a dudas las comunicaciones ocupan un lugar central y preponderante en el desarrollo de los sujetos. Desde la comunicación oral hasta

la virtual el hombre ha modificado su conducta y su manera de percibir la realidad. En la actualidad las formas de comunicación son un conjunto de tareas tanto reales como virtuales ya que son tan variadas las formas que han evolucionado desde la misma escritura en papel hasta medios electrónicos y digitales que la información que antes se consultaba solamente en papel ahora se puede consultar sobre algunas páginas de Internet. También se pueden mencionar las distintas formas de acceder a la información en los cuales abarca todas aquellas formas que las personas utilizan para conectarse a la información como tal ya sea desde un ordenador o un dispositivo móvil (teléfono celular, pda, palm, etc.).

## 2.2. Transmisión de datos entre redes de datos

### 2.2.1. Formas de transmisión

Se entiende por transmisión de datos al movimiento de información codificada, de un punto a uno o más puntos, mediante señales eléctricas, ópticas, electro ópticas o electromagnéticas. Este requerimiento, ha nacido por la necesidad de poner a disposición de ellas en un punto remoto la capacidad de proceso de un ordenador, ubicado en un punto que podríamos llamar central. Ese punto puede estar dentro de la propia organización, próximo o alejado del ordenador central.

La diferencia importante reside en la distancia y la geografía del problema a considerar, pues en función de estos parámetros, puede ser necesario o no el uso de redes de comunicaciones. Se puede así hablar de dos formas de transmisión de datos:

**Local o en planta:** la propia organización generalmente construye las líneas de comunicaciones necesarias y por lo tanto, los problemas técnicos cuando las distancias son pequeñas resultan mínimos y no requieren consideraciones especiales.

**Remota o fuera de planta:** se necesitan líneas de telecomunicaciones para que sea efectiva, por lo que hay que tener en cuenta una serie de técnicas especiales: la Teleinformática o Telemática. En estos casos existen fuertes restricciones externas derivadas de las regulaciones legales de los sistemas de comunicaciones públicos.

Los sistemas teleinformáticos se tienen así que adaptar a las características técnicas de la infraestructura de telecomunicaciones existente, que inicialmente es siempre la construida para el “servicio telefónico”.

### a) Red Ip

Una red ip es una red de computadoras que utilizan el protocolo TCP/IP y la tecnología subyacente a éste. Tiene muchas ventajas ya que existen una serie de servicios TCP/IP prácticamente universales gracias al desarrollo de Internet, como la Web, el correo electrónico, estándares de videoconferencia, servidores de grupos de noticias etcétera. Y por supuesto, en una red IP se pueden usar esos servicios. Cuando se habla de una red IP en el contexto de un operador de telefonía se está hablando de una red gigantesca implantada por todo el territorio nacional y cuya función es atender a las necesidades de conectividad de usuarios y empresas.

### b) Red ATM

Es una técnica de intercambio rápido de paquetes, es decir es de conmutación de paquetes, orientada a la conexión, diseñada especialmente para trabajar sobre enlaces digitales de alta confiabilidad y con baja tasa de errores. Puede trabajar sobre SVC's o PVC' pero se recomiendan los últimos. Se pretende que, con el tiempo, tiendan a reemplazar a los enlaces punto a punto.

Las velocidades de trabajo van de 64kbps a 2Mbps y por su modo de transmisión en forma de ráfagas es ideal para la interconexión entre redes LAN. La información de señalización en estas redes va por un canal virtual diferente, evitando así cualquier problemática que pudiera surgir y con esto se garantiza la secuencia de entrega de las células transmitidas por el mismo canal virtual.

No existe protección contra errores ni control de flujo en la transferencia de información entre los enlaces. Estos se realizan extremo a extremo entre los terminales de manera transparente a la red, aunque existe un control del tráfico y la congestión en la red.

### *c)* Red *frame relay*

Tecnología paquete-intercambio, esta en el enlace de datos y la especificación de la capa física que proporciona alta funcionamiento. *Frame relay* supone que los medios utilizados provocan menos errores que cuando se usaron X.25 y que ellos transmiten datos con menos sobre la cabecera del paquete. *Frame relay* es más rentable que un enlace punto-a-punto y puede correr típicamente a las velocidades de 64Kbps a 1.544Mbps. *Frame relay*

mantiene rasgos de asignación del ancho de banda dinámica y congestión mando.

### 2.2.2. Tipos de conexiones

Existen tres tipos de conexión a una red, la conexión punto a punto, la conexión multipunto y la conexión inalámbrica.

#### a) Inalámbricas

Como su nombre lo indica es una red que casi no utiliza cables. Básicamente, las redes inalámbricas se basan en el uso de dos tecnologías: ondas de radio y luz infrarroja, que tienen sus pros y contras, específicamente en términos de la velocidad de transmisión, compatibilidad y medio en el cual se instala. Estos pros y contras se pueden resumir así:

Ventajas.

1. Buenas características de desempeño
2. Resistencia a la interferencia externa
3. Bajos costos de operación
4. Facilidad de instalación
5. Facilidad de mantenimiento y detección de fallas
6. Menor tiempo de instalación
7. Buen nivel de integración con redes tradicionales existentes

Limitaciones.

1. Potencia y distancia limitada
2. Velocidad de transmisión limitada
3. Alto costo por unidad

**b) Punto a punto**

Es una conexión de dos dispositivos entre ellos y nadie más. Por ejemplo, una conexión de dos computadores mediante fibra óptica, un cable paralelo o un cable utp.

**c) Multipunto**

Utiliza un sólo cable para conectar más de dos dispositivos. Por ejemplo, un cable coaxial, que tiene varios dispositivos conectados al mismo.

## 2.3. Transmisión de datos entre redes telefónicas

### 2.3.1. Comunicación celular

Este servicio, conocido como TMA (Telefonía Móvil Automática) celular o simplemente TMA, tiene como propósito poder proporcionar al usuario un servicio telefónico público móvil. La telefonía móvil permite mantener comunicación telefónica desde equipos móviles de la misma forma que si utilizaran un teléfono fijo convencional. Un usuario móvil puede efectuar y recibir llamadas telefónicas automáticas con cualquier otro abonado fijo o móvil de la red telefónica.

El usuario de Telefonía móvil puede realizar llamadas nacionales e internacionales en sus desplazamientos, manteniendo en su zona de cobertura la disponibilidad telefónica de su domicilio.

TMA maneja un gran número de abonados móviles dispersos por una amplia zona con explotación automática. Esto supone resolver una serie de aspectos:

- Conmutación automática de la comunicación y su continuidad.
- Radio búsqueda de un móvil, que debe preceder a toda comunicación.
- Consecución de un nivel de calidad de la conmutación con la selección automática de estaciones para mantener esa calidad en el curso de la conversación.

En los sistemas TMA se necesita conseguir una amplia cobertura con gran capacidad de tráfico y con un número limitado de frecuencias. Esto se consigue gracias a la reutilización sistemática de las frecuencias, lo que se logra mediante estructuras celulares.

#### 2.3.1.1 Definición y principios de la comunicación móvil

Un sistema de comunicaciones móvil celular usa un número grande, de bajo - poder para transmisores inalámbricos para crear la **–** célula; el área de servicio geográfica básica de un sistema de comunicaciones inalámbrico. Los niveles de poder inconstantes permiten a las células ser clasificado según tamaño según la densidad del subscriptor y exigir dentro de una región particular. Cuando los usuarios móviles viajan de la célula a la célula, sus conversaciones son "dar fuera de" entre las células para mantener servicio no amarrado. Cauces (frecuencias) usó en una célula puede reutilizarse lejos en otra célula un poco de distancia. Pueden agregarse células para acomodar crecimiento y pueden crear nuevas células en áreas sin servicio o las células recubriendo en áreas existentes.

Los sistemas de radiocomunicaciones móviles permiten el intercambio de información entre estaciones fijas o móviles (o entre dos móviles) utilizando como medio de transmisión el espectro radioeléctrico. Permiten conectar centros de control públicos o privados y redes telefónicas con personas o vehículos equipados con sistemas de radio.

Cuando el ámbito de aplicación de los sistemas de radiocomunicaciones móviles se centra en el servicio telefónico se habla entonces de servicio de radiotelefonía móvil (SRTM).

Actualmente, se está extendiendo el ámbito de utilización de sistemas móviles a servicios no telefónicos como son los de transmisión digital (datos, tele media, telemando, alarmas). Dentro de los sistemas de radiocomunicaciones móviles puede citarse con entidad propia el sistema de radio búsqueda.

#### 2.3.1.2 Componentes de un sistema celular

Los elementos o componentes básicos del sistema TMA son las estaciones base, las centrales de conmutación, zona de cobertura y las estaciones móviles.

**Estaciones base:** las estaciones base son los equipos que establecen el contacto con los teléfonos móviles del cliente y por tanto determina la cobertura del servicio. Consiste en una computadora y un transmisor/receptor conectado a una antena. Existe una amplia red de estaciones base las cuales están conectadas a centrales de conmutación específicas para la Telefónica Móvil (MTSO, Mobil Telephonic Switch Office o MSC, Mobil Swith Center).

**Centrales de conmutación para telefonía móvil:** dan servicio a las estaciones base y a su vez se conectan con las centrales de la red telefónica fija, para sostener conversaciones tanto entre teléfonos móviles como entre teléfonos móviles y fijos. En grandes sistemas son necesarios múltiples MTSO conmutándose éstos en un segundo nivel de MTSO y así sucesivamente.

**Zona de cobertura:** la zona de cobertura del servicio contempla la totalidad del territorio nacional, especialmente las áreas urbanas y vías de comunicación más importantes. La superficie total a la que se extiende el servicio es dividida en subáreas o celdas atendidas por una estación base.

**Estación móvil:** es el terminal telefónico móvil. El propio teléfono móvil indicará al usuario cuando se encuentra dentro de la zona de cobertura.

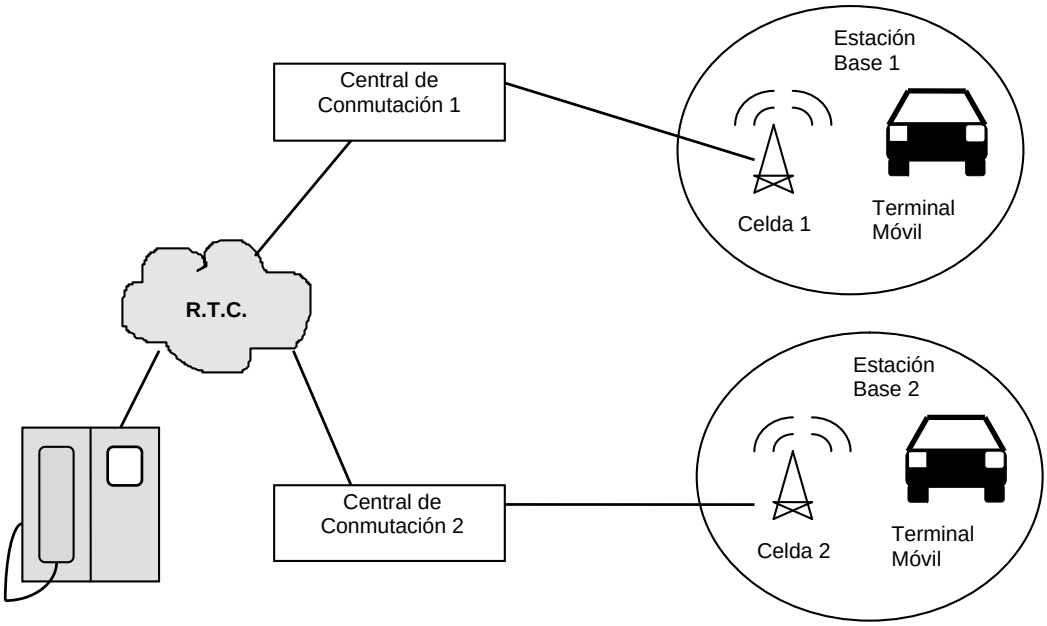
Las personas que quieran establecer una comunicación con un usuario del servicio de telefonía móvil no necesitan saber dónde se encuentra éste ya que el propio sistema se encarga automáticamente de localizarle para establecer la comunicación.

#### 2.3.1.3 Estructura de un sistema celular

La comunicación base-móvil o móvil-móvil en una frecuencia específica sólo es posible si no se supera una distancia entre ellos denominada radio de cobertura, cuyo valor es proporcional a la altura de las antenas de la estación móvil y la estación base.

Superada esta distancia la atenuación es tan elevada que no es posible la comunicación.

Figura 1: Estructura de un sistema celular TMA




Los sistemas celulares se basan en subdividir la superficie total a cubrir en zonas más pequeñas llamadas **celdas o células,** a las que se asigna una estación base con un cierto número de frecuencias o canales.

Como el espectro radioeléctrico y el número de canales o comunicaciones posibles al mismo tiempo son limitados, se puede dividir la superficie total a cubrir en celdas de modo que las frecuencias que se usan en una celda puedan ser reutilizadas en otra celda lejana. Separando adecuadamente las celdas a una distancia (llamada distancia cocanal o de reutilización) determinada por la relación de protección de RF, puede reutilizarse el mismo juego o conjunto de frecuencias en diversas celdas. Reutilizando frecuencias, un sistema celular puede cursar un tráfico superior al número de frecuencias asignadas a la banda.

En la práctica, el número total de canales disponibles “C” se divide entre las celdas de una configuración unitaria básica denominada **grupo básico**. Un tamaño típico para el grupo es siete si las estaciones base utilizan antenas omnidireccionales, nombrándose las celdas, de la A a la G.

### 2.3.2. Tipos de redes telefónicas

Desde el punto de vista de la conformación de las redes telefónicas, estas pueden ser clasificadas como redes de telecomunicaciones conmutadas o de difusión.

#### 2.3.2.1 Redes conmutadas

Este tipo de red consiste en una sucesión alternada de nodos y canales de comunicación, debiendo entender a los nodos como los repetidores de la información, ya que una vez que un mensaje viaja por los canales de comunicación, llega aun nodo que a su vez lo retransmite a la red de nuevo hasta que llega a otro nodo y así sucesivamente hasta el destino final.

Existen dos tipos de conmutación en este tipo de redes; (i) la de paquetes, que es cuando el mensaje se divide en pequeños paquetes, y a cada uno de ellos se le agrega cierta información de control (Ej. la información de su origen y la del destino) y esta circula de nodo en nodo siguiendo diferentes rutas, y al llegar al usuario final se reensambla el mensaje y se le entrega; y (ii) la de circuitos, que busca y reserva una trayectoria entre los usuarios de la red, se establece una comunicación y se mantiene durante todo el tiempo de transferencia de información (Ej. Internet), para establecer este tipo de conexión, se requiere de una señal que reserve los diferentes segmentos que

necesita la misma, pero una vez establecida este medio de transmisión quedará únicamente reservado para ese fin (Ej. la línea telefónica en conexiones a Internet)

#### 2.3.2.2 Redes de difusión

Este tipo de red tiene un canal al que están conectados todos los usuarios, pero solo pueden extraer del sistema los mensajes que identifican su dirección como destinatarios, estos sistemas tienen solamente un nodo (llamado “nodo transmisor”), mismo que inyecta la información en un canal al que están conectados todos los usuarios.

Para todo tipo de redes, el usuario requiere de un equipo terminal, para tener acceso a la misma, pero que no forma parte de ella, de tal manera que si un usuario necesita comunicarse con otro no lo realiza mediante su equipo terminal, sino que tiene que enviar la información a la red y esta la hará llegar al equipo terminal del destinatario.

Es importante el señalar que no en todos los sistemas de telecomunicaciones los usuarios pueden transmitir información en las redes; ya que en el caso de la radio y la televisión entre otros, los usuarios son pasivos, es decir, únicamente pueden recibir la información que se manda mediante las estaciones transmisoras, mientras que en la telefonía todos los usuarios pueden transmitir y recibir información.

Otra característica importante de las redes de telecomunicaciones es su cobertura geográfica, ya que esta determinará y/o limitará el área en la que el usuario puede conectarse, (Ej. un intranet corporativo, conocido como LAN

Local Area Network), aunque también existen redes de cobertura más amplia conocidas como WAN (Wide Area Network).

Caso aparte son las redes de cobertura urbana que distribuyen señales de televisión por cable en una ciudad, y cuando estas se reúnen forman las redes nacionales, y la unión de esta configuran las redes globales de información, con lo que cualquier usuario del mundo tiene acceso a la mayoría de los acontecimientos que son de su interés, lo que ha originado el término de "globalización de la información".

### 2.3.3 Formas de acceso

Existen tres tipos de técnicas de acceso básicas: FDMA (frecuency division multiple access), TDMA (time division multiple access) y CDMA (code division multiple access).

#### 2.3.3.1 FDMA

Esta técnica asigna a cada usuario una frecuencia de 30 KHz de ancho de banda en el sistema analógico AMPS (Advanced Mobile Phone System). Como el espectro es limitado, solo se podían acomodar un número fijo de usuarios. Por lo que al ingresar más usuarios al sistema, se empezaron a bloquear los canales.

#### 2.3.3.2 TDMA

Es un sistema de acceso múltiple divide el canal de 30 KHz en 3 ranuras de tiempo. TDMA, técnica conocida también como IS-54, fue adoptada en 1991

en Estados Unidos (EUA) por la TIA (Telephone Industry Association) bajo la presión de fabricantes europeos que intentaban vender sus equipos al mercado estadounidense. TDMA vino a triplicar en magnitud de 3 el número de usuarios en comparación con el sistema analógico AMPS de la primera generación de celulares. Al incrementarse el número de usuarios, esta técnica de acceso múltiple también es ineficiente. TDMA es una técnica de transmisión vía satélite en la cual diversas estaciones terrestres tienen acceso al total de la potencia y del ancho de banda del transponedor, con cada estación trasmitiendo secuencialmente y en pequeños trenes de impulso.

#### 2.3.3.3 CDMA

Tecnología desarrollada por Qualcomm, utiliza la tecnología de espectro disperso en la cual muchos usuarios comparten simultáneamente el mismo canal pero cada uno con diferente código. Lo anterior permite una mayor capacidad en usuarios por celda. Un canal puede ser visto como una porción del espectro radioeléctrico, el cual es asignado temporalmente para un propósito específico, tal como una llamada telefónica.

Una técnica de acceso múltiple define como se divide el espectro de frecuencias en canales y como los canales son asignados a los múltiples usuarios en el sistema. Visto de otra manera, el seleccionar una técnica eficiente de acceso múltiple significa que los operadores telefónicos (portadoras o carriers) obtendrán más ganancias al acomodar más usuarios en sus redes inalámbricas.

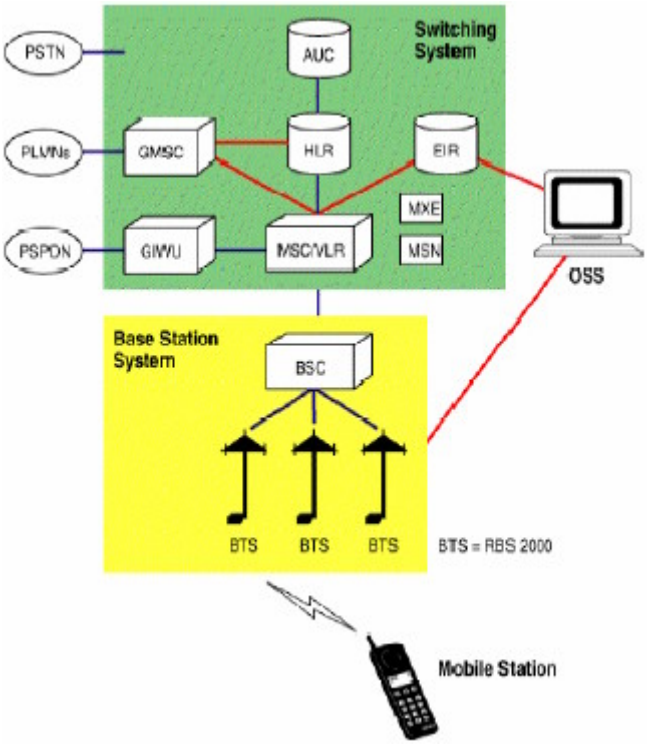
Las técnicas de acceso múltiple son utilizadas en el ambiente de las comunicaciones para que varios dispositivos [computadoras, teléfonos, radios, etc.] puedan acceder al medio o canal de comunicación de manera ordenada. Sin las técnicas de acceso múltiple, las comunicaciones entre dispositivos sería

un caos. Las técnicas de acceso múltiple nos permiten compartir un mismo canal de comunicación para varios usuarios.

#### 2.3.3.4 GSM(siglas derivadas originalmente de Group Special Mobil)

La tecnología celular desarrollada en Europa es considerada como la tecnología celular más madura, con mas de 200 millones de usuarios en mas de 100 países alrededor del mundo. GSM es un servicio de voz y datos basado en conmutación de circuitos de alta velocidad la cual combina hasta 4 ranuras de tiempo en cada canal de radio. Especifica tres modalidades estándar de transmisión: 144kbits/s para usuarios de mucha movilidad, 384kbits/s para movilidad "de a pie", y 2mbit/s para usos estacionarios, en construcción GSM proporciona recomendaciones, no requisitos. Las especificaciones de GSM definen las funciones y requisitos de la interface en detalle pero no se dirige al hardware. La razón para esto es limitar a los diseñadores tan pequeño como posible pero inmóvil para hacerlo posible para los operadores comprar equipo de los proveedores diferentes. La red de GSM es dividido en tres sistemas mayores: el sistema cambiando (SS), el sistema de la estación bajo (BSS), y el funcionamiento y sistema de apoyo (OSS). El GSM básicos conectan una red de computadoras se muestran elementos en figura 2.

Figura 2: Elementos de la red GSM

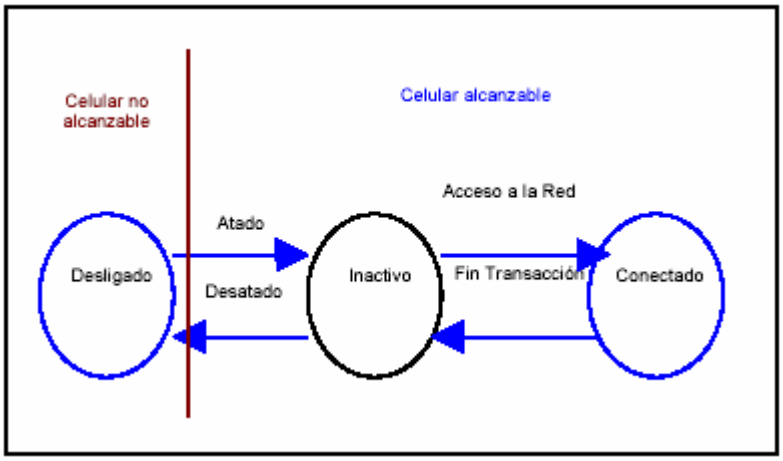



La estación Base del Sistema (BSS): todas las funciones radio-relacionadas se realizan en el BSS que consiste en estación base a directores (BSCs) y la estación transrecibidor bajo (BTS).

**La BSC:** proporciona todo el mando funciones y los enlaces físicos entre el MSC y la BTS. Es un interruptor de alta-capacidad que proporciona funciones como handover datos de configuración de celda y mando de frecuencia de la radio (RF) el poder nivela en estaciones del transrecibidor. El número de BSCs es servido por un MSC.

**BTS:** maneja la interface de la radio a la estación móvil. El BTS es el equipo de la radio (transrecibidores y antenas) necesarias para cada servicio de la celda en la red. Un grupo de BTSs se controla por un BSC.

Figura 3. Modo de conmutación de circuito.




El proceso de una llamada es tal como se muestra en la figura 3. Los funcionamientos y centro de mantenimiento (OMC) se conecta a todo el equipo en el sistema cambiando al BSC. La aplicación de OMC se llama el funcionamiento y sistema de apoyo (OSS). El OSS es la entidad funcional de que el operador de la red supervisa y mandos el sistema. El propósito de OSS es ofrecer apoyo rentable al cliente para centralizar, regional, y localmente operaciones y actividades de mantenimiento que se requieren para una red de GSM. La función importante de OSS es proporcionar una apreciación global de la red y apoyar las actividades de mantenimiento de funcionamiento diferente y organizaciones de mantenimiento.

# 3 REDES FÍSICAS Y REDES LÓGICAS

A nivel estructural la clasificación de una red siempre se inclina hacia una de dos categorías las cuales pueden ser físicas y lógicas ya que el hecho de la realización y manipulación de una red debe primero ser concebida a un nivel lógico para que luego pueda ser construida en un medio físico.

Las conexiones físicas permiten a los dispositivos transmitir y recibir señales directamente y las conexiones lógicas, o virtuales, que permiten intercambiar información a las aplicaciones informáticas, por ejemplo a un procesador de textos. Las conexiones físicas están definidas por el medio empleado para transmitir la señal, por la disposición geométrica de los dispositivos (topología) y por el método usado para compartir información.

## 3.1 Redes de datos

Las redes de datos son aquellas por medio de las cuales se transmite información de un ordenador hacia uno o más computadoras conectados a la red.

### 3.1.1 Elementos de una red de datos

Existen muchos componentes en las redes de datos pero los principales elementos que necesitamos para instalar una red son:

- Tarjetas de interfaz de red
- Cable

- Protocolos de comunicaciones.
- Sistema operativo de red.
- Aplicaciones capaces de funcionar en red

Tarjetas de interfaz de red: las tarjetas de interfaz de red (NICs - Network Interface Cards) son adaptadores instalados en un dispositivo, conectándolo de esta forma en red. Es el pilar en el que sustenta toda red local y el único elemento imprescindible para enlazar dos computadoras a buena velocidad (excepción hecha del cable y el *software*).

**Cables:** utilizados para formar una red se denomina a veces medio. Los tres factores que se deben tener en cuenta a la hora de elegir un cable para una red son:

- Velocidad de transmisión que se quiere conseguir.
- Distancia máxima entre ordenadores que se van a conectar.
- Nivel de ruido e interferencias habituales en la zona que se va a instalar la red.

Los cables más utilizados son el par trenzado, el cable coaxial y la fibra óptica.

**Protocolos de comunicaciones:** conjunto de reglas de comunicaciones entre dispositivos (computadoras, teléfonos, enrutadores, conmutadores, etc). Los protocolos gobiernan el formato, sincronización, secuencia y control de errores. Sin estas reglas, los dispositivos no podrían detectar la llegada de bits.

**Sistema operativo de red:** el *software* de red consiste en programas informáticos que establecen protocolos, o normas, para que las computadoras se comuniquen entre sí. Estos protocolos se aplican enviando y recibiendo

grupos de datos formateados denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente.

**Aplicaciones capaces de funcionar en red:** está formado por programas informáticos que se comunican con los usuarios de la red y permiten compartir información (como archivos, gráficos o videos) y recursos (como impresoras o unidades de disco). Un tipo de *software* de aplicaciones se denomina cliente-servidor. Las computadoras cliente envían peticiones de información o de uso de recursos a otras *computadoras* llamadas servidores, que controlan datos y aplicaciones. Otro tipo de *software* de aplicación se conoce como “de igual a igual” (peer to peer). En una red de este tipo, los ordenadores se envían entre sí mensajes y peticiones directamente sin utilizar un servidor como intermediario.

### 3.1.2 Cableado estructurado

El sistema de cableado constituye el nivel de infraestructura básica de una red de comunicaciones corporativa, su buen diseño y correcta instalación son importantes teniendo en cuenta que es una de las principales causas que pueden afectar al buen funcionamiento de una red. Por otra parte, siempre hay que tener presente los estándares que marcan la calidad en un sistema de cableado, utilizando material de fabricantes reconocidos y las instalaciones se deben llevar a cabo siguiendo las normativas más adecuadas en cada caso. Un sistema de cableado estructurado tiene (en su parte física) dos partes fundamentales, y en este sentido están fijados por las normas.

Por un lado está el cable en sí mismo, y las normas exigen para cada cable y para cada modo de funcionamiento unas determinadas formas de

comportamiento, fundamentalmente relacionadas con la velocidad de transmisión, la longitud del cable y la atenuación que se produce en la señal.

Por otra parte, tenemos el modo de conexionar el cable, fijándose una serie de recomendaciones en el sentido de hacer lo más común para todas las instalaciones la manera de conectar los distintos subsistemas que forman parte de la red.

### 3.1.3 Repetidores

Dispositivo electrónico que opera sólo en la capa física del modelo OSI (capa 1). Un repetidor permite sólo extender la cobertura física de una red, pero no cambia la funcionalidad de la misma. Un repetidor regenera una señal a niveles más óptimos. Es decir, cuando un repetidor recibe una señal muy débil o corrompida, crea una copia bit por bit de la señal original. La posición de un repetidor es vital, éste debe poner antes de que la señal se debilite. En el caso de una red local (LAN) la cobertura máxima del cable UTP es 100 metros; pues el repetidor debe ponerse unos metros antes de esta distancia y poner extender la distancia otros 100 metros ó más.

Existen también regeneradores ópticos conocidos como EDFA (Erbium-Doped Fiber Amplifier) los cuales permiten extender la distancia de un haz de luz sobre una fibra óptica hasta 125 millas.

## 3.2 Niveles lógicos en las redes de datos

En las redes de datos para hacer posible la comunicación entre ordenadores es necesario el establecimiento de la forma lógica como la información debe de ser transportada por el medio físico. El primer nivel lógico

establecido para las redes de datos se le conoce como modelo de referencia OSI. Cuando ese establecimiento lógico por medio del cual los datos van a ser transportados se le denomina como protocolo. En las redes de datos el protocolo más utilizado es el modelo tcp/ip.

### 3.2.1 Modelo de referencia OSI

El modelo OSI (Open System Interconnection) es el comienzo de cualquier estudio de redes. Es un modelo idealizado de 7 capas o niveles que representa la subdivisión de tareas teórica que se recomienda tener en cuenta para el estudio o diseño de un sistema.

A cada capa se le asigna una función bien específica y las mismas se apilan desde la inferior a la superior de forma que cada una depende de la inmediata inferior para su funcionamiento. Esto no significa que todas las redes cumplan o deban cumplir exactamente con este modelo y de hecho, normalmente no lo hacen pero de todas formas se recomienda siempre tener en cuenta el modelo OSI como referencia, ya que conocimiento del mismo posibilita la correcta comprensión de cualquier red e inclusive facilita el poder realizar la comparación entre sistemas diferentes.

Las 7 capas son las siguientes:

- **Capa 1 (física)**: define las reglas para transmitir el flujo de bits por el medio físico.
- **Capa 2 (enlace)**: organiza los bits en grupos lógicos denominado tramas o frames. Proporciona además control de flujo y control de errores.
- **Capa 3 (red)**: Proporciona la posibilidad de rutear la información agrupada en paquetes.

- **Capa 4 (transporte)**: realiza el control de extremo a extremo de la comunicación, proporcionando control de flujo y control de errores. Esta capa es asociada frecuentemente con el concepto de confiabilidad.
- **Capa 5 (sesión)**: conexión y mantenimiento del enlace.
- **Capa 6 (presentación)**: frecuentemente forma parte del sistema operativo y se encarga de dar formato los datos.
- **Capa 7 (aplicación)**: servicios para el usuario como ser e-mail, servicios de archivos e impresión, emulación de terminal, login, etc.

Es importante aclarar con respecto a esta última que no cualquier aplicación que corra dentro de una PC encuadra en la capa aplicación del modelo OSI, sino solamente las aplicaciones a los efectos del trabajo en red.

### 3.2.2 Modelo de referencia TCP/IP

Las capas de la suite de TCP/IP son menos que las del modelo de referencia OSI, sin embargo son tan robustas que actualmente une a más de tres millones de nodos en todo el mundo.

La capa inferior, que podemos nombrar como física respecto al modelo OSI, contiene varios estándares del Instituto de Ingenieros Electrónicos y Eléctricos (IEEE en inglés) como son el 802.3 llamado ethernet que establece las reglas para enviar datos por cable coaxial delgado (10Base2), cable coaxial grueso (10Base5), par trenzado (10Base-T), fibra óptica (10Base-F) y su propio método de acceso, el 802.4 llamado token bus que puede usar estos mismos medios pero con un método de acceso diferente, el X.25 y otros estándares denominados genéricamente como 802.X.

La siguiente capa cumple, junto con la anteriormente descrita, los niveles del modelo de referencia 1,2 y 3 que es el de red. En esta capa se definió el protocolo IP también conocido como "capa de Internet". La responsabilidad de este protocolo es entregar paquetes en los destinos indicados, realizando las operaciones de enrutado apropiadas y la resolución de congestionamientos o caídas de rutas.

La capa de transporte es la siguiente y está implantada por dos protocolos: el TCP (Transmission Control Protocol) y el UDP (User datagram Protocol). El primero es un protocolo confiable y orientado a conexiones, lo cual significa que nos ofrece un medio libre de errores para enviar paquetes. El segundo es un protocolo no orientado a conexiones y no es confiable. El TCP se prefiere para la transmisión de datos a nivel red de área amplia y el otro para redes de área local.

La última capa definida en la suite de TCP/IP es la de aplicación y en ella se encuentran decenas de aplicaciones ampliamente conocidas actualmente. Las más populares son el protocolo de transferencia de archivos (FTP), el emulador de terminales remotas (Telnet), el servicio de resolución de nombres (Domain Name Service DNS), el WWW, el servicio de correo electrónico (Simple Mail Transfer Protocol SMTP), el servicio de tiempo en la red (Network Time Protocol NTP), el protocolo de transferencia de noticias (Network News Transfer Protocol NNTP) y muchos más.

## 3.3 Redes telefónicas

Las redes telefónicas han sido las primeras manifestaciones de redes tanto a nivel físico como a nivel lógico ya que la arquitectura que poseen ha sido la base para las redes de datos actuales.

### 3.3.1 Elementos de una red telefónica

En una red telefónica existen un conjunto de elementos interactuando para completar el proceso por medio del cual dentro de una red telefónica pueden ser utilizados los recursos que se poseen. Los principales elementos que se tienen en estas redes son los nodos de información y los enlaces o canales.

#### 3.3.1.1 Nodos de información

Son parte fundamental de cualquier red de telecomunicaciones, son los encargados de realizar las diversas funciones de procesamiento que requieren cada una de las señales o mensajes que circulan o transitan mediante los enlacen en una red.

Los nodos proporcionan enlaces físicos entre los diversos canales que conforman la red, generalmente los nodos son equipos digitales, aunque pueden tener parte analógica como un modulador, y realizan las siguientes funciones:

- **Establecimiento y verificación de un protocolo:** garantizando una comunicación exitosa utilizando los canales que los entrelazan.
- **Transmisión:** los nodos se adaptan al canal a la información o a los mensajes que contiene para su adecuada y efectiva transportación en la red.
- **Interfase:** el nodo se encarga de proporcionar al canal las señales que serán transmitidas de acuerdo con el medio del que está formado el canal, adecuando la salida a la manera de transmisión sin importar si ingresaron codificadas para otro tipo de sistema.

- **Recuperación:** si en una transmisión no se completa el paso de la información, los nodos permiten recuperar lo transmitido, y enviar de nuevo el total o el faltante.
- **Formateo:** se utiliza en el caso de que las terminales de una red no utilicen todas el mismo formato, los nodos permiten cambiar la información al formato requerido, o bien el reformatear la misma.
- **Enrutamiento:** proporcionan los nodos la información del usuario de origen y del de destino de la información, esto debe de realizarse en cada nodo, ya que como lo mencionamos, existen diversos nodos en una red.
- **Repetición:** es una retransmisión acorde a los protocolos establecidos, que se realiza mediante petición automática del nodo receptor al transmisor.
- **Direccionamiento:** los nodos detectan direcciones para poder hacer llegar mensajes a su destino mediante un canal predeterminado.
- Control de flujo: detecta la saturación de los canales de información.

#### 3.3.1.2 Enlaces o canales

El canal es el medio físico mediante el que la información viaja de un punto a otro, y sus características son sumamente importantes para una comunicación efectiva, ya que de ellos depende la calidad de las señales recibidas, y de acuerdo con el tipo de material del que se encuentre hecho el canal, serán los valores de transmisión que pueda tener, acorde a la siguiente tabla:

Tabla I. Velocidad de transmisión por tipos de cable

| | |
|---|---|
| 30 – 300 Kilohertz<br>Cable de cobre (par trenzado) | Hasta 4 Mbps (4 millones de bits por segundo) |
| Cable coaxial | Hasta 500 Mbps (500 millones de bits por segundo) |
| Fibra óptica | Hasta 2000 Mbps (2000 millones de bits por segundo, o bin 2 “giga” bsp: 2Gbps) |

Los cables de cobre siguen siendo el medio más utilizado para la transmisión analógica como digital, ya que son la base de las redes telefónicas urbanas (con todo y la incursión de la fibra óptica), pero la desventaja que presenta es que dependiendo de la señal, debe de ser colocados repetidores de la misma cada 5 ó 6 kilómetros.

Los cables coaxiales tienen un aislante que separa al conductor central de ruido en la transmisión mediante un blindaje, son muy utilizados en telecomunicaciones de larga distancia y en transmisiones de televisión, y de manera más reciente en la transmisión de datos; pero la distancia entre las repetidoras debe de ser la misma que en los cables de cobre, ya que se utiliza una mayor banda para la transmisión, lo que permite una mejor tasa en la comunicación digital.

La fibra óptica transmite señales ópticas en lugar de eléctricas, es un material mucho más ligero que los anteriormente mencionados, y transmiten tasas más altas que los primeros; además, aunque las señales se vean

afectadas por ruido, no se alteran si es eléctrico, y soportan distancias mayores en las repetidoras –del orden de los 100 kilómetros-, se utiliza principalmente para enlaces de larga distancia, metropolitanos y redes locales.

Por otra parte, también hay que hacer mención de los canales que difunden una señal sin la necesidad de una guía, como los de radio, las microondas y los enlaces satelitales.

Los enlaces satelitales funcionan de una manera muy parecida a las microondas, un satélite recibe de una estación terrena o terrestre, las amplifica mediante un transponedor y las envía mediante otra banda de frecuencias.

El principio de funcionamiento de un satélite es muy sencillo; se envían señales de una antena de cualquier tipo a un satélite artificial estacionado en un punto fijo alrededor de la tierra (“satélite geoestacionario”) o de “órbita móvil”.

Los satélites tienen un reflector o “transponedor” orientado hacía el lugar en donde se pretende hacer llegar la señal reflejada, en donde también se tienen antenas que reciben la señal de origen, a partir de su recepción la señal se procesa o retransmite y se hace llagar a su lugar de destino final.

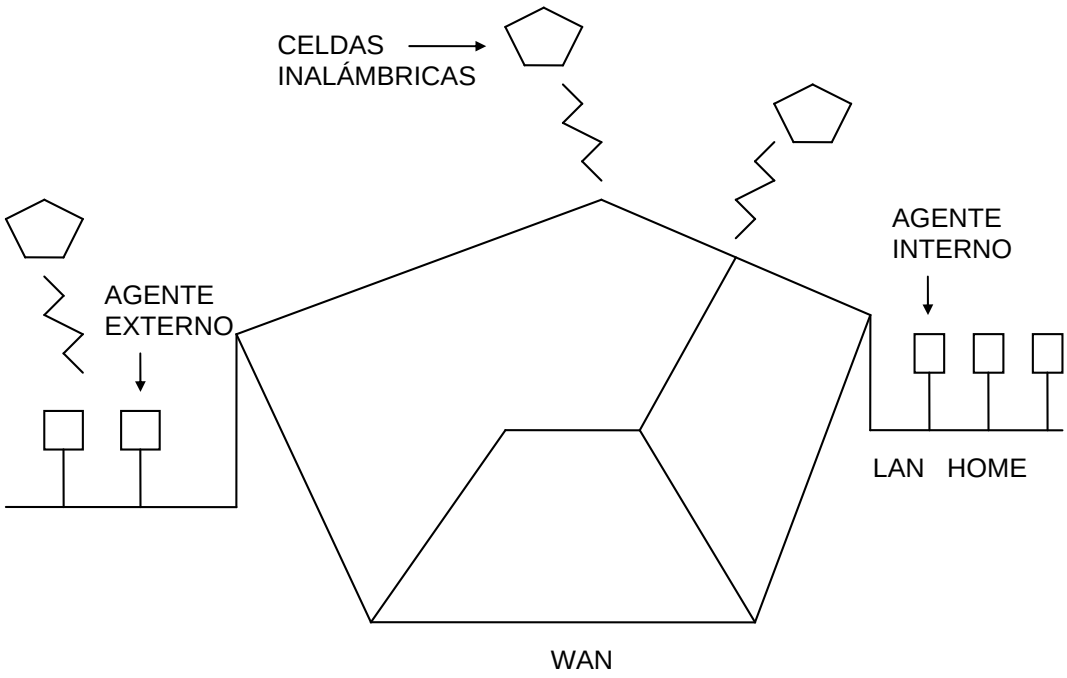
Las ventajas de la comunicación por satélite son muy evidentes; ya que se puede transmitir a larga distancia sin importar la orografía, hidrografía o clima imperante en ambos lugares (el de transmisión y el de recepción); se pueden utilizar antenas de gran cobertura, de tal manera que pueden transmitir y recibir señales al mismo tiempo, las tasas de transmisión pueden ser desde las más pequeñas hasta las más grandes, los requerimientos de acceso múltiple, manejo de diversos tipos de tráfico, establecimiento de redes,

integridad de los datos y seguridad, se manejan mediante la tecnología VSAT (Very Small Aperture Terminals).

### 3.3.2 Ruteo para *host* móviles

Hoy en día millones de personas tienen computadoras portátiles y generalmente quieren leer su correo y acceder normalmente a los sistemas de ficheros donde quiera que estén. Aparece entonces una nueva complicación para enrutar un paquete de un *host* móvil, la red primero tiene que localizarlo. El tema de incorporar un *host* móvil en la red es muy joven, pero veamos algunas soluciones. Supongamos una WAN con varias LANs.

Figura 4: Esquema de ruteo para *host* móviles



Los usuarios que nunca se mueven son estacionarios. Son conectados a la red por fibras ópticas o cobre. Por otro lado, distinguimos otros tipos de usuarios. Los usuarios migratorios son usuarios básicamente estacionarios que se mueven de un sitio fijado a otro pero usan la red sólo cuando ellos están físicamente conectados a ella. Los usuarios móviles (roaming) son los que quieren mantener su conexión mientras están en movimiento.

Todos los usuarios están asumidos en una localización permanente (casa), que nunca cambia. También tienen una dirección de casa que indica cual es su localización permanente, parecida al prefijo de los números de teléfono. El ruteo en un sistema con usuarios móviles hace posible enviar paquetes a usuarios móviles usando su dirección de casa, dejando los paquetes donde quiera que estén.

En la figura 4 encontramos pequeñas divisiones (geográficas) de áreas que son LAN o celdas inalámbricas. Cada área tiene una o más agentes externos, los cuales siguen la pista a todos los usuarios móviles visitantes en el área. Además cada área tiene agentes internos (casa) que siguen la pista de los usuarios que tienen su casa en este área pero que están visitando otra área.

Cuando un nuevo usuario entra en un área, bien para conectarse por ejemplo en una LAN o simplemente para errar por la celda, esta computadora debe registrarse como agente externo. Este registro provoca seguir los siguientes pasos:

1. Periódicamente, cada agente externo envía un paquete en broadcast comunicando su existencia y dirección. Una llegada de un host móvil esperará uno de estos mensajes, pero si no llega rápidamente el host

móvil puede enviar un broadcast diciendo "*¿Hay algún agente externo?"*

2. El móvil es registrado por el agente externo dando su dirección de casa, su dirección del nivel de enlace y alguna otra información de seguridad.

3. El agente externo contacta con el agente interno del móvil y le dice: *"¿Uno de tus host está aquí".* El mensaje del agente externo al agente interno contiene la dirección de red del agente externo. También incluye información de seguridad para convencer al agente interno que realmente el *host* móvil está allí.

4. El agente externo examina la información de seguridad la cual contiene un *timestamp*, para probar que fue generado hace pocos segundos. Si es correcta, le comunica al agente externo que puede continuar.

5. A continuación introduce la información en sus tablas y comunica al host que ha quedado registrado.

Idealmente, cuando un usuario abandona un área, debería anunciarlo para ser eliminado su registro, pero muchos usuarios apagan bruscamente sus computadoras.

Cuando un paquete se envía al usuario móvil, se enruta a la LAN casa del usuario. Los paquetes que se envían al usuario móvil (a su LAN) son interceptados por el agente interno. El agente interno mira donde se encuentra

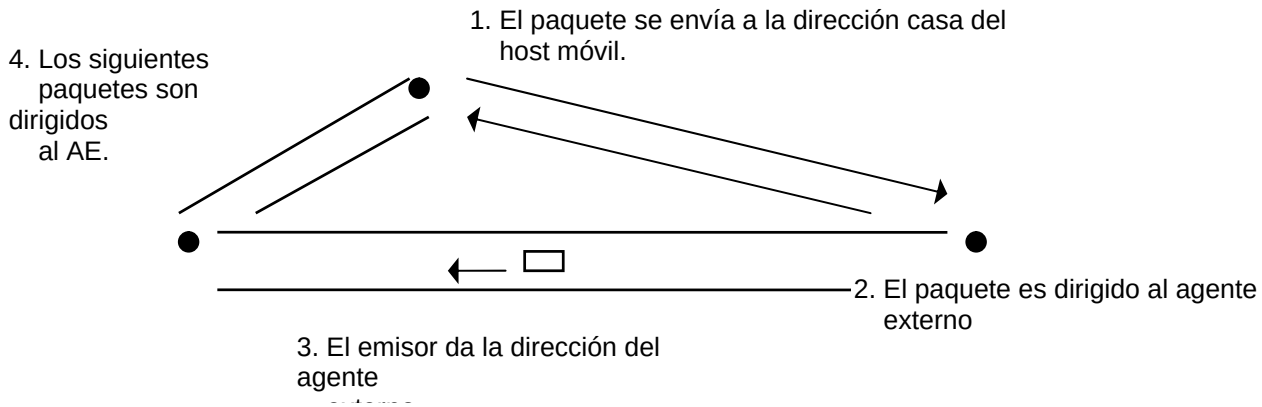
en ese momento el móvil y busca la dirección del agente externo correspondiente. El agente interno hace entonces dos cosas:

1. Encapsula el paquete en el campo *payload* de un paquete de salida y se lo envía al agente externo. Este mecanismo se llama *tunneling*. Después de haber cogido el paquete encapsulado, el agente externo envía el campo payload como una trama de datos.

2. El agente interno dice al emisor que a partir de ese momento envíe paquetes al host móvil encapsulándolos en el *payload* de los paquetes explícitamente dirigidos al agente externo, en vez de enviarlos a la dirección casa.

Los siguientes paquetes ya pueden dirigirse directamente al agente externo.

Figura 5: Ruteo de un paquete en un *host* Móvil




Se han propuesto diferentes esquemas. Primero, está el asunto de protocolos para router y host. Segundo, algunos esquemas para enrutadores registran las direcciones así pueden interceptar y redirigir el tráfico incluso antes

de dar la localización casa. Tercero, en algunos esquemas cada visitante tiene una única dirección temporal, en otras la dirección temporal se refiere a un agente que maneja tráfico para todos los visitantes. Cuarto, los esquemas difieren en cómo ellos manejan el orden de paquetes que son dirigidos a un destino para ser repartidos por uno. Uno elige su cambio de dirección destino y retransmite el paquete modificado. Alternativamente, el paquete, la dirección casa y todo puede encapsularse dentro del paquete *payload* de otro paquete enviando la dirección temporal. Finalmente, hay diferencias en los aspectos de seguridad.

### 3.3.3 Sistema de radiocomunicaciones móviles

Los sistemas de radiocomunicaciones móviles permiten el intercambio de información entre estaciones fijas o móviles (o entre dos móviles) utilizando como medio de transmisión el espectro radioeléctrico. Permiten conectar centros de control públicos o privados y redes telefónicas con personas o vehículos equipados con sistemas de radio.

Cuando el ámbito de aplicación de los sistemas de radiocomunicaciones móviles se centra en el servicio telefónico se habla entonces de servicio de Radiotelefonía Móvil (SRTM).

Actualmente, se está extendiendo el ámbito de utilización de sistemas móviles a servicios no telefónicos como son los de transmisión digital (datos, telemedia, telemando, alarmas).

### 3.3.4 Ip móvil

Muchos usuarios de Internet tienen ordenadores portátiles y quieren quedar conectados a Internet cuando visitan un lugar alejado. Desafortunadamente, el sistema de direccionamiento IP hace que trabajar desde casa sea más fácil de lo que parece.

Una desventaja del esquema de direccionamiento en sí mismo. Cada dirección IP contiene tres campos: la clase, el número de red y el número de *host*. Por ejemplo, en la dirección 160.80.40.20, el 160.80 indica: clase B y dirección de red 8272; el 40.20 es el *host* 10260. Todos los enrutadores del mundo tienen tablas de ruteo diciendo qué línea usar para llegar a la red 160.80.

Si por sorpresa, la máquina destino se apaga mientras está en algún sitio distante, los paquetes continúan enrutándose a su LAN casa (o ruta). El propietario no podrá recibir más correo ni ninguna otra cosa. Que la máquina dé una nueva dirección IP correspondiendo a su nueva localización es una solución poco atractiva debido al gran número de personas, programas y bases de datos que tendrían que ser informados del cambio.

Otra posibilidad es que el router tenga uso completo de direcciones IP para enrutar, en vez de ajustar la clase y la red. Sin embargo, esta estratega requeriría que cada router tuviera millones de entradas en sus tablas.

Cuando la gente comenzó a adquirir host móviles, el grupo de trabajo del IETF encontró una solución. Se formularon un conjunto de reglas consideradas deseables en cualquier solución:

1. Cada host móvil debe ser capaz de usar su dirección IP local en cualquier lugar.
2. No se permite cambiar la dirección de los host fijos.
3. No se permite cambiar el software del router ni sus tablas.
4. La mayoría de paquetes para host móviles no deberían dar rodeos.

La solución elegida es la que se indicó en el apartado anterior. Recordemos que cada lugar que quiera permitir a sus usuarios merodear tiene que crear un agente interno. Cada lugar que quiera permitir visitantes debe tener un agente externo. Cuando un móvil se introduce en un lugar externo contacta con el agente externo que debe registrarlo. El agente externo contacta con el agente interno dándole una *care-of address* normalmente su dirección IP. Cuando un paquete llega a la LAN del usuario, llega a un router de ella. El router intentará localizar al host de forma usual enviando una trama ARP. El agente interno responde dando su dirección Ethernet. El router entonces envía paquetes al agente interno.

Además, lo dirige a la *care-of address* encapsulándolos en el campo de payload de un paquete IP dirigido al agente externo. Entonces el externo los desencapsula y libera metiéndolos en la trama dirigida al *host* móvil. Además, el agente interno da la *care-of address* al transmisor, para que los futuros paquetes puedan ser encauzados directamente al agente externo.

Un pequeño detalle es importante de mencionar. A la vez que el *host* móvil se mueve, el router probablemente tiene su dirección Ethernet fijada. Para reemplazar la dirección Ethernet por la del agente interno, existe un truco llamado *gratuitious ARP*. Eso es un mensaje especial no solicitado al router, que le permite reemplazar una entrada específica, en este caso, la que el *host*

móvil permite. Cuando, más tarde, el *host* móvil regresa, el mismo truco es usado para actualizar la entrada del router.

Nada previene en el diseño que el *host* móvil pueda ser su propio agente externo, pero en la realidad sólo trabaja si el *host* móvil (en su capacidad de agente externo) está conectado a Internet en su sitio común. También, debe ser capaz de adquirir una *care-of address* IP para su uso. Esta dirección IP debe pertenecer a la LAN a la cual comúnmente se conecta.

La solución IETF para *host* móviles resuelve un número de problemas no mencionados. Por ejemplo, ¿cómo se localizan los agentes?. La solución para todos los agentes es hacer periódicamente un broadcast de su dirección y el tipo de servicios que está dispuesto a ofrecer (interno, externo, ambos). Cuando un *host* móvil llegue a algún sitio, puede oír esos broadcasts, llamados *advertisements* (advertencias). Alternativamente, pude mandar un broadcast anunciando su llegada y esperando que el agente externo local le responda.

Otro problema que debe ser resuelto es qué hacer con el *host* móvil que abandona sin decir nada. La solución está en hacer un registro válido sólo por un intervalo de tiempo fijo. Si no es refrescado periódicamente, pasado un tiempo el host externo puede limpiar sus tablas.

Para la seguridad son usados los protocolos de criptografía implementados para este propósito.

# 4 SERVICIOS DE RED

Los servicios de red son un desarrollo creciente. Los sistemas de redes como Internet permiten intercambiar información entre computadoras, y ya se han creado numerosos servicios que aprovechan esta función. Entre ellos figuran los siguientes: conectarse a una computadora desde otro lugar (telnet); transferir ficheros entre una computadora local y una computadora remota (protocolo de transferencia de ficheros, o FTP) y leer e interpretar ficheros de computadoras remotas (gopher). El servicio de Internet más reciente e importante es el protocolo de transferencia de hipertexto (http), un descendiente del servicio de gopher. El http puede leer e interpretar ficheros de una máquina remota: no sólo texto sino imágenes, sonidos o secuencias de video. El http es el protocolo de transferencia de información que forma la base de la colección de información distribuida denominada World Wide Web. Internet permite también intercambiar mensajes de correo electrónico (e-mail); acceso a grupos de noticias y foros de debate y conversaciones en tiempo real (chat, IRC), entre otros servicios.

## 4.1 Redes de datos

Las redes de datos están diseñadas para prestar un conjunto de servicios por medio de los cuales la información fluya de una forma efectiva para con las necesidades del usuario final y con esto provee gran utilidad y funcionamiento.

### 4.1.1 Compartimiento de recursos

El servicio para compartir impresoras y archivos para redes de un sistema operativo de red que permita compartir recursos que permiten montar una red par a par con equipos en los que se encuentre instalado el sistema operativo de red, en donde cada computadora de la red puede actuar tanto como cliente ó como servidor. Actuando como servidor puede compartir carpetas (incluyendo unidades de disco completas) e impresoras. Como cliente podrá acceder a las carpetas (y a los archivos que contienen) y utilizar impresoras conectadas a otros ordenadores, si dichos recursos se encuentran compartidos en esos equipos. Mediante este tipo de sistema es posible compartir otros recursos de la red tales como tarjetas de sonido, módems, escáneres, etc., esto depende del sistema operativo de red que estemos utilizando.

## 4.2 Redes telefónicas

Las redes telefónicas en la actualidad tienen un conjunto de servicios que brindan que con el nacimiento de esta era de tecnología brinda un conjunto de servicios que son íntegros tanto para las redes de datos como para las redes telefónicas.

### 4.2.1 Servicios básicos

Los servicios básicos de telecomunicación se dividen a su vez en dos categorías:

- Servicios portadores.
- Teleservicios.

Los servicios portadores proporcionan la capacidad de transferencia entre terminales conectados a la red local (HPLMN), así como con equipos conectados a otras redes: RTB, RDSI, etc. Abarcan funciones relativas a los tres primeros niveles de la torre OSI, es decir, atributos de bajo nivel (Capacidad baja de capa).

Datos asíncronos, por conmutación de circuitos, a 300, 1.200, 1.200/75, 2.400, 4.800 y 9.600 bit/s.

Datos síncronos, por conmutación de circuitos, a 300, 1.200, 1.200/75, 2.400, 4.800 y 9.600 bit/s.

Acceso asíncrono a PAD a 300, 1.200, 1.200/75, 2.400, 4.800 y 9.600 bit/s.

Acceso síncrono (paquetes) a redes de conmutación de paquetes a 2.400, 4.800 y 9.600 bit/s.

Telefonía alternada con datos.

Los Teleservicios son aquellos servicios de telecomunicación que proporcionan plena capacidad de comunicación entre usuarios o terminales, de acuerdo con protocolos preestablecidos. Así pues, los teleservicios están caracterizados por atributos asociados a los niveles 1-3 de red (Capacidad baja de capa) y a los niveles superiores (Capacidad alta de capa).

### 4.2.2 Servicios telemáticos

Un servicio telemático puede descomponerse en cuatro elementos. Debe incluir uno o varios equipos informáticos: un ordenador o computadora que procesa los datos, un terminal y dispositivos de comunicaciones (como conmutadores, multiplexores y módem) o periféricos (cintas, discos). Además, debe poseer un sistema de comunicación para establecer una conexión entre

estos diferentes equipos. Este sistema puede ser una red pública (nacional o internacional) o una red privada (local o supralocal). Así, un servicio telemático puede emplear tanto la red telefónica o telegráfica como un enlace vía satélite. Todo servicio debe incluir también una fuente de información (bases de datos, ficheros, etc.). Por último, cada servicio telefónico debe contener programas de tratamiento y de transmisión, que constituyen la inteligencia artificial de ese servicio.

### 4.2.3 Servicios de difusión

Los servicios de difusión son aquellos por medio de los cuales se puede transmitir toda la información dependiendo del medio que se este utilizando, ya que como medios de difusión se tiene un conjunto de medios en los cuales se tienen medios tales como la radiodifusión, medios escritos, medios digitales tales como el Internet y medios televisivos, entre otros.

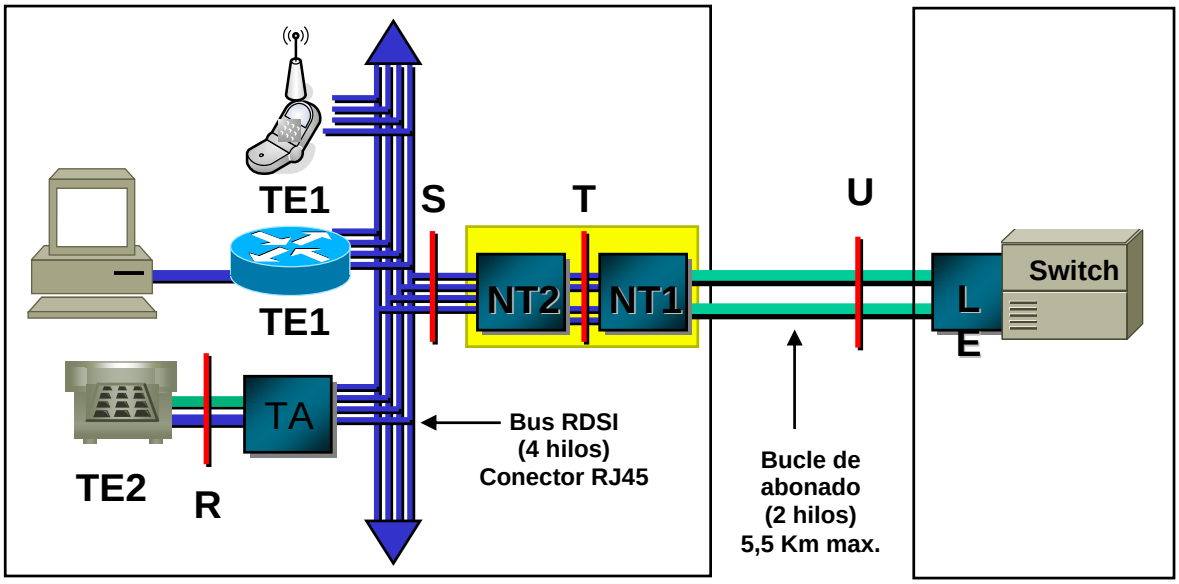
## 4.3 RDSI

Es la evolución de las redes telefónicas actuales. Originalmente, todo el sistema telefónico estaba compuesto por elementos analógicos, y la voz era transportada por las líneas telefónicas modulada como una forma de onda analógica. Posteriormente, aparecieron las centrales digitales, que utilizan computadores y otros sistemas digitales.

Estas son menos propensas a fallos que las centrales analógicas y permiten controlar más líneas de usuarios y realizar las conexiones mucho más rápidamente. En estas centrales la voz se almacena y transmite como información digital, y es procesada por programas informáticos.

La RDSI supone el último avance: la comunicación digital entre el abonado y su central telefónica. Esto supone una comunicación digital de extremo a extremo que conlleva un gran número de ventajas. Así, las recomendaciones de la serie I de la CCITT2 definen la RDSI como una red desarrollada a partir de la red telefónica que proporciona una conexión digital de extremo a extremo que soporta una gran variedad de servicios.

Figura 6. Red digital de servicios integrados




La RDSI ofrece múltiples canales digitales que pueden operar simultáneamente a través de la misma conexión telefónica entre central y usuario; la tecnología digital está en la central del proveedor y en los equipos del usuario, que se comunican ahora con señales digitales. Este esquema permite una transferencia de datos a velocidad mucho mayor. Así, con un servicio de acceso básico, y empleando un protocolo de agregación de canales, se puede alcanzar una velocidad de datos sin comprimir de unos 128 Kbps.

### 4.3.1 Ventajas de la RDSI

La RDSI ofrece gran número de ventajas, entre las que se pueden discutir a continuación:

#### 4.3.1.1 Velocidad

Actualmente el límite de velocidad en las comunicaciones a través de una línea telefónicas empleando señales analógicas entre central y usuario mediante el uso de módems está alrededor a los 56Kbps. En la práctica las velocidades se limitan a unos 45Kbps debido a la calidad de la línea.

La RDSI ofrece múltiples canales digitales que pueden operar simultáneamente a través de la misma conexión telefónica entre central y usuario; la tecnología digital está en la central del proveedor y en los equipos del usuario, que se comunican ahora con señales digitales. Este esquema permite una transferencia de datos a velocidad mucho mayor.

Así, con un servicio de acceso básico, y empleando un protocolo de agregación de canales, se puede alcanzar una velocidad de datos sin comprimir de unos 128 Kbps. Además, el tiempo necesario para es establecer una comunicación en RDSI es cerca de la mitad del tiempo empleado con una línea con señal analógica.

Conexión de múltiples dispositivos. Con líneas analógicas resulta necesario disponer de una línea por cada dispositivo del usuario, si estos se quieren emplear simultáneamente. Resulta muy costoso enviar datos (archivos o vídeo) mientras se mantiene una conversación hablada. Por otra parte, se

requieren diferentes interfaces para emplear diferentes dispositivos al no existir estándares al respecto.

#### 4.3.1.2 Señalización

La forma de realizar un llamada a través de una línea analógica es enviando una señal de tensión que hace sonar la "campana" en el teléfono destino. Esta señal se envía por el mismo canal que las señales analógicas de sonido. Establecer la llamada de esta manera requiere bastante tiempo. Por ejemplo, entre 30 y 60 segundos con la norma V.34 para módems. En una conexión RDSI, la llamada se establece enviando un paquete de datos especial a través de un canal independiente de los canales para datos. Este método de llamada se engloba dentro de una serie de opciones de control de la RDSI conocidas como señalización, y permite establecer la llamada en un par de segundos. Además informa al destinatario del tipo de conexión (voz o datos) y desde que número se ha llamado, y puede ser gestionado fácilmente por equipos inteligentes como una computadora.

#### 4.3.1.3 Servicios

La RDSI no se limita a ofrecer comunicaciones de voz. Ofrece otros muchos servicios, como transmisión de datos informáticos (servicios portadores), télex, facsímil, videoconferencia, conexión a Internet y opciones como llamada en espera, identidad del origen entre otros. Los servicios portadores permiten enviar datos mediante conmutación de circuitos (con un procedimiento de llamada se estable un camino fijo y exclusivo para transmitir lo datos en la red, al estilo de las redes telefónicas clásicas) o mediante conmutación de paquetes (la información a enviar se divide en paquetes de tamaño máximo que son enviados individualmente por la red).

#### 4.3.1.4 Canales y servicios

**a) Canales de transmisión**

La RDSI dispone de distintos tipos de canales para el envío de datos de voz e información y datos de control: los canales tipo B, tipo D y tipo H.

**Canal B:** los canales tipo B transmiten información a 64Kbps4, y se emplean para transportar cualquier tipo de información de los usuarios, bien sean datos de voz o datos informáticos. Estos canales no transportan información de control de la RDSI. Este tipo de canales sirve además como base para cualquier otro tipo de canales de datos de mayor capacidad, que se obtienen por combinación de canales tipo B.

La velocidad de 64Kbps permite enviar datos de voz con calidad telefónica. Considerando que el ancho de banda telefónico es de 4KHz, una señal de esta calidad tendrá componentes espectrales de 4KHz como máximo, y según el teorema de muestreo se requerirá enviar muestras a una frecuencia mínima de $2 \cdot 4KHz = 8KHz = 8000$ muestras por segundo, es decir, se enviará un dato de voz cada 125 seg. Si las muestras o datos de voz son de 8 bits, como es el caso de las líneas telefónicas digitales, se requieren canales de $8 \cdot 8000$ bps = 64Kbps.

**Canal D:** los canales tipo D se utilizan principalmente para enviar información de control de la RDSI, como es el caso de los datos necesarios para establecer una llamada o para colgar. Por ello también se conoce un canal D como "canal de señalización". Los canales D también pueden transportar datos cuando no se utilizan para control. Estos canales trabajan a 16Kbps o 64kbps según el tipo de servicio contratado.

**Canales H:** combinando varios canales B se obtienen canales tipo H, que también son canales para transportar solo datos de usuario, pero a velocidades mayores. Por ello, se emplean para información como audio de alta calidad o vídeo. Hay varios tipos de canales H entre ellos los siguientes:

- Canales H0, que trabajan a 384Kbps (6 canales B).
- Canales H10, que trabajan a 1472Kbps (23 canales B).
- Canales H11, que trabajan a 1536Kbps (24 canales B).
- Canales H12, que trabajan a 1920Kbps (30 canales B).

## 4.4 SONET

Tecnología de la capa física diseñada para proporcionar una transmisión universal y los multiplexores forman planos, con proporciones en la transmisión del Gigabit por segundo funcionamiento sofisticado y sistemas de dirección. Esta tecnología es regularizada por las normas nacionales americanas instituya (ANSI) T1 comité. Una tecnología parecida es el SDH, es regularizada por la unión de las telecomunicaciones internacionales (ITU) y es muy similar a SONET solo que su jerarquía del multiplexado es una jerarquía de SONET.

## 4.5 SDH

Es un conjunto de estándares internacionales para transmisiones digitales sincronas por fibra óptica, publicado por CCITT en 1989, considerado por algunos como una variante de SONET y por otros como un conjunto que abarca a SONET.

La principal razón para la creación de SDH fue proporcionar una solución a largo plazo para estandarizar los accesos a redes entre proveedores, es decir, permitir que equipos de diferentes proveedores puedan comunicarse entre sí.

Esta capacidad se refiere a la intercomunicación entre equipos de múltiples proveedores permitiendo a un elemento de la red SDH comunicarse con otro, así como la sustitución de varios de ellos que pudieran haber sido utilizados previamente sólo para propósitos de interface. La segunda ventaja del SDH es que es síncrono. En la actualidad, la mayoría de los sistemas de multiplexado son plesiócronos. Es decir, no existe un reloj de red al que se encuentren sincronizados todos los elementos.

## 4.6 ADSL

Es una tecnología para módems, convierte el par de cobre que va desde la central telefónica hasta el usuario en un medio para la transmisión de aplicaciones multimedia, transformando una red creada para transmitir voz en otra útil para cualquier tipo de información, sin necesidad de tener que reemplazar los cables existentes, lo que supone un beneficio considerable para los operadores, propietarios de los mismos.

ADSL (estándar ANSI T1.413) proporciona un acceso asimétrico y de alta velocidad a través del par de cobre que los usuarios tienen actualmente en su casa u oficina, para la conexión a la red telefónica. Sus principales aplicaciones son la comunicación de datos a alta velocidad (por ejemplo, para acceso a Internet, remoto a LANs y teletrabajo) y el vídeo bajo demanda. Frente a los módems de cable ADSL ofrece la ventaja de que es un servicio dedicado para cada usuario, con lo que la calidad del servicio es constante, mientras que con los otros módems se consigue velocidades de hasta 30 Mbit/s pero la línea se comparte entre todos los usuarios, degradándose el servicio conforme más de estos se van conectando o el tráfico aumenta.

Muchas de las aplicaciones sobre ADSL incorporaran vídeo digital comprimido, que al ser una aplicación en tiempo real no tolera los procedimientos de control y corrección de errores propios de la redes de datos, por lo que los propios módems incorporan técnicas de corrección de errores FEC (Forward Error Correction) que reducen en gran medida el efecto provocado por el ruido impulsivo en la línea, aunque introduce algún retardo.

## 4.7 Servicios combinados entre redes de datos y redes telefónicas en Guatemala

Los servicios que se prestan de las redes telefónicas hacia las redes de datos en Guatemala están categorizados como un conjunto de servicios que la infraestructura que poseen las compañías telefónicas guatemaltecas tiene a disposición de los usuarios. Además, es importante mencionar que ya con la infraestructura existente y la tecnologías en uso tal como lo representan las tecnologías gsm y cdma que poseen las compañías en Guatemala se puede brindar un conjunto de servicios que aún no prestan, pero que debido a que se considera que hasta que no creen la demanda necesaria para el uso de algunos servicios no lo pondrán a funcionar, tal es el caso de la personalización de avisos de noticias sociales.

### 4.7.1 Videotexto

La palabra videotexto es un término genérico utilizado para designar un tipo de servicios de difusión de la información, distribuidas mediante el teléfono y el televisor doméstico. La información se codifica en clave en el sistema en páginas discretas, pudiendo recuperarse y leerse a continuación empleando un receptor doméstico de televisión modificado. El videotexto propiamente dicho se transmite por teléfono, de modo que el usuario ha de marcar el número del

sistema, pero el número de páginas disponibles es, en principio, ilimitado y puede obtenerse mediante páginas indexadas de modo prácticamente interactivo, lo cual permite localizar y mostrar con bastante rapidez las páginas de información solicitadas. A través de él se puede acceder a las bases de datos de forma interactiva utilizando el televisor, un microordenador y el cable telefónico.

En ambos casos, la información es muy variada y no especializada: está pensada para uso del gran público. Los sistemas de videotexto y teletexto ofrecen información general, comunicaciones, transacciones, servicios de telemando y telecontrol y programas de ordenador. Su función en las bibliotecas puede ser múltiple, siempre dependiendo del uso y la orientación que se le dé en un futuro; actualmente, su papel más habitual es el de acercar la biblioteca pública al usuario. Ofrece las ventajas de la rapidez, exactitud y selectividad de la información.

### 4.7.2 Teletexto

Se difunde por radio y suele limitarse a unos cuantos centenares de páginas de información que se emiten en secuencias, por lo que el usuario ha de esperar un poco para obtener la página solicitada. No es interactivo y se utiliza la pantalla del televisor para su recuperación. Es un sistema de videografía que permite la presentación de textos informativos (de actualidad, servicios, ocio, programas de televisión, etc) en el televisor, así la subtitulación de programas. El usuario puede consultar, a su voluntad, distintos apartados y páginas de información.

### 4.7.3 Correo electrónico

El correo electrónico ("E-Mail" o "Electronic Mail" en inglés) es el segundo servicio más usado de la red Internet (el primero es la navegación por la world wide web). Dos personas que tengan acceso a una cuenta de correo en Internet pueden enviarse mensajes escritos desde cualquier parte del mundo a una gran velocidad. Lo normal es que un mensaje tarde entre unos pocos segundos y unos pocos minutos, dependiendo de la cantidad de texto que se envíe. Hoy en día los mensajes de las cuentas de correo pueden ser accedidos desde el propio teléfono celular (esto aplica cuando las compañías de teléfono soportan este tipo de servicio actualmente en Guatemala solamente comcel brinda este tipo de servicio).

### 4.7.4 Internet

Es una red de alcance mundial que une una gran cantidad de redes grandes de computadoras. Esto afecta al usuario de Internet, puesto que le permite contactar con gente y ordenadores de todo el mundo desde su propia casa. Internet funciona con la estrategia "Cliente/Servidor", lo que significa que en la red hay ordenadores servidores que dan una información concreta en el momento que se solicite y, por otro lado, están los ordenadores que piden dicha información, los llamados Clientes.

Existe una gran variedad de lenguajes que usan los ordenadores para comunicarse por Internet. Estos lenguajes se llaman protocolos. Se ha establecido que en Internet, toda la información ha de ser transmitida mediante el protocolo TCP/IP.

Es necesario establecer que para que desde un teléfono se pueda acceder a Internet es necesario que exista el servicio, por parte de la compañía telefónica por una parte ya que por otra es necesario de que el teléfono cuente con el software necesario para poder navegar hacia Internet.

# 5. SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN

## 5.1. Asuntos de seguridad

En lo referente a este tipo de aspectos es muy considerable en la transmisión de información de un tipo de red como lo son las redes celulares hacia una red de datos y con esto existen un conjunto de métricas que se derivan tanto de factores sociales como de otros factores que siempre han acosado al intercambio de información tal y como lo representan las personas que se dedican al robo de información.

Los teléfonos celulares son totalmente inseguros. Cualquiera que tenga un receptor de radio a toda banda puede sintonizar y oír cualquier cosa emitida en una celda. Como la mayoría de los usuarios no se da cuenta de lo inseguro que es este sistema, a menudo dan números de tarjetas de crédito y otras informaciones confidenciales. Otro problema es el robo del "tiempo de aire". Con un receptor a toda banda añadida al ordenador, un ladrón puede monitorizar el canal de control y registrar los 32 bits serie de un número y los 34 de un número de teléfono de todos los teléfonos móviles que oiga.

Solamente con conducir alrededor de un par de horas por la ciudad puede construirse una gran base de datos. El ladrón puede entonces escoger un número y usarlo para sus llamadas. Esta trampa podrá usarse hasta que la víctima reciba un recibo semanas más tarde.

Algunos ladrones ofrecen un servicio de telefonía a bajo costo al hacer llamadas por sus clientes usando los números robados. Otros reprograman teléfonos con los números robados y los venden como teléfonos en los que

puede llamarse libremente. Algunos de estos problemas podrían resolverse por encriptación, pero entonces la policía no podría realizar "wiretaps" con criminales inalámbricos. Otro asunto en el área general de la seguridad es el vandalismo y daño a antenas y estaciones base. Todos estos problemas son graves y cuestan cientos de millones de dólares al año en pérdidas a la industria celular.

## 5.2. Criptografía

La criptografía responde a la necesidad de codificar mensajes que sólo pueda descifrar el destinatario y se ha aplicado tanto a defensa, como a secretos industriales y en los últimos años, sobre todo, al comercio electrónico. Esto es así porque actualmente la seguridad de los sistemas informáticos se ve debilitada por el fuerte crecimiento de las redes y cuando se trata este tema hay que tener en cuenta un aspecto tan importante como la privacidad e integridad de los datos.

### 5.2.1. Concepto de criptografía

Ciencia que trata del enmascaramiento de la comunicación de modo que sólo resulte inteligible para la persona que posee la clave, o método para averiguar el significado oculto, mediante el criptoanálisis de un texto aparentemente incoherente. En su sentido más amplio, la criptografía abarca el uso de mensajes encubiertos, códigos y cifras. Los mensajes encubiertos, como los ocultos en textos infantiles o los escritos con tinta invisible, cifran todo su éxito en no levantar ninguna sospecha; una vez descubiertos, a menudo no resultan difíciles de descifrar. Los códigos, en que las palabras y las frases se representan mediante vocablos, números o símbolos preestablecidos, por lo

general resultan imposibles de leer si no se dispone del libro con el código clave.

### 5.2.2. Ventajas y uso de la criptografía

El uso de la criptografía es algo que en la actualidad en las comunicaciones es un medio muy común ya que es una forma por medio de la cual se transmite la información de un medio hacia otro en forma aparentemente segura o que por lo menos si es interceptada no puede ser accedida por terceros que son ajenos a los mensajes que fluyen por la red ya sea telefónica celular ó una red de datos mundial como lo es Internet por lo que el uso de la codificación de los mensajes es una buena opción para la transmisión de la información y que para el uso que los interesados lo utilizan es una ventaja ya que existen transacciones que se realizan por la red y que por el tipo de transacción debe de representar algo confiable para las personas que usan de servicios en los cuales la confidencialidad es un factor muy importante y que los medios de encriptamiento representan un uso considerable.

### 5.2.3. Algoritmos de encriptamiento para las redes de datos

A través del tiempo, se ha presentado la necesidad de transmitir mensajes de una manera en la cual sólo la persona correcta pueda entenderlos, la criptografía llena esta necesidad, a través de sus diversos algoritmos matemáticos es necesario indicar que estos tipos de algoritmos no solamente funcionan para redes de datos también funcionan para otros entornos pero el uso de los mismos sobre las redes de datos los han hecho muy populares sobre el entorno de las redes de datos.

#### 5.2.3.1. Algoritmos simétricos

Los algoritmos simétricos consisten en encriptar el mensaje que se desea enviar con una clave, la misma clave será utilizada para desencriptarlo. Es el tipo de criptografía más conocido. En la práctica, suele ser muy rápido, y por esta característica, es todavía ampliamente utilizado en el mundo de la computación. La gran desventaja de este método es que la clave debe transmitirse por un canal seguro, ya que todo el que posea la clave podrá desencriptar y entender el mensaje. El problema radica en la comunicación de esta clave a la otra persona cuando el contacto entre las personas es imposible.

#### 5.2.3.2. Algoritmos asimétricos

Los algoritmos asimétricos obtiene su nombre del hecho de que existen dos claves distintas, si un mensaje es encriptado con una de las claves, sólo la otra clave podrá desencriptar y viceversa. Se soluciona entonces el problema de la comunicación segura de la clave secreta de la siguiente manera: se generan las dos claves. Se designa una de las claves como "clave pública" y se difunde tan libremente como se desee sin ningún tipo de riesgo.

La otra clave se resguarda tan bien como se pueda, toda la seguridad del proceso depende de esta clave, esta debe ser absolutamente secreta. Para recibir un mensaje, se envía la clave pública al emisor (o este la busca en algún sitio: página web, directorio de claves, etc.), el mensaje es encriptado con esa clave pública y es enviado al receptor. El receptor desencripta el mensaje con su clave privada (que es la única clave que puede hacerlo). Las dos claves de este sistema están relacionadas matemáticamente, sin embargo, no es posible obtener una a partir de la otra.

### 5.2.4. Algoritmos de encriptamiento para las redes telefónicas

La disposición de cada uno de los elementos presentes en una comunicación digital tiene una función muy concreta. El elemento de encriptamiento, como su nombre indica, sirve para hacer ininteligible la información que va por el canal a cualquier persona que lo escuche, y que no sea el interlocutor al que va dirigida la comunicación, y que por supuesto no conozca la clave. Posteriormente, la codificación de canal da fiabilidad al mismo añadiendo una cierta redundancia y, por último, en el transmisor se efectuarán las oportunas operaciones, con el fin de adaptar la señal lo mejor posible al medio por el que será transmitida.

a) **Codificación de la información.** Para los sistemas telefónicos el proceso de codificación es algo muy importante y que en sistemas tales como cdma y gsm lo implementan. La meta de seguridad en los sistemas de comunicación celular, es proveer seguridad para las conversaciones y datos de intercepciones, así como de prever fraudes telefónicos. Para ello hacen uso de algoritmos tales como el A3, A5 y A8 entre otros para poder proveer datos sobre la red en forma segura.

b) **Algoritmo A3.** Es el algoritmo de autenticación. Es el que hace que cada teléfono móvil sea único. Permite, entre otras cosas, saber a quién hay que cobrar la llamada.

c) **Algoritmo A5.** Es el algoritmo de cifrado de voz. Gracias a él, la conversación va encriptada. Se trata de un algoritmo de flujo (stream cipher) con una clave de 64 bits. Hay dos versiones, denominadas A5/1 y A5/2; esta última es la versión autorizada para la exportación, y en consecuencia resulta más fácil de atacar.

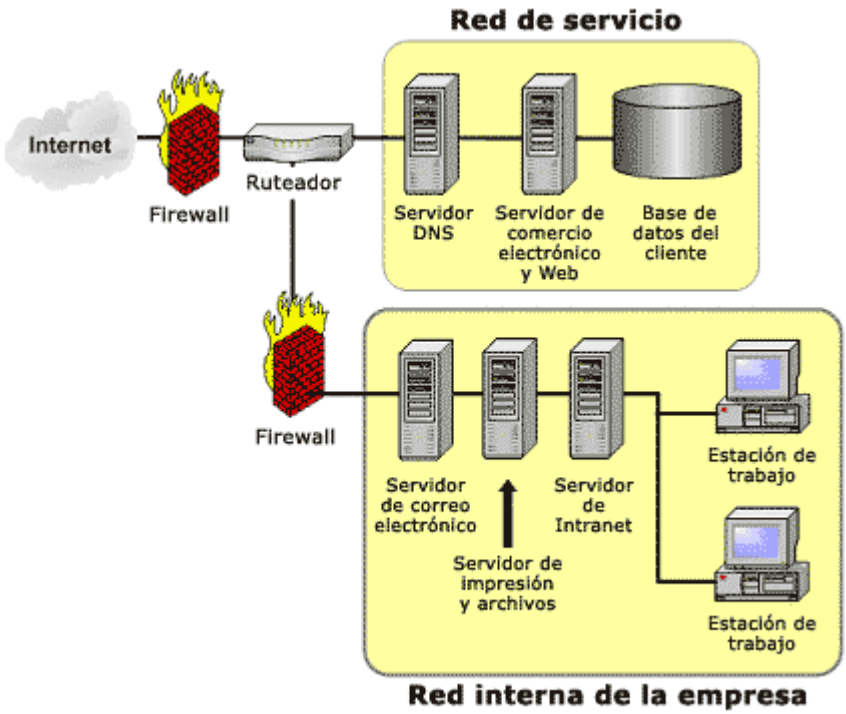
**d) Algoritmo A8.** Es el algoritmo que genera claves tanto para autenticación (A3) como para encriptación (A5). Básicamente, se trata de una función unidireccional parecida a las funciones "hash" (tipo MD5 o SHA-1) que permiten la firma digital en los documentos electrónicos.

## 5.3. Diseño de la seguridad de la red

### *5.3.1. Firewall*

Un *Firewall* en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El *firewall* determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un *firewall* sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El *firewall* podrá únicamente autorizar el paso del tráfico y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este. Este tipo de mecanismo lo podemos observar en la figura 7.

Figura 7. *Firewall* en la red de una empresa




### 5.3.2. Estrategias para proteger las conexiones

En la actualidad, las empresas interesadas en la transmisión de la información toman en cuenta con mayor regularidad la un conjunto de estrategias para la protección de sus conexiones, para transmitir datos esto para que la información que se transmite de un lugar hacia otro aunque sea por medio de un canal que no solo está dedicado hacia una empresa particular no vaya a ser interferido por un tercero y esto para que la información sea privada y que no sea pública para todos y con ello existen un conjunto de estrategias que sirven para proteger las conexiones, esto se realiza en su mayoría por medio de la encriptación de la información en sus diversas formas ya sea por algoritmos simétricos o asimétricos en los datos y en canales de comunicación por voz por mecanismos como el gsm que también usan de la encriptación para

proteger la conexión o enlace de la información para que de esta forma los mensajes transmitidos por algún medio publico tal como Internet sea seguro.

### 5.3.3. Importancia en la seguridad de la información

La información como tal tiene la importancia que cada quien le proporcione ya que para algunos puede ser una prioridad con un mayor nivel que para otros. Es muy importante indicar que teniendo el nivel establecido en importancia de la protección de la información establezcamos un conjunto de políticas de seguridad las cuales vamos aplicar para que la información que manejamos este segura.

Regularmente la seguridad de la información va asociada a la integridad que debe de poseer los datos que transmitimos por cualquier medio ya que de ninguna forma queremos tener información adulterada y por ello se debe de tener un mecanismo responsable de esto ya que para poder corresponder a la seguridad e integridad de la información de mecanismos tales como lo conforman las redes celulares y las redes de datos es recomendable establecer dentro de las políticas de la seguridad de la información capas de seguridad de la misma ya que si queremos transmitir información de una red celular hacia una red de datos debemos de establecer capas por medio de las cuales hacemos compatibles redes que aunque en comportamiento son similares en estructura divergen.

### 5.3.4. Gestión de seguridad celular

La autentificación de los usuarios que utilizan el sistema celular se realiza pidiendo al terminal el resultado de un cálculo específico sobre un número aleatorio (RAND) que envía el sistema y comprobando después este resultado con el correcto.

Este proceso de cálculo depende de hecho de una clave secreta (Ki) que es específica para cada tarjeta SIM de cada abonado. El cálculo se hace siguiendo un algoritmo de cifrado A3, que tiene la propiedad de que conociendo el resultado y una entrada (RAND), no puede deducirse prácticamente la otra entrada (Ki). La clave secreta (Ki) y el algoritmo A3 se almacenan, con protección, en la tarjeta SIM y en el HLR.

El cifrado de la ráfaga de datos se logra con un segundo algoritmo de cifrado A5, que se aplica a una clave (Kc) que se escoge para cada conexión y aun número que cambia en cada ráfaga.

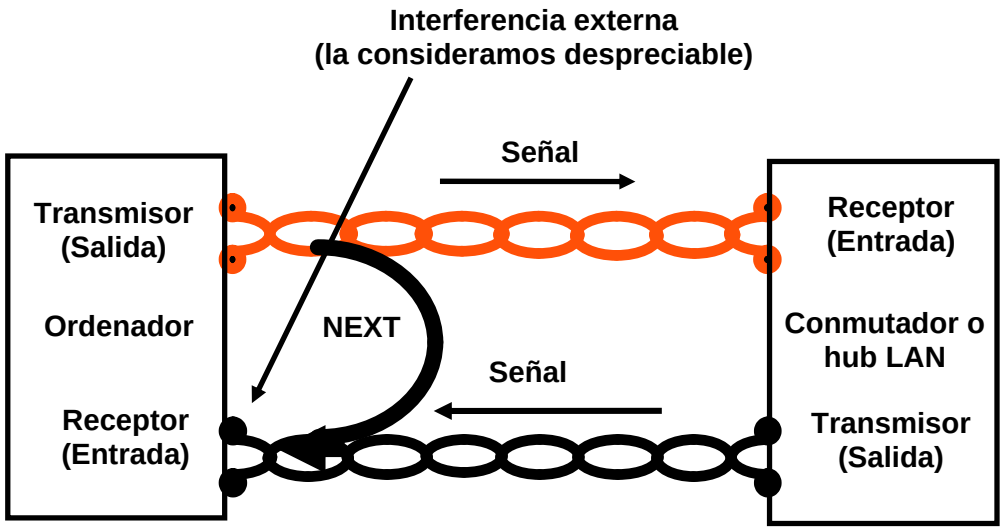
La clave Kc se calcula en el terminal y en el HLR con un tercer algoritmo A8, similar al A3. Los algoritmos A3 y A8 no se especifican en las recomendaciones del GSM, sino que se dejan a la elección del operador.

## 5.4. Vulnerabilidad de las comunicaciones

Las formas por medio de las cuales se llevan a cabo las comunicaciones en muchas ocasiones se ven afectadas por fenómenos que hacen vulnerables a la forma por medio de la cual nos comunicamos, entre estos fenómenos que nos afectan encontramos a la interferencia la cual es considerada como un tipo de degradación de la señal deseada que es causada por otras transmisiones

que operan a la misma frecuencia, o por lo menos, muy cercanas. Y el ruido el cual es considerado como una fluctuación aleatoria de voltaje que obstaculiza la recepción normal de la señal recibida y no es controlable por el hombre. Con lo cual las comunicaciones se ven directamente afectadas por ambos fenómenos. En la figura 8 podemos observar como afecta el ruido a la señal de las comunicaciones.

Figura 8. Forma de interferencia señal /ruido




### 5.4.1. Fuentes de ruido

Un fenómeno que afecta a las comunicaciones son las fuentes de ruido el cual es considerado como la interferencia o señal presente en un sistema de comunicaciones, distinta de la señal transmitida, que disminuye la inteligibilidad o la correcta recepción de la misma. Dependiendo del enfoque que se le dé se ha categorizado al ruido en niveles detallistas que explican toda la teoría del mismo. Aquí será tratado de tres formas distintas las cuales son:

- ruido térmico
- ruido de choque
- ruido atmosférico

**a) Ruido térmico.** Todos los objetos cuya temperatura esta por encima del cero absoluto (0 grados Kelvin) generan ruido eléctrico en forma aleatoria debido a la vibración de las moléculas dentro del objeto. Este ruido es llamado ruido térmico. La potencia de ruido generada depende solo de la temperatura del objeto, y no de su composición. Ya que esta es una propiedad fundamental, el ruido frecuentemente definido por su temperatura equivalente de ruido. La temperatura de ruido puede darse tanto en grados Kelvin como en decibeles. La temperatura del aire alrededor de nosotros es aproximadamente 300 K (27C), y la temperatura del sol es muy alta (alrededor de 5,700 K).

**b) Ruido de choque.** Los diodos limitados por la temperatura, los cuales virtualmente incluye a todos los semiconductores, generan ruido de choque cuando la corriente es pasada a través del diodo. El ruido resultante es debido por la corriente que es pasada por en forma de partículas discretas (electrones) y un impulso es generado por el paso de cada partícula. El ruido es proporcional a la corriente. La corriente cero es igual al ruido térmico.

**c) Ruido atmosférico.** Existe un ruido que es interceptado por la antena llamado ruido atmosférico. El ruido atmosférico es muy alto para bajas frecuencias, y decrece cuando se incrementa la frecuencia. Esta presente en toda la banda de radiodifusión AM y éste no puede ser eliminado con el amplificador y el diseño de la antena. El ruido atmosférico decrece bastante en frecuencias de TV y FM.

### 5.4.2. Fuentes de interferencia

La interferencia como tal se considera como un efecto que se produce cuando dos o más ondas se solapan o entrecruzan. Cuando las ondas interfieren entre sí, la amplitud (intensidad o tamaño) de la onda resultante depende de las frecuencias, fases relativas (posiciones relativas de crestas y valles) y amplitudes de las ondas iniciales. Se puede catalogar a las fuentes de interferencia desde mecanismos tales como la luz por ondas electromagnéticas que pueden interferir entre sí. Así como las ondas de radio interfieren entre sí cuando rebotan en los edificios de las ciudades, con lo que la señal se distorsiona. Arrojando objetos al agua estancada se puede observar la interferencia de ondas de agua, que es constructiva en algunos puntos y destructiva en otros. Otros ejemplos que podemos indicar como fuentes de interferencia a continuación:

- Sistema de encendido de vehículos,
- Motores eléctricos, líneas de alta tensión,
- Luces de neón y fluorescentes
- Computadoras.

Otros tipos de transmisión, tales como la radio amateur, CB (Banda Civil), radio de la policía y otros servicios públicos, inclusive otras estaciones de FM o TV.

## 5.5. Aspectos principales de interferencia de las comunicaciones inalámbricas en la ciudad de Guatemala

Las comunicaciones inalámbricas y específicamente a los que engloba a las telecomunicaciones se basan sobre la transmisión de la señal de radio. Esta

es afectada por el ruido y la interferencia, el ruido es considerado como el resultado de los procesos aleatorios que producen energía de radiofrecuencia. La relación entre el nivel de la señal y el nivel de ruido es la relación señal a ruido (RSR) ó la relación entre la portadora y el ruido, P/R. Está última es la medida más básica de la calidad de la señal. Por, su parte la interferencia es una forma de degradación de la señal producida por otras emisiones de radio.

Existen dos tipos de interferencia, la primera la de canal adyacente, que ocurre cuando la energía de una portadora está presente en un canal adyacente y la de co-canales, la cual ocurre cuando dos transmisiones en la misma frecuencia de portadora llegan a un receptor. El interés de la transmisión de información por medio del espectro de señal radio digital es la reducción y simplificación de todas las fuentes de degradación de las características de la señal de radio digital, dicho de otra forma, la disminución de la ocurrencia de errores durante la transmisión de las señales digitales, lo cual es definido como el rango de error de los bits (BER).

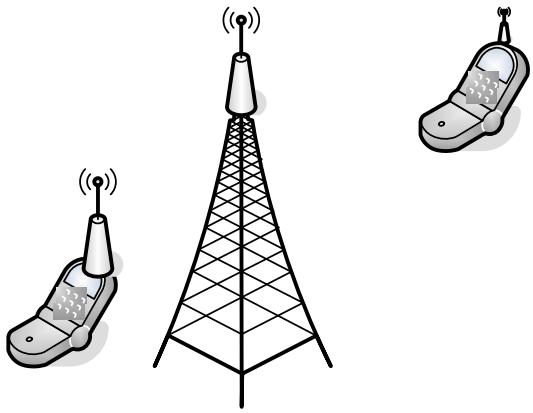
**Pérdidas en el espacio**: este es un aspecto de la propagación de la onda de radio el cual determina la calidad de la transmisión. A lo largo de su trayectoria, la señal es expuesta a una serie de obstáculos que pueden impedir que alcance su receptor probable, una falta del enlace de radio durante algunos milisegundos puede producir una degradación notable del canal de comunicaciones. Estos obstáculos son de tres tipos principalmente:

a) **Espacio libre:** en el caso más simple, transmisor omnidireccional, la potencia recibida de la señal disminuye cuando el receptor se aleja del transmisor. En el vacío, “espacio libre”, la intensidad de la señal disminuirá en forma inversa y proporcional al cuadrado de la distancia. En otras palabras, si la señal recibida a un kilómetro de distancia del

transmisor es de 1 Watt. Esta misma señal será de un cuarto de Watt a 2 kilómetros. En la práctica debido a que las telecomunicaciones móviles no se realizan en el espacio libre las pérdidas de la trayectoria son más severas de lo que prevé este teorema debido a que en la realidad este teorema refleja los efectos del terreno, la atmósfera y otros elementos de la tierra. Estas pérdidas también son altamente dependientes de la frecuencia.

Hay que notar que el análisis de la propagación de las ondas de radio es todavía un campo empírico, especialmente en el caso de las nuevas aplicaciones, los servicios de transferencia de datos desde los móviles y las nuevas frecuencias elevadas.

Figura 9. Disminución de la señal por la distancia

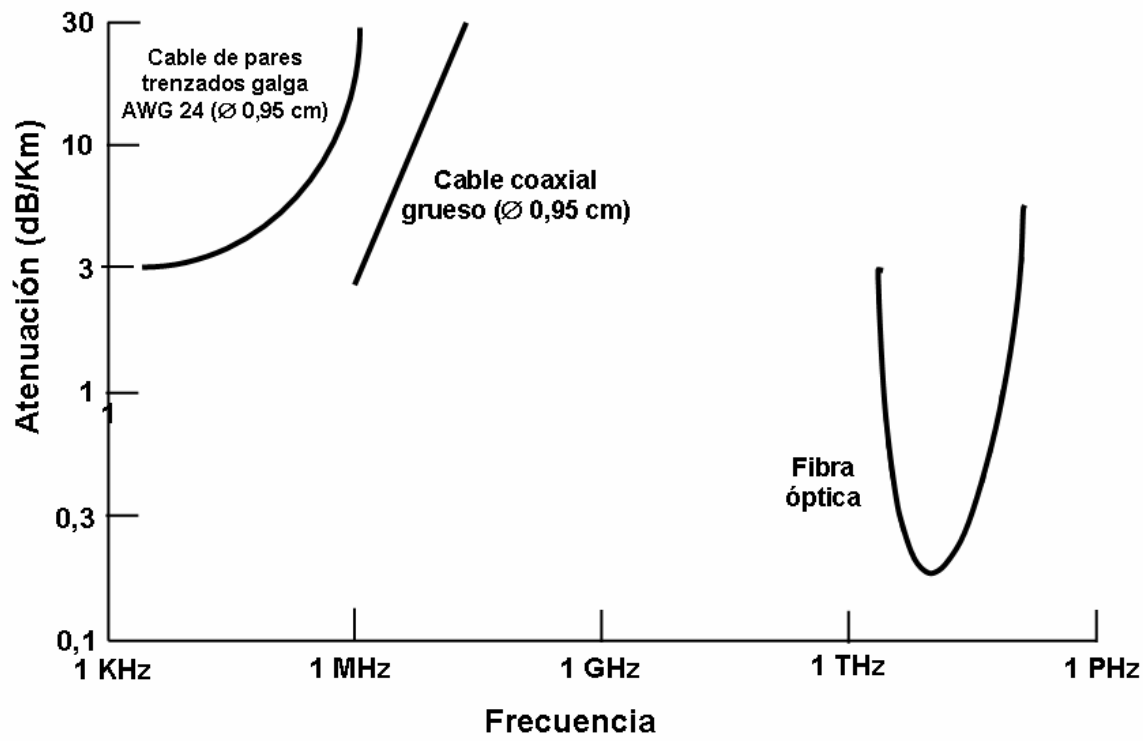


b) **Atenuación:** debido a los efectos de esta, las ondas de radio pueden ser parcial o totalmente bloqueadas cuando su energía es absorbida o bloqueada por obstáculos físicos del medio ambiente. En nuestro medio el elemento de absorción puede ser la lluvia, el follaje de los árboles, una montaña, un volcán, entre otros. La causa específica de la severidad de la atenuación depende principalmente de la frecuencia, por ejemplo las

ondas electromagnéticas de 1 GHz no son afectadas relativamente por la lluvia, por el contrario, las ondas superiores a los 10 GHz son normalmente afectadas. Cuanto más elevada sea la frecuencia mayor será la atenuación, por esta razón, para obtener el mismo nivel de calidad de una señal recibida, es necesaria una potencia de transmisión más elevada.

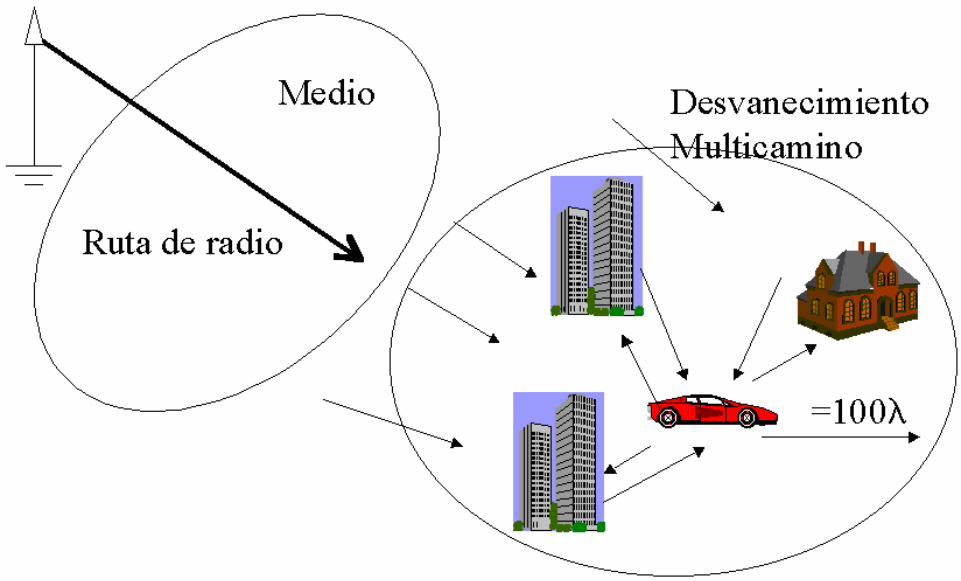
Otros efectos importantes de la atenuación de las ondas de radio, sobre todo en las zonas urbanas, son las múltiples reflexiones y la atenuación debido al follaje de los árboles, lo que lleva a la creación del efecto fantasma. En la figura 10 observamos el efecto que posee la atenuación con diferentes medios de transmisión a diferentes frecuencias.

Figura 10. Atenuación versus frecuencia



c) **Desvanecimiento**: debido a que una onda de radio también puede ser reflejada por cualquier objeto en la atmósfera, una montaña, un edificio, un aeroplano, etc. Estas reflexiones producirán necesariamente diferentes trayectorias creando uno de los problemas más difíciles en la transmisión de la radio. La dispersión por retardo (propagación de la señal por diferentes trayectorias), produce que la señal viaje por múltiples trayectorias, las cuales llegan con una diferencia en el tiempo, produciendo una deformación por retardo. Otro efecto importante presente en las aplicaciones móviles, es el desfasamiento Doppler (el movimiento de un receptor con respecto a un transmisor produce un desfasamiento Doppler); cuando un transmisor móvil envía una frecuencia a un receptor inmóvil, el receptor observará una señal ligeramente superior a la transmitida, en el caso contrario será una frecuencia ligeramente inferior. Para visualizar gráficamente este tipo de interferencia vamos a observar la figura 11 las flechas representan las ondas en el espacio.

Figura 11. Desvanecimiento de onda de la señal




Cuando las ondas multicamino rebotan en los edificios y casas forman muchos pares de ondas en el espacio. Estos pares de ondas son sumadas y se convierten en una estructura de desvanecimiento de onda.

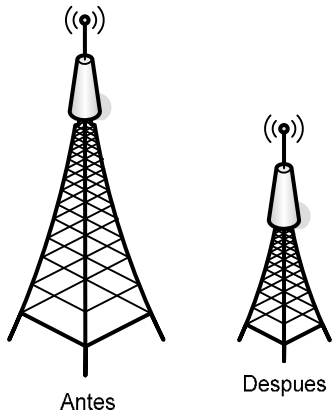
### 5.5.1. Tipos de interferencia en sistemas analógicos de telefonía móvil celular en la transmisión de datos

En sistemas de telefonía celular con rehuso de frecuencias, la interferencia es inevitable. Algunos equipos mal diseñados permiten la interferencia pero a la vez se les ha incorporado elaboradas medidas que contrarresten sus efectos en éste ambiente de radiocomunicación. Los síntomas de interferencia van desde la caída y bloqueo de llamadas hasta el cruce de conversaciones. Para el usuario, el efecto de la interferencia puede significar bloqueo al acceso del sistema, ruido, o hasta voz ilegible, esto es muy

parecido al cruce de conversaciones en una red de líneas fijas. El diseñador del sistema de telefonía celular debe estar consciente de la naturaleza, causas y control de interferencia para alcanzar un efectivo rehuso de frecuencias. La mayoría de las grandes ciudades tienen problemas de interferencia, ésta es la mayor causa de insatisfacción de los usuarios y que contribuye a aumentar el costo de los sistemas, ya que los canales bloqueados no pueden usarse para el servicio. Fuera de los períodos pico, la interferencia no es problema, ya que en estos períodos de operación es cuando más afecta al sistema, limitando así su capacidad, durante estos períodos de mayor ocupación es cuando más capacidad se necesita y la interferencia la limita. Más o menos la mitad de la interferencia se debe a equipo mal calibrado, la otra mitad es inevitable por las características intrínsecas de los sistemas de radio celular.

En la mayoría de las grandes ciudades del mundo es evidente el mal diseño de ubicación de sitios, las antenas celulares se colocan en lugares muy altos, en torres en astas y comisas de edificios, donde todo es muy obvio, no existe una buena ubicación de estos equipos. Entre las medidas utilizadas para contrarrestar esta mala ubicación de sitios está el uso excesivo de downtilt (inclinación hacia abajo) en las antenas, lo que las hace ver deformadas. Una de las formas más efectiva para reducir la interferencia es bajando de altura las antenas en la torre.

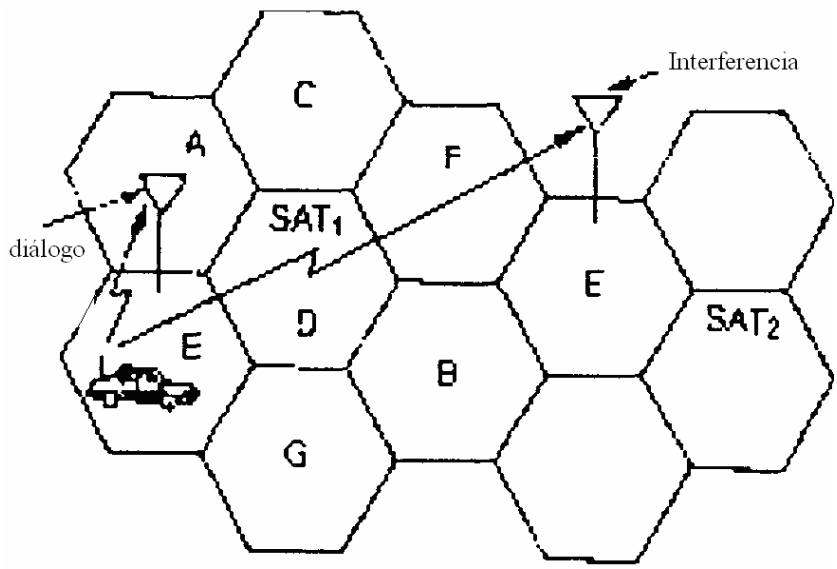
Figura 12. Reducción del tamaño de antenas




Esta técnica, puede reducir la interferencia pero conduce a la pérdida de cobertura en el área de servicio, pues el downtilt la reduce. Donde hay rehuso de frecuencias es prioritario colocar lo más bajo posible las antenas, tanto como lo permitan las condiciones geográficas del terreno.

**Interferencia por rehuso de frecuencia:** la interferencia puede ocurrir de muchas maneras, pero la interferencia más significativa en la telefonía celular es la producida desde una unidad móvil (teléfono celular) hacia una celda distante que tenga operando un canal con la misma frecuencia. La figura 13 muestra ésta forma de interferencia, que no suele ser notada por el usuario, pero puede bloquear temporalmente el canal que está siendo interferido, causando interferencia audible por algunos momentos.

Figura 13. Interferencia de un móvil




En los sistemas AMPS y TACS las celdas adyacentes son proveídas con SAT (Supervisor de tonos de audio) diferente, con tonos de alrededor de 6 Khz, que se utilizan para identificar señales portadoras extrañas. Estos tonos minimizan la probabilidad de tomar decisiones erróneas al controlar la interferencia por co-canal o canal adyacente. Normalmente, se asume que la interferencia es un problema entre la portadora y el canal interferido, el valor es proporcional a 18 dB o menos en sistemas analógicos. En ambientes de poca multitrayectoria (uso de aparatos de mano estacionarios) se transforma en un problema de bajo nivel, específicamente en los sistemas de alta desviación, este valor de 18 dB permite un funcionamiento exitoso aunque el ambiente sea de severa interferencia.

Para evitar los problemas de interferencia en lo sistemas AMPS, se utiliza un sistema de detección de códigos de SAT externos (esto implica también a las portadoras de los teléfonos móviles conectados a otra celda), otra

forma es bloquear temporalmente el canal interferido, si el canal está en servicio entonces ocurre un *handoff* (traspaso de llamada a otro canal libre).

En ambos casos, el canal que experimenta interferencia se inhabilita para el tráfico, reduciendo la capacidad del sistema, por lo que podemos decir que la interferencia ha alcanzado un nivel definido en el mismo. En sistemas con rehuso múltiple de frecuencia, el nivel de interferencia de los canales bloqueados se puede reducir para incrementar la capacidad de tráfico del sistema, de lo contrario se tendría que operar con interferencia.

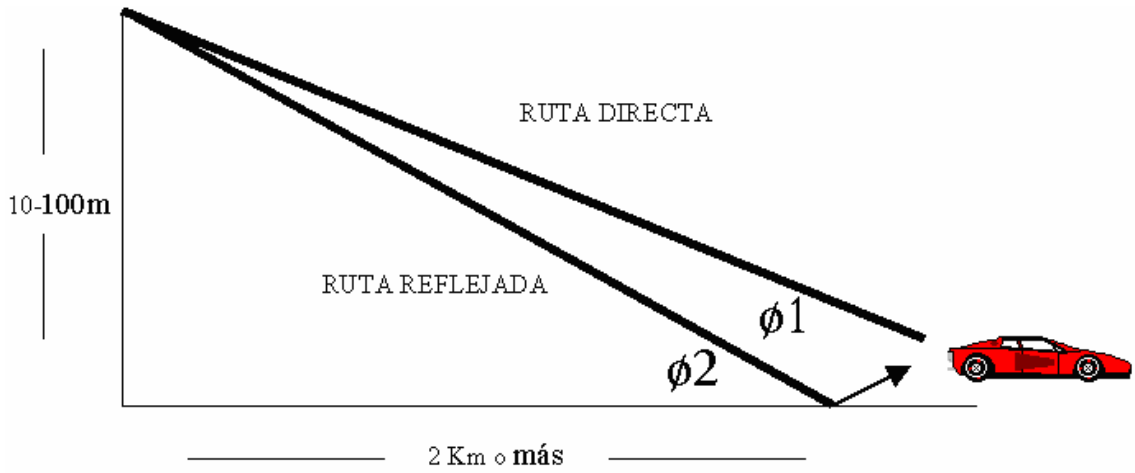
El cruce de conversaciones y la caída de llamadas puede ser resultado de la interferencia por co-canal y no necesariamente por el rehuso de frecuencia. Este tipo de interferencia usualmente está asociada con los sitios altos (ubicación geográfica alta), esto sería como estar utilizando los teléfonos de mano en la azotea de edificios, o estarlos operando desde colinas, por ésta razón no se recomienda la operación de teléfonos en aeronaves. Si se incrementa el rehuso de frecuencias inicialmente se aumenta la capacidad del sistema, también se incrementan los problemas de interferencia, lo que significa que en realidad el rehuso de frecuencia disminuye la capacidad del mismo, por lo tanto el objetivo será maximizar el rehuso de frecuencia minimizando la interferencia.

**Interferencia por co-canal:** esta es la forma de interferencia más frecuentemente encontrada en telefonía celular, y afortunadamente la más fácil de monitorear y controlar. Usando la información recolectada en el *drive test* (conducir un vehículo alrededor de una celda con teléfonos de prueba para recolectar datos) figura 14, es posible plotear el contorno de 20 dBpV/m para la estación base bajo estudio, entonces se sobrepone ésta gráfica a la gráfica de co-canal ploteada inicialmente a 40 dBuV/m (o a 39 dBuV/m si éste fuera el

valor usado), esto revelará inmediatamente algunos puntos de traslape entre la gráfica del teléfono móvil en servicio y la de la estación base a la que esté causándole interferencia (con una fuerza de campo de 40 dBuV/m).

En muchas áreas de interferencia por traslape puede reducirse con: *downtilt* (inclinación hacia abajo de las antenas), con la reducción de altura de las antenas o programando el inicio anticipado de *handoff*.

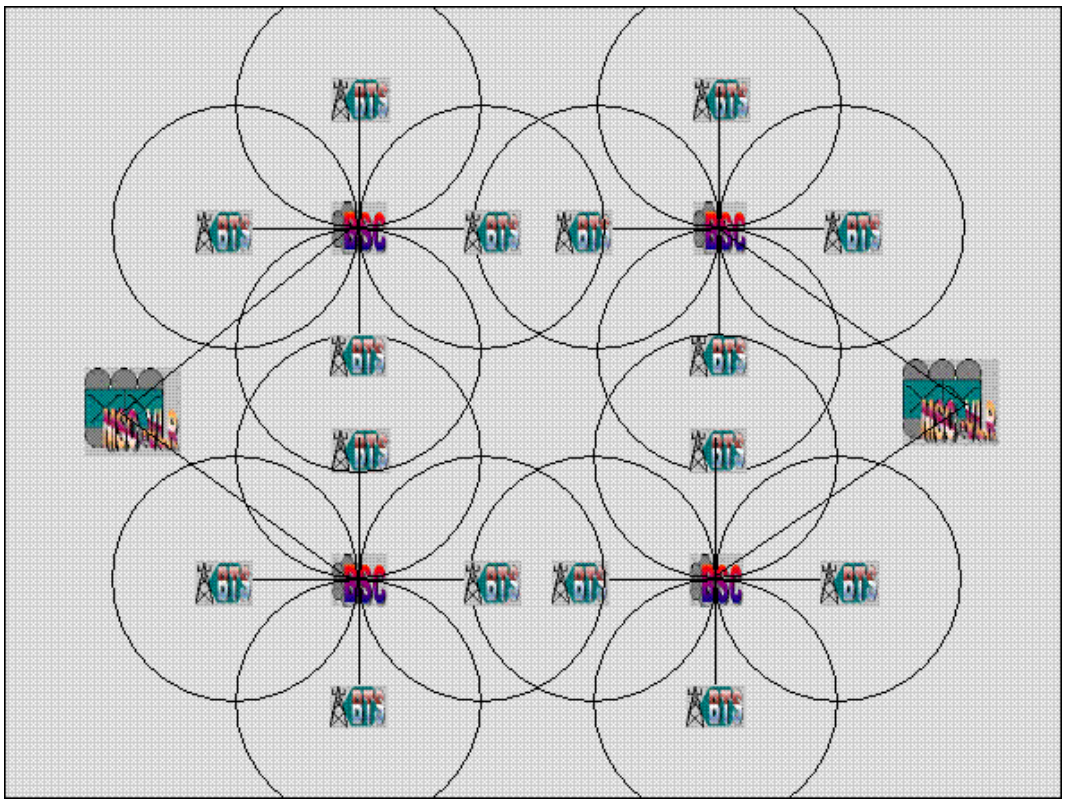
Figura 14. *Drive Test*




**Interferencia desde otros sistemas:** en muchos países hay por lo menos dos sistemas que compiten por el servicio, en Guatemala tenemos cuatro compañías compitiendo por la prestación del servicio celular, mientras los sistemas se diseñen para operar en la misma región geográfica la interferencia entre ellos puede ocurrir, por el ejemplo para Guatemala la interferencia de otros sistemas celulares se puede dar con los instalados en países vecinos como México, Belice, Honduras o El Salvador, siempre y cuando estos sistemas operen en la misma banda que los instalados en nuestro país.

En los sistemas AMPS generalmente es aceptado que hasta cuatro canales separados puedan causar interferencia de canal adyacente. En estos sistemas habrá dos regiones en donde esto puede ser potencialmente un problema. Este problema se puede observar por la figura 15.

Figura 15. Problemas por fallos de cobertura



Los canales están en los límites de las bandas A/B los canales 716 y 717 y los canales de control 333 y 334. Es aconsejable para los operadores con problema (y son la mayoría) coordinar con el competidor el uso de canales. En Guatemala otro caso de interferencia entre sistemas se da entre las frecuencias de los canales de voz del sistema celular y las frecuencias de operación de los

enlaces de radio de la compañía que opera la telefonía fija, en la región suroccidental los radios de transmisión de Telgua de los enlaces que conectaban la región de Malacatán, San Marcos; se salían de servicio porque operaban en la misma frecuencia de canales de voz de la celda ubicada en el cerro siete orejas, por algún tiempo se bloquearon los canales de voz de la celda para dar tiempo a la empresa Telgua para cambiar las frecuencias a sus enlaces de radio.

Otro problema de interferencia que ocurre es el provocado por equipos de radiocomunicación que operan en la en la región del espectro de 800 a 900 MHz, que es donde opera la banda B de telefonía celular de Comcel, este caso también sucedió en la celda del cerro siete orejas, para éste problema se rastrean con un analizador de espectro todas las frecuencias de los canales de voz, midiendo directamente en las antenas celulares; los que están interferidos se bloquean para evitar que la interferencia afecte a los usuarios, luego se detecta el equipo que está provocando la misma, si las frecuencias no están autorizadas para operar entonces se procede a sacarlos de servicio para poder realizar el cambio de sus frecuencias.

Los sistemas celulares están diseñados para operar en un ambiente de interferencia. Una forma utilizada por el sistema para reducir interferencia es programando instrucciones a los teléfonos móviles para que reduzcan su potencia cuando están lo suficientemente cerca de la estación base para realizar adecuadamente éste procedimiento de reducción de potencia por *software* se dan instrucciones a la celda desde la central telefónica para que los teléfonos bajen paso a paso sus niveles de potencia, dependiendo de la distancia a la que se encuentren. Para AMPS y TACS, la potencia de salida de un teléfono móvil puede estar alrededor de 28 los dB durante una conversación. Una facilidad similar está disponible en los sistemas NMT. En la tabla II se

muestra la reducción de niveles de potencia en los sistemas AMPS, tomando en consideración que éste es el sistema utilizado por la empresa que se utiliza como área de campo investigada.

Tabla II. Reducción de niveles de potencia en los sistemas AMPS

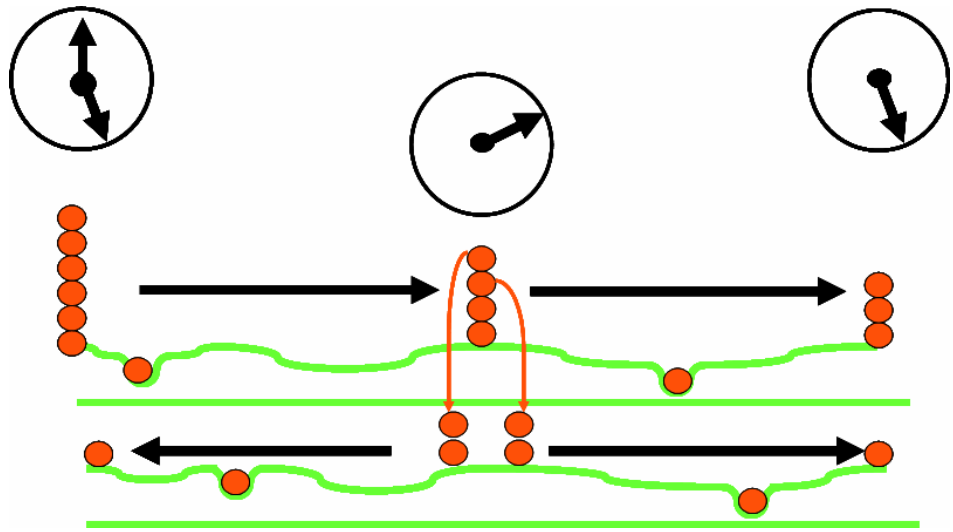
| **Nivel** | **Reducción de potencia en (dB)** |
|---|---|
| 1 | 4 |
| 2 | 8 |
| 3 | 12 |
| 4 | 16 |
| 5 | 20 |
| 6 | 24 |
| 7 | 28 |

No es usual que en los nuevos sistemas la banda reservada para uso celular tenga usuarios previamente establecidos, ya que estos puedan ser identificados, porque obviamente serían bloqueados al ser detectados por los otros operadores ya que estos usuarios ocuparían espacios de su frecuencia. Esto ocurrió en un principio porque la CCIR recomendó que las asignaciones del espectro de frecuencia no incluyeran espectro para los sistemas celulares. Sin embargo, esto ha cambiado y ahora existe un rango definido del espectro de frecuencia para operación de la telefonía celular, que es el situado entre los 800 y 900 MHz, aunque ahora existen otros segmentos del espectro para la telefonía digital de PCS, a veces se encuentran "otros usuarios" en este rango del espectro, la mayoría de las veces son frecuencias de los enlaces punto a punto de microonda, estos sistemas operan continuamente y en forma direccional, por lo que su área de interferencia es limitada.

### 5.5.2. Interferencia en sistemas digitales

En éste caso se hace referencia al sistema Análogo/digital D-AMPS instalado en Guatemala, trataremos algunos casos de interferencia que se dan en la parte digital del sistema, se enfatiza en la forma de atacar esta problemática. Ya que el problema de la diafonía digital consiste en que la señal eléctrica transmitida por un par induce corrientes en pares vecinos y el efecto es tal como se observa en la figura 16.

Figura 16. Problema de la diafonía digital



**Control de la diafonía digital:** una causa importante de perturbaciones en los sistemas de telefonía es el eco que se produce cuando parte de la energía de la señal de voz del abonado que habla se refleja y regresa al origen. En una conversación telefónica, el eco es irritante cuando tiene una demora sustancial (demora física o de procesado en el trayecto de transmisión). Una fuente típica de eco es un desajuste de impedancia en la conversación de cuatro hilos a dos

hilos en los interfaces de abonado de la PSTN. Hoy, en los centros de conmutación internacionales y móviles es común usar supresores para controlar el eco generado en el bucle local del extremo de PSTN en la conexión.

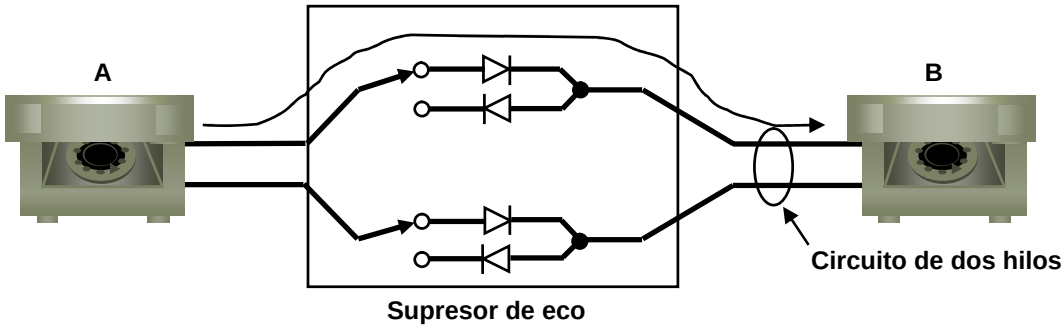
También puede producirse eco en las redes celulares como consecuencia de diafonía acústica dentro de los teléfonos portátiles a causa de la conexión acústica entre el micrófono y el alta voz portátil digital. La mejor forma de controlar este tipo de eco es dentro del propio teléfono, como reconocen varias recomendaciones internacionales.
Aún cuando los teléfonos móviles satisfacen los requisitos de atenuación de eco, en ciertas condiciones los usuarios todavía notar el eco producido por diafonía acústica. Esto se debe principalmente a dos factores:

- La especificación de ensayo no tiene en cuenta todas las variaciones posibles en la posición del portátil durante una conversación normal.

- Los niveles de línea entre el sistema de telefonía pueden desviarse de los niveles nominales.

El eco por diafonía acústica puede ser molesto para los usuarios. Si puede suprimirse, mejorando la calidad del habla general del sistema. No obstante, debido a que este eco difiere considerablemente del de las redes convencionales para suprimirlo hacen falta soluciones diferentes.

Figura 17. Supresor de eco para un circuito de dos hilos



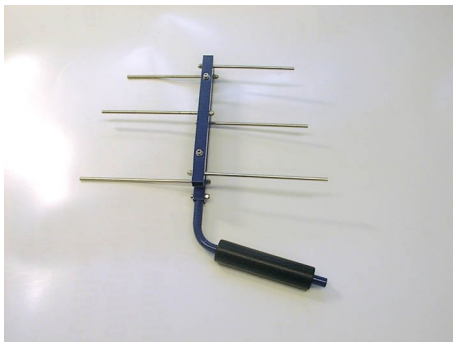

**Los supresores de eco en redes:** en la actualidad los centros de conmutación internacional y móvil usan supresores de eco para controlar la resonancia producida en el bucle local de la PSTN. Los medios para eliminar este tipo de eco han sido objeto de amplios estudios. Ordinariamente, pueden hacerse modelos exactos del trayecto de eco de la PSTN usando un filtro de respuesta de impulso finito lineal (FIR) con coeficientes que son constantes o que varían lentamente en el transcurso del tiempo. Usualmente, el supresor de eco está ubicado en el sistema, de modo que la duración del trayecto de eco sea inferior a 64 milisegundos.

**Interferencia móvil e intermitente:** este tipo de interferencia es la más problemática porque la fuente ofensiva es muy difícil de localizar esta es mayormente asociada a sistemas no digitales. No hay realmente una forma eficaz de rastrear el móvil ofensivo en un ambiente urbano, excepto cuando se tiene una gran paciencia y un gran equipo de rastreo. La naturaleza intermitente de estas transmisiones significa que debe esperarse mucho tiempo para erradicarlas. Una vez la transmisión comienza, el método más efectivo es usar dos vehículos equipados cada uno con antenas direccionales y comunicación en las dos vías, para localizar el objetivo, preferiblemente hacer el rastreo en

dos direcciones diferentes y usando la intersección del vector de direccionamiento de búsqueda para localizar el objetivo.

Recordar, sin embargo, que el modo de propagación es tal que encontrar soluciones exactas es casi imposible, por eso es necesario fue el blanco transmita durante un tiempo considerable (normalmente horas) para localizarlo. Los dispositivos de efecto doppler están disponibles, estos usan cuatro receptores y dan una lectura directa de la interferencia por medio de un lector digital. Menos difícil de localizar, pero no por eso fáciles son las intermitencias de enlaces o repetidores. El primer paso es medir la fuerza del campo desde varias estaciones base celulares diferentes en posición triangular respecto del objetivo. El siguiente paso es obtener una medida de la fuerza del campo del portátil receptor, equipado con una antena yagi como la de la figura 18, luego salir a buscar. A menos que las fuentes estén muy cerradas de aquí en adelante será fácil localizarlas, y podría utilizarse una semana en localizar al interferente.

Figura 18. Antena yagi



## 5.6. Mecanismos utilizados por las empresas de telecomunicaciones en Guatemala en la transmisión de datos

De acuerdo con el material proporcionado por las empresas de telecomunicaciones en Guatemala las cuales por medidas de confidencialidad no se indicarán los nombres de las empresas que proporcionaron este tipo de material el cual trata en parte del tipo de tecnología GSM del cual usan estas empresas y el cual consideran como un mecanismo muy confiable ya que para estas empresas las motivaciones referentes a la seguridad en los sistemas de telecomunicaciones celulares son asegurar las conversaciones y datos de señalización de potenciales interceptaciones así como impedir posible fraude en telefonía celular.

Con los sistemas de telefonía celular analógicos más antiguos como AMPS (Advanced Mobile Phone System) y TACS (Total Access Communication System) es relativamente simple para cualquier aficionado a cuestiones de radio interceptar conversaciones telefónicas celulares con un simple escaner de la policía. Otra consideración referente a la seguridad de los sistemas analógicos de telecomunicaciones celulares que tiene que ver con la identificación de credenciales utilizando el ESN (Electronic Serial Number) es que se transmite en claro (sin cifrar). Con equipos sofisticados es posible recibir el ESN y utilizarlo para cometer fraude de teléfono celular suplantando otro teléfono celular y realizando llamadas con él.

El procedimiento en donde la estación móvil registra su localización con el sistema también es vulnerable a la interceptación y permite monitorizar la localización del abonado incluso cuando una llamada no está en progreso. Los mecanismos de seguridad (confidencialidad, autenticación, etc.) incorporados en GSM hacen que sea el estándar de comunicaciones móviles más seguro y

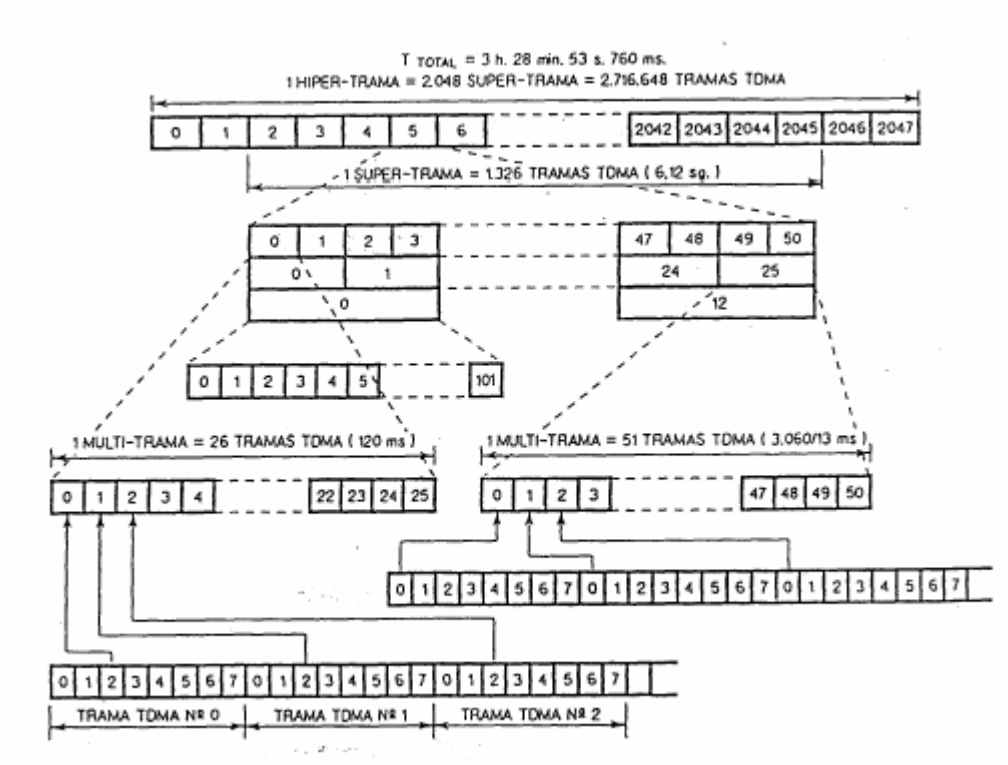
disponible en la actualidad; particularmente en comparación con los sistemas analógicos antes citados. Parte de la seguridad mejorada de GSM se debe al hecho de que es un sistema digital que utiliza un algoritmo de codificación de voz, modulación digital GMSK (Gaussian Minimum Shift Keying), lento salto de frecuencia y arquitectura de ranuras de tiempo TDMA (Time Division Multiple Access). Para interceptar y reconstruir esta señal deberían necesitarse equipos más caros y especializados que un simple escaner de la policía para realizar la recepción, sincronización y decodificación de la señal. Además, las capacidades de cifrado y autenticación aseguran la seguridad de las conversaciones de teléfono celular GSM y de las credenciales de identificación del abonado contra posibles escuchas clandestinas.

En Guatemala, el estándar GSM especifica las bandas de frecuencia de 890 a 915 MHz. para la banda del enlace saliente y 935 a 960 MHz. para la banda del enlace entrante; cada banda se divide en canales de 200 KHz. Otras características del interfase de canal de radio son la alineación de tiempo adaptativa, la modulación GMSK, la transmisión y recepción discontinua y el salto de frecuencia lento. La alineación de tiempo adaptativa permite a la estación móvil corregir su ranura de tiempo de transmisión para retardos de propagación. La modulación GMSK proporciona eficiencia espectral e interferencia fuera de banda baja requerida en el sistema GSM. La transmisión y recepción discontinua se refiere a la caída de potencia de la estación móvil durante períodos de inactividad y sirve al doble propósito de reducir la interferencia entre canales y aumentar el tiempo de vida de la batería de la unidad portable. El salto de frecuencias lento es una característica adicional del interfaz de canal de radio GSM que ayuda a contrarrestar efectos de desvanecimiento Rayleigh y de la interferencia entre canales.

Los canales de 200 KHz. de cada banda se subdividen en ranuras de tiempo de 577 milisegundos. Si se juntan ocho ranuras de tiempo se forma "una trama" TDMA de 4,6 milisegundos. Juntando 26 ó 51 tramas TDMA se forma una "multitrama" (120 ó 235 milisegundos) dependiendo de si el canal es para tráfico o datos de control. Juntando 51 ó 26 multitramas (de nuevo, dependiendo del tipo de canal) se forma una "supertrama" (6.12 segundos). Una "hipertrama" se compone de 2048 supertramas, totalizando una duración de 3 horas, 28 minutos, 53 segundos y 760 milisegundos.

La estructura de trama TDMA tiene asociado un número de secuencia de 22 bits que identifica de forma única una trama TDMA dentro de una hipertrama dada. La figura 19 muestra las diversas estructuras de tramas TDMA. Los distintos canales lógicos que son convertidos en la estructura de tramas TDMA pueden ser agrupados en canales de tráfico (o TCHs, Traffic Channels) utilizados para transportar voz o datos de usuario y canales de control (o CCHs, Control Channels) utilizados para transportar señalización y datos de sincronización. Los canales de control se dividen en canales de control de difusión, canales de control común y canales de control dedicados. Cada ranura de tiempo dentro de una trama TDMA contiene datos modulados denominados ráfaga (o "burst").

Figura 19. Estructura de las tramas




Existen cinco tipos de ráfagas: normal, corrección de frecuencia, sincronización, dummy (de relleno) y ráfagas de acceso. La tasa de bits del canal de radio es de 270,833 Kbps que corresponde a la duración de una ranura de tiempo de 156,25 bits. La ráfaga normal se compone de una secuencia de arranque (o "start") de tres bits, 116 bits de carga útil (o "payload"), 26 bits de secuencia de entrenamiento utilizada para ayudar a contrarrestar los efectos de la interferencia multicamino, 3 bits de secuencia de parada (o "stop") necesitados por el codificador de canal y un período de guarda (de una duración de 8.25 bits) que es un "colchón" para permitir tiempos de llegada diferentes de ráfagas en ranuras de tiempo adyacentes desde estaciones móviles dispersas geográficamente. Dos bits de la carga útil de 116 bits se utilizan por el canal de control asociado rápido (o FACCH, Fast Associated Control Channel) para señalar que una ráfaga dada ha sido tomada, dejando un total de 114 bits de carga útil.

El algoritmo de codificación de voz utilizado en GSM está basado en un codificador predictivo lineal excitado por impulso rectangular con predicción a largo término (o RPE-LTP, Rectangular Pulse Excited linear predictive coder with Long-Term Prediction). El codificador de voz produce muestras a intervalos de 20 milisegundos a una tasa de bits de 13 Kbps, produciendo 260 bits por muestra o trama. Estos 260 bits se dividen en 182 bits de clase 1 y 78 bits de clase 2 basándose en una evaluación subjetiva de su sensibilidad a los errores de bits, los bits de clase 1 son más sensibles. La codificación de canal supone la adición de bits de comprobación de paridad y codificación convolucional de media tasa de la salida de 260 bits del codificador de voz. La salida del codificador de canal es una trama de 456 bits, que se divide en 8 componentes de 57 bits y se entremezcla ("interleaved") sobre ocho tramas consecutivas TDMA de 114 bits. Cada trama TDMA consta de dos conjuntos de 57 bits procedentes de dos tramas separadas de codificador de canal de 456 bits. El resultado de la codificación de canal y del entremezclado es para contrarrestar los efectos de desvanecimiento de interferencia de canal y otras fuentes de errores de bits.

**Descripción de las características de seguridad**

Los aspectos de seguridad de GSM se describen en las recomendaciones GSM 02.09 (Aspectos de Seguridad), 02.17 (Módulos de Identidad del Abonado o SIMs), 03.20 (Funciones de Red Relacionadas con la Seguridad) y 03.21 (Algoritmos Relacionados con la Seguridad).

La seguridad en GSM consta de los siguientes aspectos:

(1) Autenticación de la identidad del abonado.
(2) Confidencialidad de la identidad del Abonado.

(3) Confidencialidad de los datos de señalización.
(4) Confidencialidad de los datos del usuario.

El abonado se le identifica de forma única utilizando la identidad de abonado móvil internacional (o IMSI, International Mobile Subscriber Identity). Esta información junto con la clave individual de autenticación de abonado (Ki) constituyen las credenciales de identificación sensibles, análogas al ESN (Electronic Serial Number) de los sistemas analógicos como AMPS (Advanced Mobile Phone System) y TACS (Total Access Communication System). El diseño de los esquemas de cifrado y autenticación es tal que esta información sensible nunca se transmite por el canal de radio. En su lugar se utiliza un mecanismo de desafío-respuesta para realizar la autenticación. Las transmisiones de datos reales se cifran utilizando una clave temporal de cifrado generada aleatoriamente (Kc).

La estación móvil (o MS, Mobile Station) se identifica por medio de la identidad temporal de abonado móvil (o TMSI, Temporary Mobile Subscriber Identity) que emite la red y puede cambiarse periódicamente (por ejemplo durante momentos de no intervención o *hand-offs*) para mayor seguridad.

Dentro de la red GSM, la información de seguridad se distribuye entre el AUC (Authentication Center), el registro de localización doméstico (o HLR, Home Location Register) y el registro de localización del visitante (o VLR, Visitor Location Register). El Centro de Autenticación (o AUC) es responsable de generar los conjuntos de RAND (Número aleatorio), SRES (Respuesta firmada) y Kc (clave de cifrado temporal generada aleatoriamente) que se encuentran almacenados en el HLR y en el VLR para su utilización posterior en los procesos de autenticación y cifrado.

**Proceso de autentificación**

La red GSM autentifica la identidad del abonado utilizando un mecanismo de "desafio-respuesta". Se envía a la estación móvil un número aleatorio de 128 bits (denominado RAND). La estación móvil (o MS) calcula la respuesta firmada de 32 bits (denominada SRES, Signed Response) basándose en el cifrado del número aleatorio (RAND) con el algoritmo de autenticación (denominado A3) utilizando la clave individual de autenticación de abonado (Ki). Al recibir del abonado la respuesta firmada (SRES), la red GSM repite el cálculo para verificar la identidad del abonado.

Hay que notar que la clave individual de autenticación de abonado (Ki) nunca se transmite sobre el canal de radio. Está presente en el SIM del abonado, así como en las Bases de Datos del AUC, HLR y VLR. Si el SRES recibido coincide con el valor calculado, la estación móvil ha sido autentificada con éxito y puede continuar. Si los valores no coinciden la conexión se termina y se indica un fallo de autenticación a la estación móvil. El cálculo de la respuesta firmada (SRES) se realiza dentro del SIM. Esto proporciona mayor seguridad, debido a que la información del abonado confidencial como la IMSI o la clave individual de autenticación del abonado (Ki) nunca salen del SIM durante el proceso de autenticación.

**Proceso de confidencialidad de los datos y señalización en GSM**

El SIM contiene el algoritmo de generación de claves de cifrado (denominado A8) que se utiliza para producir la clave de cifrado (Kc) de 64 bits. La clave de cifrado se calcula aplicando el mismo número aleatorio (RAND) utilizado en el proceso de autenticación con el algoritmo de generación de la clave de cifrado (A8) con la clave individual de autenticación de abonado (Ki).

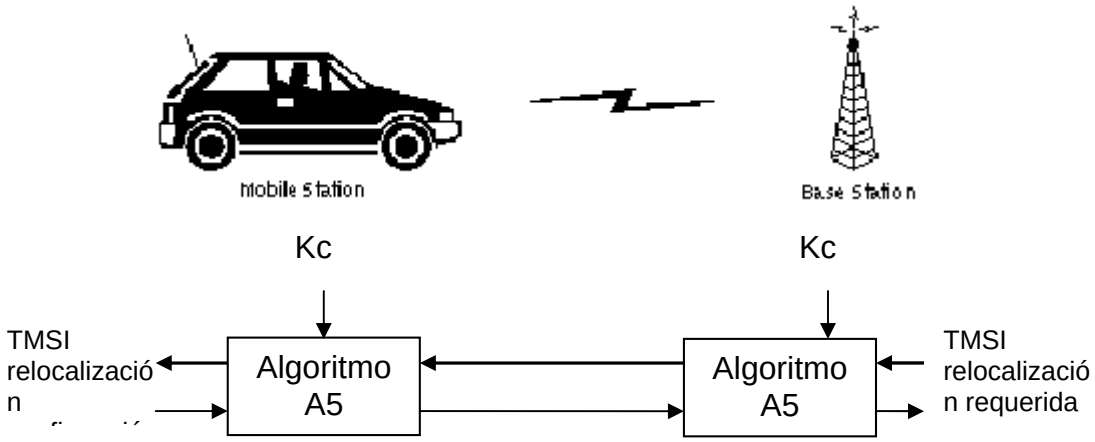
La clave de cifrado (Kc) se utiliza para cifrar y descifrar los datos transmitidos entre la estación móvil y la estación base. Se proporciona un nivel adicional de seguridad al haber medios para cambiar la clave de cifrado, haciendo al sistema más resistente contra posibles "escuchas clandestinas".

La clave de cifrado puede cambiarse a intervalos regulares según lo requieran las consideraciones de seguridad y diseño de red. El cálculo de la clave de cifrado (Kc) tiene lugar internamente dentro del SIM. Por tanto, la información sensible como la clave individual de autenticación de abonado (Ki) nunca la revela el SIM. Las comunicaciones de datos y voz cifradas entre la estación móvil y la red se realizan utilizando el algoritmo de cifrado A5. La comunicación cifrada se inicia por un comando de "petición de modo de cifrado" desde la red GSM. Al recibir este comando, la estación móvil empieza el cifrado y descifrado de datos utilizando el algoritmo de cifrado (A5) y la clave de cifrado (Kc).

**Proceso de confidencialidad de la identidad del abonado**

Para asegurar la confidencialidad de la identidad del abonado se utiliza la TMSI. La TMSI se envía a la estación móvil después de que han tenido lugar los procedimientos de autenticación y cifrado. La estación móvil responde confirmando la recepción de la TMSI. La TMSI es válida en el área de localización en la que fue emitida. Para comunicaciones fuera del área de localización, es necesario además de la TMSI, la LAI (Location Area Identification). El proceso de asignación/reasignación de la TMSI se muestra en la figura 20.

Figura 20. Utilización del MTSI




## 5.7. Críticas a los aspectos de seguridad en la transmisión de datos y a los servicios que prestan las empresas de telecomunicaciones en Guatemala

En Guatemala tanto los servicios y las formas de seguridad que ofrecen las tecnologías de tercera generación para las redes celulares CDMA y GSM no poseen ningún valor agregado que haga de estos protocolos competentemente seguros ya que a éstos en su forma convencional se les ha descubierto un conjunto de aspectos que hacen muy vulnerable al sistema. En cuanto a las redes de datos si se puede indicar que se tiene un mayor control de la seguridad en nuestro país ya que por el uso de mecanismos de seguridad tal como los protocolos seguros, algoritmos asimétricos, entre otros, hacen que las seguridad dentro de la red de datos sea algo que posee un estándar aceptable en cuanto a seguridad en la red de datos. A diferencia de la red telefónica celular el cual posee algunos errores de los cuales se comentarán.

En Guatemala algunas compañías que prestan el servicio de telefonía celular y sus diversos tipos de servicios para la transmisión de datos aún tienen habilitados los servicios de telefonía bajo protocolos inseguros tales como el TACS, este permite fácilmente tomar la información bajo este sistema que no encripta la información; es utilizado para la transmisión de la voz y no se le da tanto uso para transmitir datos, para la transmisión de datos es común el uso de CDMA y GSM el cual utiliza un algoritmo de codificación, modulación digital GSMK, lento salto de frecuencia y arquitectura de ranuras de tiempo TDMA.

El GSM ha sido muy gestionado a nivel mundial, uno de los usos que se le había asignado en sus inicios es que se podría utilizar un móvil con este tipo de tecnología como una forma alternativa de pago, tal como se hace con una tarjeta de crédito pero ante el aumento del fraude en el uso de las tarjetas de crédito tradicionales y hasta que se generalice el uso de las tarjetas basadas en chip inteligente que sean más seguras, el teléfono GSM se está convirtiendo en un firme candidato a cubrir este nicho del mercado.

Las compañías telefónicas en Guatemala podrían considerar que este tipo de problemas no se llegue a dar en Guatemala pero esto es algo que puede ocurrir y a lo que se debe de tener una plan de contingencias para que en el futuro, si estas compañías se dedican más a la transmisión de la información por medio de las redes de datos deben tener una infraestructura que sea totalmente confiable. Pero esto bajo el esquema que trabaja GSM sin ningún valor agregado no es totalmente confiable.

En primer lugar, el usuario está identificado en la red a través de su tarjeta SIM, la cual en teoría, es personal e intransferible. Cada tarjeta dispone, de un código interno o clave, a la que se le asocia un número de teléfono usando el sistema de gestión de la red. Por ello, el usuario siempre está

identificado en la red por su código SIM, que teóricamente es secreto y no se puede extraer de la tarjeta, impidiendo así, la posibilidad de clonar la tarjeta y hacerse pasar por el usuario. Opcionalmente, se puede proteger la tarjeta SIM, utilizando un código de cuatro cifras, que solamente le será solicitado, cuando se active el teléfono.

En segundo lugar, las comunicaciones entre la base y el teléfono móvil GSM, están codificadas mediante un algoritmo, propietario y secreto, denominado A5/1, que en teoría, impide interceptar las comunicaciones de voz o de datos, pero hay que recordar que dicha codificación se realiza solamente en el tramo vía radio. Lo que pase cuando la comunicación entre en la red del operador, dependerá de cada red y no hay mucha información respecto a ello.

Lo que se puede indicar de la codificación del GSM es que la mayoría de los proveedores GSM utilizan un mismo algoritmo, denominado COMP128, para el cifrado A3 y A8. Este algoritmo es criptográficamente débil y no es difícil romperlo con la finalidad de clonar los teléfonos GSM. El ataque requiere enviar 2^18 intentos al teléfono, lo que se puede hacer en aproximadamente 8 horas y se puede realizar con acceso físico a la tarjeta SIM (opción barata ya que cada SIM de estos en el país cuesta alrededor de Q. 45.00) o sin acceso físico, vía radio (opción que puede ser interceptada por una central telefónica).

Lo anterior se asocia al estudio de la forma como trabajan los operadores de telefonía celular en Guatemala y a lo que el grupo Berkeley en Estados Unidos publicó al análisis de este algoritmo en abril de 1998 y demostró que su seguridad no era demasiado buena, por haber sido debilitado deliberadamente. De los 64 bits que componen la clave, solamente se utilizan 54, lo que equivale a reducir la efectividad 1024 veces. Si tuviera una computadora que se tardara un año en comprobar todas las claves de 64 bits posibles, la reducción a 54

bits, supone que usando el mismo sistema informático, tardaría entre cuatro y ocho horas y media en descubrir la clave correcta. Seguramente, esta reducción en el tamaño de la clave fue motivada por el deseo de acceder a la escucha de las conversaciones GSM con una relativa facilidad. Incluso hay una versión del algoritmo, mucho más débil denominada A5/2, que tenía como objetivo la exportación a determinados países y en su diseño intervino la NSA americana. Esta versión fue analizada en agosto de 1999 por este mismo grupo de Berkeley, descubriendo que se podía romper en tiempo real, con solamente 2^16 operaciones. Esta misma asociación, en mayo de 1999 ya había publicado la implementación del algoritmo A5/1.

Lo que sí se debe de reconocer es que cada teléfono dispone de un número, denominado IMEI, que permite identificar un teléfono en la red GSM, aunque se le cambie el SIM. Para evitar el posible uso del teléfono con otro SIM (si lo pierde, o se lo roban), puede activar una opción de seguridad, que solicitará un código de 5 cifras cuando se cambie de tarjeta SIM. Además, a los usuarios de servicios de pago a través de GSM, se les proporciona un sistema adicional de autenticación, basado normalmente en un código secreto, que deberá utilizar para realizar las operaciones de pago y que se puede cambiar en cualquier momento.

## 5.8. Sugerencias para mejorar la seguridad en la transmisión de datos y los servicios para que las redes telefónicas y las redes de datos sean fuentes más confiables

- Agregar al sistema ya existente en las redes celulares un mecanismo inteligente que pueda detectar cualquier tipo de interferencia y en caso

que sea una interferencia por un agente externo bloquear la transmisión de información.

- Si hay posibilidades, se deben reservar canales para uso exclusivo de las celdas periféricas de la ciudad, en especial para aquellas que están ubicadas en la parte alta de la ciudad capital esto para evitar cualquier tipo de interferencia del tipo co-canal.

- Disminución de altura de las antenas, cambio de tipo de antenas, a un tipo de "lóbulo suprimido" de decibeles, esto en las celdas del valle de la ciudad, con excepción de las que se denominan "servidoras" en la zona de negocios esto según el Departamento de Ingeniería de Seguridad de Ericsson Guatemala.

- Si hay posibilidad utilizar canales exclusivos para las celdas periféricas, porque podría elevarse la potencia de los sectores que alumbran hacia fuera, de manera que se disminuiría la interferencia en toda esa área, al mismo tiempo que se mejoraría la cobertura.

- Revisión y sustitución de las antenas que están provocando interferencia hacia otras celdas, principalmente con la colocación de antenas que posean una mejor relación frecuencia/cobertura.

- Reconsiderar el diseño de asignación de frecuencias y el de potencia de transmisión de todo el sistema para no encontrar frecuencias cruzadas o cercanas que causen desplazamiento de frecuencias y que la información no solamente la perciba un receptor.

- Crear una infraestructura más sólida de los servicios de transmisión de datos de redes celulares hacia redes de datos aunque en este momento no sea algo que tenga mayor demanda en el mercado guatemalteco.

- Poseer un control mayor sobre el personal que labora dentro de estas instituciones ya que el problema de la seguridad debe de iniciar desde el lugar donde se pretende establecer el control.

- Establecer mecanismos que aseguren en forma más segura la transmisión de voz y de datos con tecnologías más seguras como es el caso de la encripción UMTS el cual es mucho más robusto y se ha sometido públicamente a la comunidad internacional, para su escrutinio y comprobación.

- Establecer mayores políticas para evitar problemas de ingeniería social y que en un momento indicado una persona que labora en alguna de las instituciones de telecomunicaciones sea el causante de cualquier anomalía sobre la seguridad en la transmisión de datos.

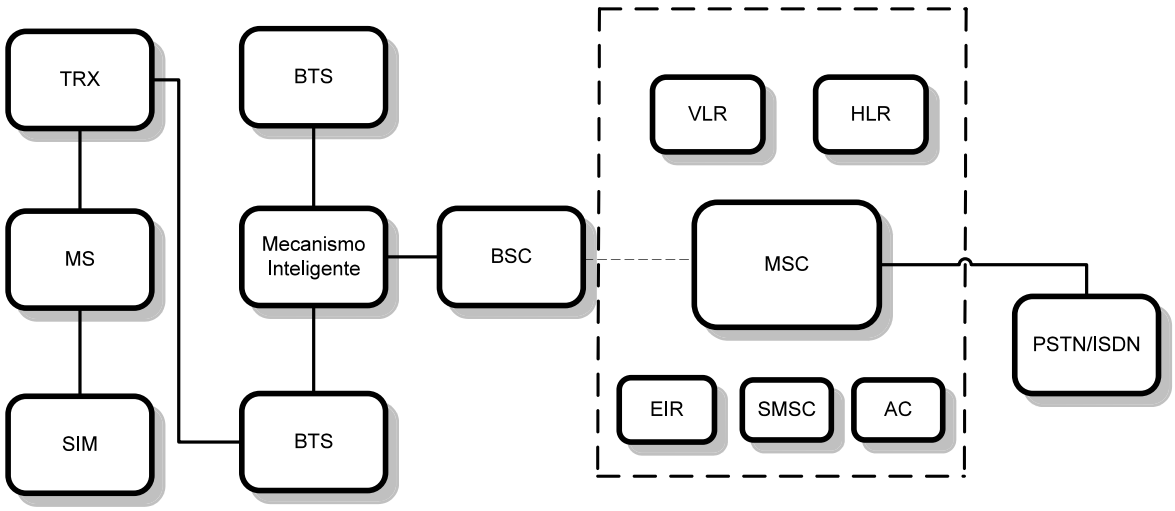
## 5.9. Ejemplo de un modelo para incrementar la seguridad en la transmisión de datos de las redes telefónicas a las redes de datos en Guatemala

Para el desarrollo e implementación de un modelo que proporcione mayor seguridad se debe de centrar en el hecho de que los algoritmos que interactúan en GSM mejor conocidos como A3 A5 y A8 son algoritmos que caen ante algoritmos de fuerza bruta por lo que se debe prestar una mayor atención en el hecho de que si se agrega un mecanismo inteligente que interactué con el

sistema ya existente que corrija y proporcione la seguridad completa del abonado y por medio de éste se autentique para que no se clonen los teléfonos.

En cuanto al desarrollo de un modelo que incremente la seguridad en los sistemas de transmisión de datos y de voz con tecnología GSM específicamente se tratará un modelo a bloques con el cual se puede mostrar cómo se puede incrementar la seguridad sobre este tipo de sistema.

Figura 21. Modelo con incremento de seguridad en una red GSM




Los elementos que se consideran para el desarrollo de este modelo son los siguientes:

TRX: *Transceiver* (Transrecibidor)
EIR: *Equipment Identity Register* (Registro de Identificación del Equipo)
MS: *Mobile Station* (Estación Móvil)
AC: *Authentication Center* (Central de Autenticación)
SIM: *Subscriber Identity Module* (Módulo de Identificación de Suscritor)

HLR: *Home Location Register* (Registro de Localización de Llamada)
BTS: *Base Transceiver Station* (Estación Transrecibidora de Base)
Mecanismo Inteligente: Mecanismo con sistema Inteligente
BSC: *Base Station Controller* (Estación Base de Control)
MSC: *Mobile services Switching Center* (Central Intercambiadora de Servicios Móviles)
VLR: *Visitor Location Register* (Registro de Localización del Visitante)
ISDN: *Integrated Services Digital Network* (Red Digital de Servicios Integrados)
PSTN: *Public Switched Telephone Network* (Red Telefónica Analógica Pública)
SMSC: *Short Message System Center* (Central de Sistema de Mensajes Cortos)

Como se puede observar este sistema GSM contiene un elemento de valor agregado, pues es un sistema inteligente que aporta un conjunto de funciones para detectar la intrusión entre el móvil y la estación base de control. La forma como podría funcionar es tomando un conjunto de hechos del comportamiento que se presenta sobre la red y sobre cada uno de los móviles ya que un sistema de transmisión de datos puede ser monitorizado con base en el comportamiento que tenga y se centraría en el hecho de hallar el máximo de anomalías ya que las anomalías o cambios repentinos pueden ser captados por un mecanismo inteligente bien adaptado para responder a esto se puede poseer un conjunto de políticas que indiquen cual es el comportamiento que el mecanismo inteligente debe tomar, esto con base en prioridades que se contengan con los datos, o con base a la importancia de la información que se estén registrando ya que si se realiza una transacción monetaria por medio de nuestro móvil no se puede permitir que un tercero cobre algo que no le corresponde.

El funcionamiento de este tipo de sistema GSM con el mecanismo inteligente adaptado sería de la siguiente forma:

La estación móvil, o terminal, contiene la tarjeta SIM, ésta es utilizada para identificar a quien usa el servicio dentro de la red. El SIM es el que provee movilidad personal al que está utilizando la tarjeta, permitiéndole acceder a los servicios de la red independientemente del teléfono móvil que use o su localización, todo esto debe ser identificado y cuestionado por el mecanismo inteligente este proporciona el acceso real del sistema al móvil. El SIM puede ser protegido contra uso indebido a través de un código (PIN) el cual es desencriptado por el mecanismo inteligente que trabajará una forma de encripción con un algoritmo asimétrico que hay que marcar cada vez que se conecta el móvil con el SIM inserido. Existe un número que identifica cada terminal individualmente, el International Mobile Susbcriber Identity (IMEI), pero que es independiente del SIM.

La estación base controla la conexión radio entre el teléfono móvil y la red y también es conocida por célula, cada célula es controlada y monitoreada también por el mecanismo inteligente, ya que cubre una determinada área geográfica. Una BSS está compuesta por dos elementos: el BTS (Base Transceiver Station) y el BSC (Base Station Controler). Cada BSS puede tener uno o más BTS. Las BTS albergan el equipo de transmisión / recepción (los TRX o transceivers) y gestionan los protocolos de radio con el terminal móvil. En áreas urbanas es en donde existen más BTS que en zonas rurales y en algunos casos con características físicas o geográficas particulares (como por ejemplo, túneles) son colocados retransmisores para garantizar el servicio. Cada estación utiliza técnicas digitales para permitir que varios utilizadores se liguen a la red, también para permitir que hagan y reciban llamadas simultáneamente. Esta gestión se denomina de multiplexing.

En esta parte el trabajo que realiza el mecanismo inteligente es muy importante ya que entre el BTS y el BSC se encuentra este mecanismo inteligente que regula de una mejor forma la ubicación GPS que se maneja entre el BTS y el móvil ya que uno de los problemas que ocurre entre la red es la clonación de los teléfonos móviles la cual sería eliminada por completo ya que recordemos que el funcionamiento del sistema celular entre el BTS, el móvil y el BSC se puede describir de la siguiente forma:

1. El móvil se reporta cada determinado lapso hacia una BTS.
2. El BTS se encuentra sobre una ubicación geográfica que es conocido por el BSC.
3. El BSC es el encargado de controlar el proceso que se establece entre una llamada que realice un móvil con cualquier otro mecanismo.

¿Qué sucede si un móvil se clona en el paso?

El BSC normalmente falla ante este tipo de anomalía. El fallo al que corresponde comúnmente equivale a 1) botar los dos móviles del sistema, 2) proveer de comunicación a ambos móviles, 3) botar a uno de los dos aleatoriamente tomará alguno. Esta es la respuesta que nos da el sistema GSM común.

Con el mecanismo inteligente este problema es atacado en el paso dos ya que la ubicación de cada uno de los móviles se puede controlar ya que con este mecanismo el teléfono que ha sido clonado, en el momento que ésta reportándose ante el BTS y esté informando al sistema inteligente que trabaja con el BSC. El mecanismo inteligente encontraría la anomalía que el móvil que

se está reportando ya se encuentra en uso y aunque el móvil original se encuentre apagado el código que se le asignó al SIM por parte del mecanismo inteligente el cual controla una encriptación asimétrica aceptaría un reto enorme para las personas que se dedicarán a este tipo de negocios, ya que al adaptar sistemas de encripción que son de uso frecuente en sistemas informáticos a sistemas celulares el reto se vuelve mayor para los comúnmente llamados *hackers*. Con este tipo de mecanismo no se puede indicar que es totalmente indestructible pero si puede presentar una mejora considerable para el GSM.

El mecanismo inteligente por medio del BSC administra los recursos de radio de una o más BTS. Entre sus funciones se incluyen el *handoff* (que ocurre cuando el utilizador se mueve de una célula para otra, permitiendo que la ligación se mantenga), esto también se adapta para el mecanismo inteligente ya que con esto puede tener un registro de la forma como el móvil se ha comportado en cuanto a ubicaciones, el establecimiento de los canales de radio utilizados y cambios de frecuencias. Finalmente, establece la ligación entre el móvil y el *Mobile Service Switching Center* (MSC), el corazón del sistema GSM.

El MSC, como ya fue referido, es el centro de la red, a través del que es hecha la ligación entre una llamada realizada de un móvil hacía las otras redes fijas (las analógicas PSTN o digitales ISDN) o móviles. El nudo en el que se encuentra posee además una serie de equipos destinados a controlar varias funciones, como el cobro del servicio, la seguridad que estaría controlada por el mecanismo que provee el sistema inteligente y el envío de mensajes SMS.

El *Home Location Register* (HLR) contiene toda la información administrativa sobre el cliente del servicio y la localización actual del terminal. Es a través del HLR que la red verifica si un móvil que se intenta ligar posee un contrato de servicio válido. Si la respuesta es afirmativa el MSC envía un

mensaje de vuelta al terminal informándole que está autorizado a utilizar la red. El nombre de la operadora aparece en pantalla, informando que se puede efectuar y recibir llamadas. Cuando el MSC recibe una llamada destinada a un móvil él va al HLR verificar la localización. Paralelamente, el terminal de tiempos a tiempos envía un mensaje para la red, para informarla del sitio donde se encuentra (este proceso es denominado polling).

El *Visitor Location Register* (VLR) es utilizado para controlar el tipo de conexiones que un terminal puede hacer. Por ejemplo, si un utilizador posee restricciones en las llamadas internacionales el VLR impide que estas sean hechas, bloqueándolas y enviando un mensaje de vuelta al teléfono móvil informando el utilizador.

El *Equipment Identity Register* (EIR) y el *Authentication Center* (AC) son utilizados ambos para garantizar la seguridad del sistema y es un mecanismo muy bueno pero podría funcionar de mejor forma con la adaptación del mecanismo inteligente ya que el EIR posee una lista de IMEI de terminales que han sido declarados como robados o que no son compatibles con la red GSM. Si el teléfono móvil está en esa lista negra, el EIR no permite que se conecte a la red. Dentro del AC hay una copia del código de seguridad del SIM. Cuando ocurre la autorización el AC genera un número aleatorio que es enviado para el móvil. Los dos aparatos, de seguida, utilizan ese número, junto al código del SIM y un algoritmo de encriptación denominado A3, para crear otro número que es enviado de nuevo para el AC. Si el número enviado por el terminal es igual al calculado por el AC, el utilizador es autorizado a usar la red.

Lo anterior sería totalmente funcional si los algoritmos de encripción que utiliza GSM fueran más confiables y no presentaran errores de diseño como ha

sido descrito en la sección de críticas a los aspectos de seguridad de las compañías de telecomunicaciones en Guatemala.

El *Short Message System Center* (SMSC) es responsable por generar los mensajes cortos de texto. Algunos equipos utilizados en redes GSM pueden adjuntar el recaudo de llamadas, la conexión a Internet, la caja de mensajes de voz, etc.

**Descripción del sistema inteligente**

El sistema inteligente como tal tiene un conjunto de tareas que se han indicado que realiza para brindar una mayor seguridad al sistema GSM, esto lo realiza debido a que este mecanismo inteligente debe de ser un sistema experto el cual estará diseñado para resolver problemas que normalmente son solucionados por expertos humanos en la rama de la autenticación y mediante esquemas propios que permitan la identificación de cada uno de los abonados que se encuentran activos, para que de esta forma el sistema experto tenga un razonamiento y aprendizaje automático para apoyar al sistema GSM actual en cuanto a la seguridad.

Este sistema experto como tal deberá ser alimentado de todas las formas posibles como estará activado un abonado, ya que existen algunos escenarios para los cuales el sistema experto deberá de responder tal como cuando un abonado es apagado por un período indefinido y luego es encendido, y no precisamente es encendido en el mismo lugar en donde fue apagado, otro escenario podría ser cuando cambia de BTS hacia otra BTS proceso denominado como handoff. Este y otros escenarios serían alimentados para el sistema experto, para que este provea de mayor seguridad conteniendo todos los hechos que suceden dentro del sistema telefónico para que de esta forma

cuando necesite enviar información hacia una red de datos no vaya a ser información adulterada la que se está transmitiendo. Debido a que el sistema experto como tal está sometido a un conjunto de hechos marcados claramente como sucesos que se dan o que no existen se aconseja que este sistema experto deba ser basado en reglas.

Entre los elementos que podemos describir que este sistema experto como tal debe de contener para su funcionalidad se encuentra los siguientes:

**Base del conocimiento**: en esta se almacenan los datos a partir de su concepción como objetos, relaciones y niveles de jerarquía marcados por la herencia. Cuando las premisas de algunas reglas coinciden, en su totalidad o en parte, con las conclusiones de otras, se produce lo que se llama un encadenamiento de reglas. Esto es lo que para este sistema se debe poner mucha atención, ya que de esta base de conocimientos que nosotros agreguemos a nuestro sistema saldrán las conclusiones que el sistema, como tal, tome con respecto de la realidad. Entre las reglas que podemos incluir dentro del sistema se encontrarían las que se muestran en la tabla III. Reglas del sistema experto.

Tabla III. Reglas del sistema experto

| Regla No. | Descripción |
|---|---|
| 1 | **Si** no señal abonado **entonces** registrar apagado |
| 2 | **Si** cambio posición abonado **entonces** regla 3 |
| 3 | **Si** abonado no esta en área cobertura **entonces** handoff |
| 4 | **Si** señal abonado **entonces** registrar encendido |
| 5 | **Si** abonado encendido **entonces** registrar posición |
| 6 | **Si** regla 5 **Y** IMEI coincide con SIM **entonces** agregar a la red **Sino** reconocimos a un Pirata en una posición |
| 7 | **Si** handoff **entonces** regla 5 |

**Motor de inferencias**: las reglas que se establecieron anteriormente sirven para obtener nuevos hechos o conclusiones a partir de verdades o hechos iniciales, ya que si el hecho representado por la premisa de una regla es cierto, el hecho representado por su conclusión también lo es. Se llamarán conclusiones simples a aquellas que resultan de la aplicación de solo una regla y conclusiones compuestas a las que resultan del encadenamiento de varias reglas. Tanto los hechos iniciales como los que resultan de la aplicación de las reglas forman el conocimiento concreto, que reside en la memoria de trabajo del sistema experto a desarrollar.

Algo muy importante de indicar en este nivel, es que para la obtención de conclusiones se utilizan diferentes tipos de estrategias de inferencia y control del razonamiento, así, para las simples existen dos estrategias: *modus ponens* y *modus tollens*. Pero debido a que el encadenamiento de dos o mas reglas no siempre conduce a obtener conclusiones, ya que puede o no conocerse la verdad o falsedad de las premisa estas pueden conducir a la no solución por

medio de reglas entonces se sugiere además de utilizar las dos estrategias indicadas determinar niveles de probabilidad que una premisa sea cierta o falsa y así podríamos decir que A implica a B con una probabilidad P(B/A) (probabilidad de B condicionada por A o probabilidad de B supuesto que A es cierta).

## 5.10. Desempeño que realiza la SIT en Guatemala en la seguridad de la transmisión de datos de las redes telefónicas a las redes de datos en cuanto a servicios

La Superintendencia de telecomunicaciones de Guatemala es la encargada de velar en el marco legal por las telecomunicaciones en nuestro país. La Superintendencia de telecomunicaciones se creó el 17 de octubre de 1996 a raíz de la promulgación por parte del Congreso de la República del Decreto 94-96 Ley General de Telecomunicaciones, el cual fue publicado en el Diario Oficial el 18 de Noviembre de 1996.

Tiene como finalidad apoyar y promover el desarrollo eficiente de las telecomunicaciones, estimular las inversiones en el sector, fomentar la competencia entre los diferentes prestadores de servicios de telecomunicaciones, proteger los derechos de los usuarios y de las empresas proveedoras de los servicios y apoyar el uso racional y eficiente de las frecuencias del espectro radioeléctrico.

La sit cumple con tareas específicas ya que desde la promulgación de la Ley General de Telecomunicaciones y creación de la Superintendencia de Telecomunicaciones, la apertura ofrecida al público para la utilización del recurso natural llamado Espectro Radioeléctrico, se han adjudicado derechos

de usufructo de ese bien por los métodos establecidos en la norma jurídica indicada, en más del 85% de su capacidad. Desde pequeños usuarios de radiocomunicaciones privadas hasta grandes empresas operadores de telefonía inalámbrica, conviven hoy explotando el recurso de frecuencias radioeléctricas, traduciéndose dicha actividad en servicios modernos de comunicación a precios razonables para los habitantes del país.

Se han identificado los siguientes servicios, prestados a usuarios finales: telefonía fija, a nivel metropolitano o departamental, telefonía fija interurbana, a nivel nacional, telefonía móvil, telefonía satelital, telefonía internacional, servicios ISDN (Red Digital Integrada), servicios ADSL, enlaces de transmisión de datos nacionales e internacionales, enlaces de acceso a Internet, proveedores de acceso a Internet, servicio de buscapersonas y radiocomunicaciones.

Cerca del 100% de las líneas telefónicas están conectadas a centrales digitales, asimismo, en su mayor parte los operadores utilizan técnica de transmisión digital para la provisión de los servicios de telefonía fija.

El servicio de telefonía satelital ha sido impulsado principalmente por el subsidio que el Fondetel ha brindado a algunas empresas que han asumido el riesgo de desarrollar telecomunicaciones en el interior del país, donde generalmente por la topografía y poca concentración de población no pudiera ser posible.

En cuanto al sector telefónico, actualmente el país cuenta con 843,766 líneas telefónicas fijas; 1,527,148 líneas móviles, de las cuales el 24% son a crédito y el 76% son prepago; 1,831 líneas satelitales; 7,523 teléfonos públicos de tarjeta y 38,621 teléfonos públicos monederos.

La Superintendencia de Telecomunicaciones SIT, desde su creación ha proporcionado todas las facilidades necesarias para el desarrollo adecuado de las telecomunicaciones en el país, por lo que puede considerarse que la demanda en ese tipo de servicio se encuentra satisfecha. Entonces en lo que respecta a las líneas de acción en el mediano plazo, estas consistirán en seguir proporcionado las facilidades mencionadas. A ello se puede agregar las siguientes acciones:

- Participación activa en las rondas de negociaciones de tratados internacionales que involucren las telecomunicaciones.
- Seguimiento al control de calidad de los servicios de telecomunicaciones
- Implementación de los mecanismos promulgados por el Congreso de la República para contrarrestar el robo de teléfonos celulares.
- Realización de subastas de frecuencias directas
- Monitoreo para la verificación del uso correcto de las frecuencias del espectro radioeléctrico, en todo el país.
- Administración del Plan de Numeración y la asignación de números a los diferentes operadores.

La SIT administrará y supervisará los rangos de ondas radioeléctricas asignadas a servicios de comunicación satelital que sean usados para enlaces hacia o desde el exterior del territorio de Guatemala, en las condiciones vigentes de conformidad con los acuerdos y tratados respectivos aprobados en el seno de la UIT. Así mismo la SIT es la encargada de velar para que toda compañía que adquiera frecuencias y derechos de retransmisión cuente con el equipo más adecuado para que los servicios que presten cumplan con las condiciones mínimas de confiabilidad y calidad, para que con ello garantice la calidad de los servicios.

**Apoyo por parte de la SIT contra las interferencias premeditadas**

La superintendencia de telecomunicaciones de Guatemala proporciona apoyo considerable, en el sentido de que ante cualquier ataque derivado de cualquier forma de interferencia de una entidad ajena hacia la transmisión de información que se lleve a cabo por medio de una empresa que está registrada en la SIT para el uso de una frecuencia registrada ante este organismo, la empresa registrada se ve protegida por el artículo 53 de la Ley General de Telecomunicaciones, esta indica qué

**ARTICULO 53**. **Protección contra interferencias**. Las personas individuales o jurídicas que posean títulos de usufructo de frecuencias y que en algún momento sufran interferencias radioeléctricas, podrán denunciarlas a la Superintendencia, proporcionándole un informe técnico emitido por una entidad acreditada por la misma para la supervisión del uso del espectro radioeléctrico. Las disposiciones internas de la Superintendencia determinarán la forma en que se acreditará a las entidades supervisoras del espectro radioeléctrico. La Superintendencia notificará la denuncia al presunto causante de la interferencia, quien en un plazo no mayor de diez (10) días de haber sido notificado, expondrá los hechos y aportará las pruebas que considere oportunas. Entre ellas deberá incluir un informe técnico emitido por una entidad acreditada para la supervisión del uso del espectro radioeléctrico.

Transcurrido el plazo anterior, la Superintendencia con los informes técnicos respectivos, deberá pronunciarse dentro del plazo de diez (10) días contados a partir de la fecha en que el presunto causante presentó sus pruebas. Si en la resolución que emita la Superintendencia se determina que subsisten o se repiten las violaciones al derecho de uso o usufructo del espectro, el o los

infractores, deberán suspender los hechos que motivan la interferencia y pagar las multas que fije la Superintendencia, de acuerdo a lo estipulado en esta ley.

La parte afectada por la interferencia podrá ejercer contra el infractor las acciones judiciales por daños y perjuicios u otros que puedan corresponderle. Lo que la Superintendencia resuelva en cuanto a sanciones se sujetará a los recursos administrativos y judiciales que determina esta ley. Las interferencias de trascendencia internacional, quedarán sujetas a lo establecido en los acuerdos, tratados y convenios internacionales sobre la materia ratificados por el Gobierno de Guatemala.

Por lo que, de acuerdo con lo indicado, esta ley lo que realiza alguien sobre una frecuencia que le pertenece a una empresa que haya la adquirido y que tenga el documento de usufructo que lo ampara pues puede proceder legalmente tal y como lo indica el tercer párrafo de esta ley con lo cual la transmisión de datos de las redes telefónicas hacia las redes de datos y viceversa se ven también protegidas por este artículo ya que al estar trabajando con una compañía de telefonía en nuestro país tal como PCS de telgua, Comcel, Telefónica o Bell South. Que son compañías que poseen este titulo de usufructo y que están registradas en la SIT en el inventario de frecuencias reservadas en Guatemala y quien interfiera sobre alguna de estas frecuencias se vera penado por la ley. Con esto podemos analizar que la Superintendencia de Guatemala nos protege contra las interferencias especialmente podemos indicar que tenemos el apoyo de esta institución para cuando transmitimos información que tiene mucha importancia para nosotros.

**Multas que impone la SIT**

De acuerdo a los reglamentos que impone la SIT como entidad reguladora de las comunicaciones a nivel guatemalteco, establece una serie de

multas para toda aquella entidad que infrinja sobre los aspectos que se establecen en el artículo 81 de la Ley General de Telecomunicaciones la cual establece lo siguiente:

**ARTICULO 81. Infracciones y multas**. Se establecen las infracciones y multas siguientes:

1. Multa de 1000 a 10000 UMAs por:
    a) Usar las bandas de frecuencias para radioaficionados en contra de lo estipulado en esta ley.
    b) Causar interferencias comprobadas.
    c) Desconectar ilegalmente a otro operador.
    d) No realizar el registro en cualquiera de los casos establecidos por la ley.

2. Multa de 10001 a 100000 UMAs por:
    a) Evitar el acceso a los recursos esenciales de acuerdo a esta ley.
    b) Utilizar las bandas de frecuencias reguladas o reservadas sin la obtención previa del derecho de usufructo o del derecho de uso, respectivamente.
    c) Cometer cualquiera de las infracciones establecidas en el numeral 1 reincidente o habitualmente.
    d) Interconectarse a una red de telecomunicaciones, sin la autorización o el consentimiento del operador de la red.
    e) Alterar los datos necesarios para cobrar debidamente el acceso a recursos esenciales.

3. La reincidencia en cualquiera de las infracciones establecidas en el numeral 2, será sancionada con la multa máxima establecida.

La aplicación de cualquier sanción económica establecida en esta ley se hará sin perjuicio de deducir las responsabilidades penales y civiles que pudieran corresponder.

Estas son las multas que se establecen por parte de la sit para aquellos que se les halle que están interrumpiendo o interfiriendo sobre las frecuencias que no tienen el derecho de uso.

# CONCLUSIONES

1. La información que se transmite por medio de las redes de datos han presentado mayor seguridad que la información que se transmite por medio de las redes telefónicas celulares, ya que en las redes de datos la encripción de la información ha sido un proceso evolutivo que ha alcanzado un nivel de madurez que es efectivo actualmente.

2. La problemática de interferencia del sistema análogo/digital investigado tiene dos tipos de interferencia más pronunciados para Guatemala, que son la interferencia por co canal y la de canal adyacente, que en general son los dos tipos de interferencia más frecuentes en los sistemas análogos, tales como los que utiliza Comcel ésta es la única compañía de telecomunicaciones en Guatemala que posee una integración de un sistema análogo/digital.

3. En interferencia de sistemas digitales las diferencias fundamentales existen en el eco producido en el bucle local de la PSTN (eco de red) y el generado en aparatos móviles digitales (eco de diafonía estática) que exigen métodos diferentes para suprimirlo.

4. GSM es un protocolo estándar europeo con mucha aceptación a nivel mundial en las telecomunicaciones, pero para que sea completamente seguro debe poseer un valor agregado que garantice la seguridad, se debería considerar un cambio sobre el protocolo a nivel mundial ya que si solo algunos cambian a su modo entonces dejaría de ser un estándar.

5. Sobre las redes de datos existen un conjunto de mecanismos que colaboran para que la información que se transmite sobre esta red sea bastante segura, es más difícil que intenten interferir la comunicación dentro de este tipo de red que a través de una red telefónica celular que presenta algunos defectos estructurales de diseño.

6. La Superintendencia de Telecomunicaciones de Guatemala SIT se encarga principalmente de regular todos los tipos de comunicaciones por medios que involucran el espectro guatemalteco, éstos investigan anomalías de interferencias y actúan con respecto a la ley.

# RECOMENDACIONES

1. El sistema que actualmente presentan las telecomunicaciones como forma de interactuar con las redes de datos representa una fuente de la cual se pueden aprovechar muchos recursos con lo que se puede orientar hacia el sector comercial y financiero de la industria bancaria guatemalteca como un buen complemento para efectuar pagos por medio de teléfonos celulares.

2. La forma como interactúan las redes de datos y las redes telefónicas muestran un esquema en el cual se puede garantizar de una mejor forma la seguridad entre ambos tipos de redes para que cuando se realicen transacciones de un tipo de red hacia otra no sea vulnerable en el proceso de cambio de un tipo de red hacia otra.

3. La seguridad que se presenta sobre la integridad de la información es algo que siempre se ha considerado como muy valioso ya que a nadie le interesa que alguien ajeno al destino de un mensaje se entere de la información que está manipulando. Por lo que el aumento de la seguridad sobre las redes telefónicas celulares es algo importante.

4. Usar como estándar al GSM es una tarea que las empresas de telecomunicaciones deben considerar para la compatibilidad de los equipos involucrados en este tipo de tecnología por lo que al aumentar la seguridad a este sistema se debería de considerar una estandarización completa para mantener la compatibilidad.

# BIBLIOGRAFÍA


1. www.red.com.mx, Protocolos de comunicaciones, 2 de septiembre 2004

2. www1.monografias.com/Teleinf.htm, Bases de la Teleinformática, 12 de septiembre 2004

3. www.monografías.com/trabajos/ perifericos / perifericos.shtml, Perifericos, 25 de septiembre de 2004

4. www.aui.es/i99/prensa/nov_red_zeus.htm, Red Zeus, 3 de octubre 2004

5. www.atstake.com/research/reports/acrobat/atstake_gprs_security.pdf, Gestion de Seguridad, 8 de octubre 2004

6. wmatem.eis.uva.es/~ignfar/crypto.html, Criptología, 8 de octubre 2004

7. Menezes, A. J., van Oorschot, **P. C. Handbook of applied cryptography**. Editorial Vanstone, S. A., 2001

8. Moya Huidobro, José Manuel. **Fundamentos de Telecomunicaciones**. Editorial Paraninfo, 1997

9. Castro Lechtler, Ricardo y Rubén Jorge Fusario, **Teleinformática para Ingenieros en Sistemas de Información**. Editorial Reverté, 1998

10. A.S. Tanenbaum. **Computer Network**. 3ª Edición. Prentice Hall, 1998

11. **Telefonía Móvil Digital GSM**. Área de Ingeniería Telemática. Departamento de Comunicaciones. Universidad Politécnica de Valencia.

12. **Superintendencia de Telecomunicaciones, Ley General de Telecomunicaciones de Guatemala incluye modificaciones por la sentencia del 8 de junio de 1998 de la Corte de Constitucionalidad:** Guatemala 1996. pp.14,22.