



**INSTITUTO POLITÉCNICO NACIONAL  
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA  
UNIDAD PROFESIONAL “CULHUACAN”**



**“PROYECTO DE RED CELULAR DE TERCERA  
GENERACIÓN CDMA2000 PARA ACCESO A INTERNET  
(PDSN)”**

**QUE PARA OBTENER EL TITULO DE:  
INGENIERO EN COMUNICACIONES Y ELECTRÓNICA**

**P R E S E N T A  
José Andrés Segoviano Ochoa**

**A S E S O R E S  
Ing. Carlos León Castro Noriega  
Ing. Felipe Cruz Bautista**

**MEXICO, D.F 23 DE SEPTIEMBRE 2009**

**INSTITUTO POLITÉCNICO NACIONAL  
ESCUELA SUPERIOR DE INGENIERIA MECANICA Y ELECTRICA  
UNIDAD CULHUACAN**

**TESIS INDIVIDUAL**

Que como prueba escrita de su Examen Profesional para obtener el Título de Ingeniero en Comunicaciones y Electrónica que deberá desarrollar el C.

**JOSÉ ANDRÉS SEGOVIANO OCHOA**

**“PROYECTO DE RED CELULAR DE TERCERA GENERACIÓN CDMA2000 PARA ACCESO A INTERNET (PDSN)”**

Con este trabajo se pretende dar una perspectiva real de lo que es la implementación del servicio de paquetes de datos en una red celular de tercera generación CDMA2000. Para explicar concisa y detalladamente los principales conceptos, la arquitectura y el funcionamiento de dicha conmutación de paquetes para el acceso a Internet, se tomará como punto base el equipo encargado de dar este servicio, es decir, el Nodo de Servicio de paquetes de Datos (PDSN por sus siglas en inglés). Se pretende que este trabajo sea de gran ayuda para aquellos lectores que estén interesados en el tema y puedan tener una referencia práctica de dichas implementaciones de red en campo.

**CAPITULADO**

- I.- TECNOLOGIAS INALAMBRICAS DE BANDA ANCHA
- II.- ASPECTOS DE REDES (NETWORKING)
- III.- ARQUITECTURA DE UNA RED CELULAR 3G  
CDMA 2000
- IV.- ARQUITECTURA Y FUNCIONAMIENTO DEL PDSN9660
- V.- IMPLANTACIÓN Y PUESTA EN FUNCIONAMIENTO  
DEL PDSN9660 EN UN PROYECTO DE CDMA2000 A 450 MHZ (PROYECTO  
CDMA450)

México D. F., a 29 de julio de 2009

**PRIMER ASESOR:**



\_\_\_\_\_  
ING. CARLOS LEÓN CASTRO NORIEGA

**SEGUNDO ASESOR:**



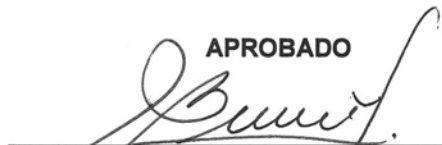
\_\_\_\_\_  
ING. FELIPE CRUZ BAUTISTA

**Vo. Bo.**



\_\_\_\_\_  
ING. IGNACIO MONROY OSTRÍA  
JEFE DE LA CARRERA DE I.C.E.

**APROBADO**



\_\_\_\_\_  
M. en C. HÉCTOR BECERRIL MENDOZA  
SUBDIRECTOR ACADÉMICO

# **AGRADECIMIENTOS**

**Este trabajo es la compilación de horas de esfuerzo y sacrificios, pero si algo he aprendido a lo largo de mi vida es que el que persevera alcanza y siempre las recompensas finales valen la pena.**

**Quiero agradecer en primer lugar a Dios por siempre estar conmigo en las buenas y en las malas a lo largo de toda mi vida.**

**A mis padres por su apoyo y confianza incondicional hacia mi, ellos me han enseñado que la constancia, la perseverancia y el amor por lo que uno hace siempre harán que cualquier persona cumpla sus sueños y metas fácilmente, también les agradezco a ellos el siempre estar siempre ahí cuando los necesito, no cabe duda que soy una persona sumamente afortunada al tener los padres que tengo ya que sin sus sabias palabras y consejos probablemente no estaría escribiendo estas líneas.**

**También quisiera agradecer a mi novia Luz que sin duda fue de gran ayuda en la traducción y corrección de muchos de los textos que fueron base para este trabajo, sin su apoyo incondicional durante todo este proceso, todo esto hubiera sido mucho mas prolongado y no tan excelentemente bien hecho.**

**A mi hermana, mis primos y a mis amigos, que siempre me han escuchado y ayudado en todo momento, encontrar personas así en tu vida ayuda enormemente a definir nuevas metas, objetivos y nuevos sueños así como también el sobrellevar muchas perdidas y desilusiones.**

**Por últimos agradezco la ayuda brindada por mis asesores de tesis los cuales pacientemente ayudaron a que definiera el camino que tendría este trabajo, así como las largas horas que me brindaron de ayuda para la realización de este trabajo.**

**A todos ustedes Gracias  
José Andrés Segoviano Ochoa**

## OBJETIVOS GENERALES

Explicar lo más detallada y concisamente posible como es que se da acceso a Internet en una red de tercera generación tipo CDMA2000. Esto se pretende lograr teniendo como eje central en este trabajo el PDSN cuya principal función es precisamente unir la Red de Paquetes de Datos (PDN por sus siglas en inglés) con la red inalámbrica celular CDMA2000 estando este equipo ubicado dentro de la red de conmutación de paquetes (PS por las siglas en inglés de Packet Switching).

De igual forma se busca complementar la teoría con un caso práctico real llevado a cabo en una de las empresas de telecomunicaciones más importante del país usando esta tecnología

## OBJETIVOS PARTICULARES

- Explicar de manera general y breve las distintas tecnologías inalámbricas de Banda Ancha que dan acceso a la Red de Paquetes de Datos (Internet) para tener una mayor visión de lo que existe hoy en día en el mercado en este rubro.
- Explicar los conceptos de Redes de Datos (Networking) fundamentales para poder entender la arquitectura y el funcionamiento del proyecto final.
- Describir de manera mas particular la arquitectura de la red CDMA2000
- Estudio y análisis de:
  1. Las interfaces que comparte el PDSN dentro de la red de conmutación de paquetes.
  2. Hardware y software del PDSN.
  3. Principales funciones del PDSN en la red CDMA2000
- Dar un ejemplo práctico para que el lector pueda comparar la teoría y verifique el uso de la misma en una implementación de campo real.

# JUSTIFICACIÓN

El trabajo presenta una descripción detallada de la arquitectura, interfaces y funcionamiento del PDSN, equipo clave en la red de conmutación de paquetes dentro de CDMA2000 para poder así describir como se da acceso a Internet en una red de este tipo implantada en México para Telefonía rural por parte de uno de los proveedores de servicios de telefonía mas importantes en nuestro país.

Es importante mencionar que durante los últimos años, el crecimiento continuo del número de usuarios en los sistemas de comunicaciones inalámbricos ha provocado una necesidad cada vez mayor de incrementar su capacidad. Con la llegada inminente de la técnica de acceso al medio por división de códigos CDMA (del inglés Code Division Multiple Access) y la implantación de nuevos servicios de tercera generación se requieren elevadas tasas binarias de información.

La bibliografía relacionada con esta tecnología 3G es extensa, sin embargo hay que mencionar que la mayoría de esta no trata códigos de configuración, y mucho menos ilustran los equipos involucrados con sus respectivas propiedades y capacidades a detalle. Por ello, el trabajo pretende introducir a los ingenieros en comunicaciones en los aspectos prácticos llevados a cabo en la parte de acceso a Internet en CDMA2000.

El trabajo de tesis transmite al lector todos los elementos para la programación de los equipos involucrados, para así lograr que el usuario final goce de los servicios multimedia, con gran ancho de banda y fidelidad satisfactoria en sus comunicaciones.

El trabajo se basa en una implementación real llevada a cabo en el departamento de comunicaciones inalámbricas Huawei Technologies Co. Ltd. para la División de Telefonía rural y satelital de Teléfonos de México S.A. de C.V. (de ahora en adelante empresa proveedora y empresa cliente respectivamente).

De igual forma el último de los anexos lo dedico a dar un pequeño análisis socioeconómico del proyecto, esto con el fin de justificarlo desde el punto de vista de implicaciones, impactos y beneficios a la sociedad que este conlleva.

# INTRODUCCIÓN

Las redes celulares hoy en día dejan de ser exclusivas de la conmutación de circuitos para dar cabida a una nueva generación de conmutación, la de paquetes. Es decir, la llamada 3G en la telefonía celular ahora abre las puertas a una nueva gama de opciones en donde además de la voz, el usuario final puede desde su Terminal 3G acceder a toda una serie de nuevos servicios como: Internet a través de banda ancha, correo electrónico inalámbrico, videoconferencias, televisión digital (video streaming), radio digital, posición geográfica (GPS), entre muchas mas.

El mundo del siglo XXI exige cada vez más tecnologías de comunicación inalámbricas con mayor capacidad de transmisión y recepción y es aquí en donde la tecnología CDMA hace su aparición. CDMA resulta ser la mejor opción para las comunicaciones de voz y de datos con respecto a otras tecnologías comerciales móviles debido a que es una tecnología de "espectro ensanchado", es decir permite a muchos usuarios en una banda ocupar el mismo periodo de tiempo y la misma frecuencia.

Como su nombre lo indica, CDMA (la División de Código Múltiple Acceso) asigna códigos exclusivos para que los canales de comunicación puedan diferenciarse unos de otros en el mismo espectro. En un mundo donde el espectro es un recurso finito, CDMA resulta ser la plataforma base de las tecnologías 3G ya que permite que mucha gente pueda compartir mas el espectro. Las normas IMT-2000, CDMA2000 y WCDMA (UMTS), se basan en CDMA.

Para el propósito de este trabajo nos enfocaremos a la red CDMA2000 y mas específicamente al equipo PDSN para la parte del servicio de datos en esta red. Trataré de explicar concisa y brevemente como es proporcionado el servicio de datos (Internet) a los usuarios finales, siendo el PDSN el equipo de mayor relevancia ya que su funcionamiento principal es el de precisamente proporcionar acceso a Internet, intranets y servidores de aplicaciones para estaciones móviles en una red de este tipo.

El trabajo se dividió en 5 capítulos. Los primeros dos explican de manera detallada los conceptos necesarios para poder entender lo que es la banda ancha móvil y la red de paquetes de datos. Los siguientes dos capítulos explican ya de manera específica el funcionamiento y la arquitectura tanto de la red 3G CDMA2000 como la del PDSN9660 y finalmente el último capítulo explicara de manera práctica como fue montado y puesto a funcionar este equipo dentro de un proyecto real de CDMA a 450 Mhz

# CONTENIDO

|   |    |
|---|----|
| 1.- Tecnologías Inalámbricas de Banda Ancha                     |    |
| 1.1 Conceptos básicos   |    |
| 1.1.1 Concepto de telefonía celular.....                        | 1  |
| 1.1.2 Banda Ancha Inalámbrica.....                              | 4  |
| 1.1.3 Evolución de las redes móviles. Quadruple Play.....       | 5  |
| 1.2 Ejemplos de tecnologías inalámbricas de Banda Ancha         |    |
| 1.2.1 GSM-GPRS/UMTS.....  | 9  |
| 1.2.2 CDMA2000 1xEV-DO.....                                     | 11 |
| 1.2.3 Wi-Fi.....  | 12 |
| 1.2.4 WiMAX .....   | 15 |
| 2.- Aspectos de redes “Networking”                              |    |
| 2.1 Terminología de Networking                                  |    |
| 2.1.1 Redes de datos.....                                       | 17 |
| 2.1.2 Dispositivos de Networking.....                           | 19 |
| 2.1.3 Topología de red.....                                     | 24 |
| 2.1.4 Protocolos de red.....                                    | 25 |
| 2.1.5 Redes de área local (LAN).....                            | 26 |
| 2.1.6 Redes de área amplia (WAN).....                           | 27 |
| 2.1.7 Redes de área metropolitana (MAN).....                    | 28 |
| 2.1.8 Red Privada Virtual (VPN).....                            | 28 |
| 2.1.9 Redes internas y externas.....                            | 30 |
| 2.2 Modelos de Networking                                       |    |
| 2.2.1 Uso de capas para analizar problemas en un flujo.....     | 31 |
| 2.2.2 Uso de capas para describir la comunicación de datos..... | 32 |
| 2.2.3 Modelo OSI.....   | 33 |
| 2.2.4 Las capas del Modelo OSI.....                             | 34 |
| 2.2.5 Comunicaciones de par a par.....                          | 36 |
| 2.2.6 Modelo TCP/IP.....  | 37 |
| 2.2.7 Proceso detallado de encapsulamiento.....                 | 41 |
| 2.3 Medios Físicos de transmisión de datos                      |    |
| 2.3.1 El cableado de la red.....                                | 42 |
| 2.3.2 Redes LAN sin cableado.....                               | 46 |
| 2.3.3 Medios inalámbricos en las Redes WAN.....                 | 46 |
| 2.4 Dirección de Internet                                       |    |
| 2.4.1 Direccionamiento IP.....                                  | 47 |
| 2.4.2 Direcciones IP reservadas.....                            | 48 |
| 2.4.3 Introducción a la división de subredes.....               | 49 |
| 2.5 Mecanismos de la división de subredes                       |    |
| 2.5.1 Clases de direcciones IP de red.....                      | 51 |
| 2.5.2 Introducción y razones para realizar subredes.....        | 51 |
| 2.5.3 Como establecer la dirección de la mascara de subred..... | 52 |
| 2.5.4 Aplicación de la mascara de subred.....                   | 55 |
| 3.- Arquitectura de una red celular 3G CDMA2000                 |    |
| 3.1 Introducción.....   | 57 |
| 3.2 Técnicas y Tecnologías CDMA2000.....                        | 58 |
| 3.3 Arquitectura de la red CDMA2000.....                        | 65 |

|   |            |
|---|------------|
| 4.- Arquitectura y Funcionamiento del PDSN9660  |            |
| 4.1 El PDSN9660 en la Red CDMA2000.....   | 67         |
| 4.2 Normas y Protocolos seguidos por el PDSN9660.....   | 70         |
| 4.3 Arquitectura del sistema  |            |
| 4.3.1 Hardware.....   | 72         |
| 4.3.2 Software.....   | 75         |
| 4.4 Protocolos de Interfaces.....   | 76         |
| 4.5 Servicios y Funciones   |            |
| 4.5.1 Ruteo.....  | 77         |
| 4.5.2 Interfaz R-P estándar.....  | 78         |
| 4.5.3 IP simple e IP móvil.....   | 79         |
| 4.5.4 Agente Extranjero o Foráneo (FA).....   | 81         |
| 4.5.5 Contabilidad ó Tarificación (Accounting).....   | 81         |
| 4.5.6 PPS.....  | 82         |
| 4.5.7 VPN móvil.....  | 83         |
| 4.5.8 Seguridad.....  | 84         |
| 4.5.9 Calidad de Servicio (QoS).....  | 86         |
| 4.5.10 Múltiples tecnologías de compresión.....   | 86         |
| 4.5.11 Otros.....   | 86         |
| 5.- Implantación y puesta en funcionamiento del PDSN en un Proyecto real de CDMA a 450 Mhz (CDMA450)  |            |
| 5.1 Antecedentes del proyecto.....  | 87         |
| 5.2 Premisas de cobertura.....  | 88         |
| 5.3 Premisas de Ingeniería.....   | 88         |
| 5.4 Coberturas.....   | 88         |
| 5.5 Plataforma del sistema CDMA450.....   | 89         |
| 5.6 Conectividad del modulo PDSN en el proyecto CDMA450.....  | 90         |
| 5.7 Ubicación de los elementos de red.....  | 92         |
| 5.8 Instalación del PDSN en la central del cliente.....   | 93         |
| 5.9 Interconexión entre PDSN-RAC´s.....   | 95         |
| 5.10 Configuración del equipo PDSN  |            |
| 5.10.1 Cableado e instalación general del Hardware.....   | 98         |
| 5.10.2 Configuración LANSWITCH.....   | 99         |
| 5.10.3 Configuración FIREWALL.....  | 103        |
| 5.10.4 Configuración subgabinete de tarjetas.....   | 105        |
| 5.11 Puesta en funcionamiento del servicio de Internet en la Terminal FWT (teléfono Inalámbrico)..... | 110        |
| 6.- Acrónimos y Abreviaciones.....  | 115        |
| 7.- Conclusiones.....   | 119        |
| 8.- Bibliografía.....   | 120        |
| 9. Anexos   |            |
| A.1 Ubicación de los 18 RACs del proveedor .....  | 121        |
| A.2 Ubicación de las Terminales de Transporte Multi Servicio (ADM)....                                | 122        |
| A.3 Arquitectura de red GRAN-UTRAN.....   | 123        |
| <b>A.4 Impacto Socioeconómico del proyecto (Brecha Tecnológica)...</b>                                | <b>124</b> |



## Índice de figuras

|   |    |
|---|----|
| Figura 1.1 Resumen de las funcionalidades de cada generación.....         | 5  |
| Figura 1.2 Velocidad de datos en Japón .....                              | 6  |
| Figura 1.3 Sistema móvil XG .....   | 8  |
| Figura 1.4 Configuración PLMN básica en GSM/UMTS.....                     | 9  |
| Figura 1.5 Configuración red CDMA2000 .....                               | 11 |
| Figura 1.6 Componentes WIN con un solo HLR.....                           | 12 |
| Figura 1.7 Componentes de una red IEEE 802.11 .....                       | 13 |
| Figura 1.8 Configuración ad-hoc .....                                     | 13 |
| Figura 1.9 Topología con punto de acceso .....                            | 13 |
| Figura 1.10 Pila de protocolos IEEE 802.11 .....                          | 14 |
| Figura 1.11 Mar de islas digitales .....                                  | 14 |
| Figura 1.12 Arquitectura de red WiMAX .....                               | 15 |
| Figura 2.1 Redes de datos .....   | 17 |
| Figura 2.2 Redes de datos .....   | 17 |
| Figura 2.3 Red LAN .....  | 18 |
| Figura 2.4 Redes LAN insuficientes .....                                  | 18 |
| Figura 2.5 Interconexión de Redes LAN para dar origen a las Redes WAN.... | 19 |
| Figura 2.6 Dimensiones relativas de las LAN y las WAN .....               | 19 |
| Figura 2.7 Dispositivos de Networking .....                               | 20 |
| Figura 2.8 Dispositivos de Networking .....                               | 20 |
| Figura 2.9 Repetidor .....  | 21 |
| Figura 2.10 Puente .....  | 21 |
| Figura 2.11 Switch .....  | 21 |
| Figura 2.12 Router .....  | 22 |
| Figura 2.13 Firewall .....  | 22 |
| Figura 2.14 ACL .....   | 23 |
| Figura 2.15 Topologías físicas .....                                      | 24 |
| Figura 2.16 Combinación de Topologías físicas.....                        | 24 |
| Figura 2.17 Protocolos de red .....                                       | 25 |
| Figura 2.18 Funciones de la red LAN .....                                 | 26 |
| Figura 2.19 Funciones de la red WAN .....                                 | 27 |
| Figura 2.20 Redes de área Metropolitana MAN .....                         | 28 |
| Figura 2.21 Redes Privadas Virtuales .....                                | 29 |
| Figura 2.22 Arquitectura de las Redes Privadas Virtuales .....            | 29 |
| Figura 2.23 Redes internas y externas .....                               | 30 |
| Figura 2.24 Ejemplos de Flujo .....                                       | 31 |
| Figura 2.25 Comunicación Origen-Destino .....                             | 32 |
| Figura 2.26 Flujo de información de capa en capa .....                    | 32 |
| Figura 2.27 Modelo OSI .....  | 33 |
| Figura 2.28 Descripción de cada una de las capas del Modelo OSI .....     | 35 |
| Figura 2.29 Comunicación de par a par.....                                | 36 |
| Figura 2.30 PDUs de cada capa .....                                       | 36 |
| Figura 2.31 Capas del Modelo TCP/IP .....                                 | 38 |
| Figura 2.32 Protocolos comunes en el Modelo TCP/IP .....                  | 39 |
| Figura 2.33 Comparación gráfica del modelo OSI con el TCP/IP.....         | 39 |
| Figura 2.34 Protocolos TCP/IP y Ethernet en el Modelos OSI.....           | 40 |
| Figura 2.35 Pasos para encapsular los datos .....                         | 41 |
| Figura 2.36 Pasos para encapsular los datos .....                         | 41 |

|   |    |
|---|----|
| Figura 2.37 Cable UTP.....  | 42 |
| Figura 2.38 Conector RJ-45.....   | 43 |
| Figura 2.39 Cable Coaxial .....   | 44 |
| Figura 2.40 Conector BNC .....  | 44 |
| Figura 2.41 Cable de fibra óptica .....   | 45 |
| Figura 2.42 Conectores y adaptadores para la fibra óptica .....                                       | 45 |
| Figura 2.43 Ejemplos de direcciones en redes .....  | 47 |
| Figura 2.44 Secuencia de bits en una dirección IP .....   | 47 |
| Figura 2.45 Conversión binario-decimal .....  | 48 |
| Figura 2.46 Direcciones IP reservadas .....   | 48 |
| Figura 2.47 Direcciones IP reservadas .....   | 49 |
| Figura 2.48 Direcciones IP reservadas .....   | 49 |
| Figura 2.49 División de subred .....  | 50 |
| Figura 2.50 Administrador en la subred.....   | 50 |
| Figura 2.51 Relación de subredes por valor de ultimo octeto.....                                      | 50 |
| Figura 2.52 Clases de direcciones IP .....  | 51 |
| Figura 2.53 Cadenas de bits en las distintas clases de direcciones IP.....                            | 52 |
| Figura 2.54 Relación de bits prestados por hosts resultantes.....                                     | 52 |
| Figura 2.55 Relación de bits prestados por mascara de red .....                                       | 53 |
| Figura 2.56 Bits prestados .....  | 53 |
| Figura 2.57 Relación bits-mascara-hosts .....   | 54 |
| Figura 2.58 Ejemplo de subred .....   | 55 |
| Figura 2.59 Relación bits-mascara-hosts .....   | 55 |
| Figura 3.1 Rangos en la banda clase 5 en CDMA2000 .....   | 58 |
| Figura 3.2 Secuencia de código de 4 digitos WALSH .....   | 59 |
| Figura 3.3 Correlación en la ortogonalidad de la secuencia WLASH.....                                 | 59 |
| Figura 3.4 Inicialización del código WALSH .....  | 59 |
| Figura 3.5 Flujo de señal de CDMA.....  | 60 |
| Figura 3.6 Interleaving.....  | 60 |
| Figura 3.7 Scrambling.....  | 61 |
| Figura 3.8 Dispersión y Des-dispersión .....  | 62 |
| Figura 3.9 Principio del receptor RAKE .....  | 65 |
| Figura 3.10 Arquitectura de un sistema de red CDMA2000 .....  | 66 |
| Figura 4.1 Bosquejo del gabinete N68-22 (in mm) .....   | 72 |
| Figura 4.2 Configuración típica del gabinete PDSN9660 (1U=44.45mm) .....                              | 72 |
| Figura 4.3 Arreglo Tipico de tarjetas .....   | 73 |
| Figura 4.4 Arquitectura del software del PDSN9660 .....   | 75 |
| Figura 4.5 Interfaces del PDSN .....  | 76 |
| Figura 4.6 Pila de protocolos A11 .....   | 76 |
| Figura 4.7 Pila de protocolos A10 .....   | 76 |
| Figura 4.8 Pila de protocolos entre PDSN y AAA .....  | 77 |
| Figura 4.9 Interfaz entre PDSN y PDN .....  | 77 |
| Figura 4.10 Sistema de servicio de prepago del PDSN9660 .....   | 82 |
| Figura 4.11 El PDSN crea una VPN con GRE .....  | 84 |
| Figura 5.1 Arquitectura General del Sistema CDMA .....  | 90 |
| Figura 5.2 Conectividad del Módulo PDSN .....   | 92 |
| Figura 5.3 Flujo de instalación de Hardware del PDSN9660 .....  | 98 |
| Figura 5.4 Conexión de los cables PGND en el cuerpo del gabinete .....                                | 98 |
| Figura 5.5 Esquema eléctrico del gabinete PDSN9660. Cables al poner la tierra y la señalización ..... | 99 |

|   |     |
|---|-----|
| Figura 5.6 Estructura física del equipo .....   | 100 |
| Figura 5.7 Imagen real del equipo .....   | 100 |
| Figura 5.8 Panel delantero y trasero del Eudemon200 .....                               | 103 |
| Figura 5.9 Imagen real del equipo .....   | 103 |
| Figura 5.10 Cable para consola .....  | 105 |
| Figura 5.11 Tarjetas subastidor PDSN .....  | 105 |
| Figura 5.12 Terminales CDMA a 450 Mhz. tipo FWT .....                                   | 112 |
| Figura 5.13 Terminal CDMA tipo FWT conectada a la computadora con cable adaptador ..... | 112 |

### **Indice de tablas**

|   |    |
|---|----|
| Tabla 1.1 Descripción de las interfaces de UMTS .....                       | 10 |
| Tabla 2.1 Categorías UTP .....  | 43 |
| Tabla 2.2 Resumen de tipos de cables .....                                  | 45 |
| Tabla 5.1 Relación de RACs y Ancho de Banda calculado .....                 | 89 |
| Tabla 5.2 Comunicación del PDSN [Interfaces y Protocolos] .....             | 91 |
| Tabla 5.3 Números asignados por división .....                              | 96 |
| Tabla 5.4 Relación de VLAN .....  | 96 |
| Tabla 5.5 Relación de estas VLAN con su respectivo direccionamiento IP..... | 97 |



# CAPITULO 1

## Tecnologías inalámbricas de banda ancha

### 1.1 Conceptos Básicos

#### 1.1.1 Concepto de Telefonía Celular

Primero que nada hay que definir el concepto de célula en la telefonía inalámbrica. Una célula, es definida como el área geográfica donde una estación base esta prestando servicio a una estación móvil, delimitando el área en las que los canales o estaciones base están siendo usadas. Una estación móvil cuando se mueve de su celda de servicio hacia alguna celda vecina esta debe ser provista de suficientes recursos para que la comunicación no sea interrumpida. Dicho proceso es conocido como traspaso (handoff o handover en inglés). Un grupo de células por las que el espectro entero es compartido constituye un *cluster*, en otras palabras un cluster es la totalidad de los canales disponibles asignados a un conjunto de células

En una situación ideal, para la transmisión omnidireccional con antenas montadas en techos o partes altas, las estaciones móviles a la misma distancia de la estación base reciben el mismo poder de señal en todas las direcciones. En la práctica, el área cubierta difiere sustancialmente de las figuras geométricas idealizadas.

#### *JERARQUÍA CELULAR*

Las Megacélulas proveen cobertura a grandes áreas y son caracterizadas por células con un radio entre los 100 y 500 kilómetros.

Las macro células proveen cobertura a áreas grandes y son caracterizadas por células con alcance de hasta los 35 kilómetros.

Las Microcélulas proveen cobertura a áreas pequeñas y son caracterizadas por un alcance de hasta 1 kilómetro.

Las pico células proveen cobertura a áreas pequeñas y se caracterizan por tener un alcance de hasta 50 metros.

En el mundo real, mega, macro, micro y pico células coexisten en el mismo ambiente.



### *TRASPASO (HANDOFF O HANDOVER)*

El traspaso es definido como “el cambio de canales físicos involucrados en una llamada mientras se mantiene esta”. El traspaso constituye una técnica diversa usada para prevenir que las llamadas móviles no se conecten cuando las estaciones móviles experimentan una condición de radio degradada.

En las redes inalámbricas FDMA y TDMA el traspaso es “difícil” (hard handoff). En el traspaso difícil, la comunicación con la antigua estación base a través de un canal es discontinuada y se establece un nuevo canal de comunicación con la nueva estación base.

En las redes inalámbricas CDMA, que es nuestro caso de estudio, existen tres tipos de traspasos:

- 1) Traspaso fácil. (Soft Handoff): Es el proceso para establecer un enlace con un sector de una estación base X antes de romper el enlace con el sector de la estación base Y que esta dando el servicio
- 2) Traspaso más fácil (Softer Handoff): Como el traspaso fácil, pero el traspaso ocurre entre multi-sectores en la misma estación base
- 3) Traspaso difícil (Hard Handoff): El traspaso difícil ocurre cuando 2 sectores no se sincronizan o no están en la misma frecuencia. Interrupción en la voz o en los datos ocurre pero esto no interrumpe la comunicación del usuario

### *ACCESO MÚLTIPLE*

Los sistemas de comunicación inalámbricos son sistemas de multiuso en los que la información es transmitida por las ondas de radio. La señales múltiples pueden aislarse fácilmente una de otra usando algún procedimiento de programación en el cual las señales están permitidas para acceder a un medio dependiendo de un plan predefinido.

La coordinación de acceso puede ser llevada a cabo en diferentes dominios: el dominio de frecuencia, de tiempo, de código y de espacio.

#### **- Dominios de frecuencia**

Para un servicio de frecuencia, la banda es repartida en sub- bandas, cada una de las cuales es asignada a diferentes operadores de servicio. Cada una de estas bandas es dividida después en dos mitades, una para el enlace de envío y el otro para el enlace de recibo. Las subsecuentes divisiones son llevadas a cabo para formar las ranuras de frecuencia.

#### **- Dominio de Tiempo**

El aislamiento en el dominio de tiempo se completa permitiendo a la información el uso de la banda de frecuencia durante un periodo específico de tiempo.



- Dominio de Código

El aislamiento también puede ser completado asignando a cada señal un código diferente (una contraseña). El código es construido como una secuencia de símbolos que pertenecen a un alfabeto. En una situación ideal estos códigos no deben de presentar alguna correlación para que estos puedan discriminarse.

- Dominio de Espacio

El aislamiento en el dominio de espacio se puede llevar a cabo en dos dimensiones posibles: distancia y ángulo. Las señales que usan la misma frecuencia pero que son transmitidas por fuentes suficientemente alejadas una de otra, puede provocar interferencia.

- División de Frecuencia de Acceso Múltiple (FDMA por sus siglas en inglés)

La DFAM ciertamente es el método de acceso múltiple más convencional y fue la primera técnica empleada en aplicaciones inalámbricas modernas. En la DFAM el ancho de banda disponible se separa en un número igual de sub-bandas, cada una de las cuales constituye un canal físico. El canal de banda ancha es una función de los servicios que se proveerán y de la tecnología disponible.

- División de Tiempo de Acceso Múltiple (TDMA por sus siglas en inglés)

La DTAM es otra técnica de acceso múltiple, la cual reemplazó a la DFAM en aplicaciones inalámbricas modernas. Aquí, antes de la transmisión la información se mantiene guardada durante un periodo de tiempo conocido como *frame* (*marco*). Así, la transmisión ocurre con un intervalo de tiempo conocido como *slot*.

- División de Código de Acceso Múltiple (CDMA por sus siglas en inglés)

La DCAM es una técnica de acceso múltiple no convencional, sin embargo inmediatamente encontró aplicaciones en los sistemas inalámbricos. En DCAM, el ancho de banda entero está disponible simultáneamente para todas las señales, a cada una de ellas se les asigna un código en particular para diferenciarse una de otra.

- División de Espacio de Acceso Múltiple (SDMA)

La DEAM es una técnica de acceso múltiple no convencional, la cual encuentra su aplicación en los sistemas inalámbricos modernos generalmente combinados con otras técnicas de acceso múltiple. En DEAM, el ancho de banda entero está disponible simultáneamente para todas las señales. Las señales se discriminan espacialmente y la trayectoria de comunicación constituye el canal físico. La implementación de una arquitectura DEAM (SDMA) se basa fuertemente en la tecnología de antena inteligente en conjunción con técnicas avanzadas de proceso de señal digital.



## DUPLEXACIÓN

Los sistemas de comunicación inalámbrica han pasado por distintos pasos y etapas de control de acceso múltiple. Un sistema de comunicación dúplex (a dos caras) es un sistema integrado por dos partes o dispositivos conectados que pueden comunicarse el uno con el otro en ambas direcciones. La comunicación dúplex puede implementarse mediante un método de división de frecuencia, de tiempo, de código o de espacio.

### - División de Frecuencia Dúplex

En la división de frecuencia dúplex, los canales de envío y de recibo usan frecuencias separadas. Sin embargo, un canal dúplex por división de frecuencia es un escenario de 2 carriles, lo que constituyen los canales físicos.

### - División de Tiempo Dúplex

En la división de tiempo dúplex, los canales de envío y recibo comparten la misma banda de frecuencia pero ocupan esta banda por periodos donde no coinciden los tiempos, estos periodos se les llama ventanas. Así, un canal dúplex es un set de 2 ventanas que no coinciden en el mismo transporte de información y que constituyen el canal físico.

### - División de Código Dúplex

En la División de Código Dúplex, los canales de envío y de recibo simultáneamente comparten la misma banda de frecuencia pero se discriminan por códigos ortogonales. Por lo tanto un canal dúplex es en sí, un set de 2 códigos ortogonales sin un transporte de información, que constituyen el canal físico.

### - División de Espacio Dúplex

En la División de Espacio Dúplex, los canales de envío y de recibo comparten la misma banda de frecuencia, pero son discriminados en el espacio.

## 1.1.2 Banda Ancha inalámbrica

Vamos a llamar ancho de banda a la cantidad de de datos que pueden ser enviados o recibidos en una cantidad fija de tiempo. El ancho de banda existe como un rango dentro de un conjunto de frecuencias (de radio) o longitudes de onda (por la luz creada por el láser). Las computadoras y otros dispositivos digitales expresan el ancho de banda en bits por segundo (bps) o Bytes por segundo (Bps). Cuando se habla de lo analógico como la voz o la electricidad, el ancho de banda es referido en ciclos por segundo, o hertzios (Hz)

Por otro lado, podemos definir a la Banda Ancha como la plataforma de transmisión que tiene un ancho de banda suficiente para llevar múltiples datos, voz, y canales de vídeo a la vez. Cada uno de los canales individuales se transmite en una frecuencia

diferente a través del medio de transmisión y son seleccionados en el receptor. El espacio vacío en la gama de frecuencias que se encuentra entre los canales garantiza que los canales no interfieran unos con otros.

Así podemos definir a la Banda Ancha inalámbrica como el acercamiento de la experiencia de Banda Ancha en un contexto inalámbrico, que ofrece a los usuarios determinados beneficios y comodidades. Existen fundamentalmente dos tipos de servicios inalámbricos de Banda Ancha. El primer tipo trata de proporcionar un conjunto de servicios similares a los de la tradicional Banda Ancha en líneas fijas, pero utilizando como medio de transmisión, el aire, es decir una red inalámbrica. Este tipo de red puede ser pensado como una alternativa competitiva al módem DSL o por cable. El segundo tipo de banda ancha inalámbrica móvil, ofrece la funcionalidad adicional de la portabilidad, nomadicidad, y movilidad.

Entre la Banda Ancha inalámbrica fija podemos encontrar como ejemplos las redes Wi-Fi o de WiMAX fijo (Worldwide Interoperability for Microwave Access). Entre la Banda Ancha inalámbrica móvil podemos encontrar como ejemplos el WiMAX móvil o las redes celulares de UMTS y EVDO.

### 1.1.3 Evolución de redes móviles y servicios: “Quadruple Play”

Una nueva generación de tecnología móvil es marcada por un avance significativo en funcionalidad. Una propuesta muy común, es que la siguiente generación de sistemas móviles operará con tecnología de Internet combinada con múltiples tecnologías de accesos y correrán a velocidades entre 100Mbps en las redes celulares, hasta, 1Gbps en redes hot-spot.

#### LA EVOLUCIÓN DE REDES MÓVILES

Como antecedente, hay que decir que ha habido tres generaciones distintas de redes celulares móviles. Las primeras tres generaciones de redes móviles son definidas convencionalmente por interfaces de aire y tecnologías de transporte. No obstante, cada generación provee un incremento en funcionalidad al usuario móvil.

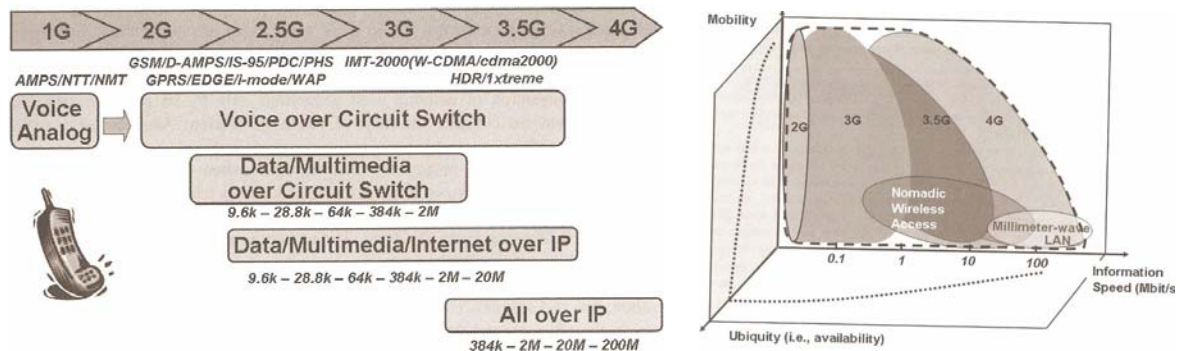


Figura 1.1 Resumen de las funcionalidades de cada generación.





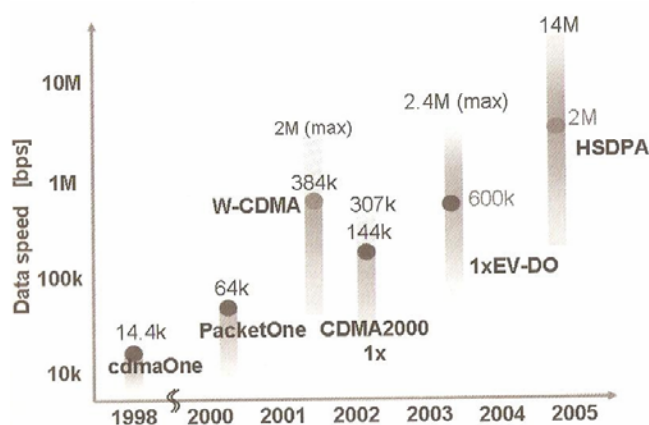
La Primera Generación (**1G**), está basada en tecnología celular análoga, como la American Mobile Phone Service en los Estados Unidos y la NTT en Japón. La tecnología de la Segunda Generación (**2G**) se basa en tecnología celular digital, los ejemplos comerciales de ésta son: Global System for Mobile Communications (GSM), la versión norteamericana del CDMA (IS-95) y el Personal Digital Cellular (PDC) en Japón.

Las redes de paquetes de servicio alterándose superpusieron hasta la mitad de la segunda generación. Generalmente, las redes de la 2G con servicio de paquete adicionados son conocidas como *redes móviles 2.5*. Estas redes móviles facilitaron las conexiones instantáneas en las cuales la información podía ser mandada y recibida casi inmediatamente y en las que no se necesitaba ninguna actividad de usuario para establecer la conexión.

La tercera generación (3G) se presentó en Octubre de 2001 cuando DoCoMo puso en marcha su red W-CDMA. La red móvil 3G se caracteriza por su habilidad para cargar datos a rangos más altos que 9.6 Kbps. La red permite una conexión a 384Kbps para bajar los datos y una velocidad de 64 Kbps en la conexión de circuitos, lo que es compatible con un N-ISDN. La red móvil 3G, provee un ancho de banda más grande y puede acomodar en esta nuevos servicios móviles como aplicaciones multimedia que no pueden ser proporcionadas por redes móviles 2.5.

### TENDENCIAS EN SERVICIOS MÓVILES

La expansión de las comunicaciones móviles ha rebasado el uso de la comunicación por voz, por lo tanto se espera un incremento en el uso de servicios multimedia. Para ejemplificar, me basaré en el caso de Japón, su mercado y sus tendencias. Japón es considerado por diferentes especialistas como un país que va dos o tres años adelante de otras regiones en el desarrollo de la tecnología 3G y es claramente el líder en el uso de Internet móvil. La figura 1.2 ilustra la velocidad de datos en este ejemplo



La figura 1.2 ilustra la velocidad de datos en Japón.



Los servicios móviles actuales de Japón son los siguientes:

Correo Electrónico: Un correo electrónico puede ser mandado a otro teléfono móvil o a cualquier persona que tenga una dirección de correo electrónico. Las terminales móviles son capaces de recibir correos electrónicos.

Navegación Web: en las redes 2.5G y 3G, es adoptado el estándar JPEG y es comúnmente usado con el estándar GIF. TFT muestra más de 260, 000 colores, 2.4 pulgadas, resolución de píxeles 240\*320 es comúnmente usado en terminales 2.5G y 3G, las cuales están creando una convergencia de contenido móvil y de contenido de Internet.

Servicios de ubicación: este servicio reparte a los usuarios una amplia gama de ubicaciones específicas en la Web. Reconoce 500 diferentes regiones, el sistema señala la ubicación de los suscriptores de acuerdo a su cercanía a la estación base y los provee de un contenido específico para esa área. La estimación de la ubicación depende del tamaño del celular y de su asociación con la estación base. La información de localización futura usará GPS y la información de red.

Aplicaciones JAVA: los teléfonos móviles más recientes son capaces de usar JAVA y capaces de correr aplicaciones de este tipo. Se espera que los teléfonos JAVA serán usados para servicios financieros y otros negocios a través del Internet, además de video juegos.

Descarga de video: este servicio 3G permite a los usuarios obtener contenido de video a velocidades de hasta 384 Kbps. Trailers de películas y archivos de música serán los contenidos principales que ofrece este servicio.

Correo multimedia: los servicios de correo con foto móvil han sido un suceso en Japón, un mail multimedia típico consiste en una foto personal o un contenido de video.

Video teléfono: el servicio de teléfono visual, es una aplicación típica de las redes 3G, este servicio utiliza un circuito de conexión de 64 Kbps.

En la próxima generación es muy poco probable que las comunicaciones móviles se limiten a crecer persona a persona, o por medio de comunicación multimedia, al contrario, el desarrollo de la telefonía celular se reflejará en una plataforma de herramientas diarias de vida. Esto esta ocurriendo por medio de interfaces como el IrDA, el bluethooth, IC y Identificación de Frecuencias de Radio (RFID).

De esta forma numerosas aplicaciones nuevas han estado apareciendo como, los servicios de seguridad del hogar, servicios de localización, máquinas vendedoras a control remoto y telemetría.

En un futuro, los artefactos capaces de comunicarse y los aparatos electrónicos domésticos formarán redes locales, las cuales operarán entre sí con las redes móviles globales. La evolución de cada generación en redes enriquece las aplicaciones móviles y estas aplicaciones brindan a las generaciones diferencias que las identifican.

Una red móvil XG será la red que remueva la brecha entre el mundo inalámbrico y el Internet en términos de conectividad y provee un súper conjunto de las utilidades que brinda el Internet a los usuarios. Esto se puede definir así:

**XG:** red móvil de servicios de Internet sin fisuras que remueve la brecha entre el mundo inalámbrico y el Internet y combina los aspectos positivos de los dos. Este sistema se ilustra en la figura 1.3

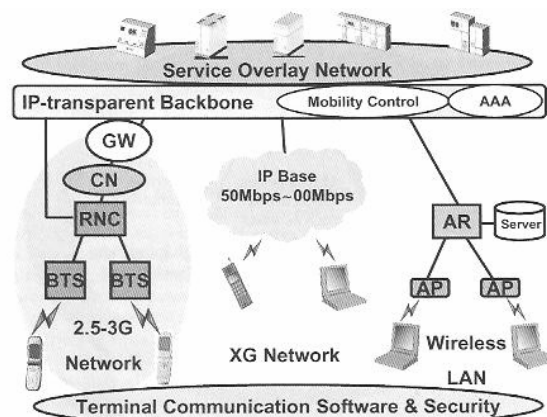


Figura 1.3. Sistema móvil XG

## 1.2 Ejemplos de tecnologías inalámbricas de Banda Ancha

Cuando los servicios de tercera generación 3G fueron inicialmente considerados, la meta era posibilitar un solo estándar de comunicación global que pudiera satisfacer las necesidades de comunicación en cualquier tiempo y lugar.

Una realización de IMT2000 es llamada *Universal Mobile Telecommunications System*, desarrollada bajo los patrones 3GPP. Este sistema envuelve desde la segunda generación GSM. La segunda versión del IMT2000 continúa siendo estandarizada bajo el 3GPP2 y es referida como el sistema CDMA2000 o 3GPP2. Este sistema toma desde la segunda generación IS-95.

Estos dos sistemas son similares en términos funcionales, particularmente desde el punto de vista del usuario. Sin embargo, usan tecnologías de acceso de radio bastante diferentes y difieren en sus detalles arquitectónicos, haciéndolas muy incompatibles.

## 1.2.1 GSM-GPRS/UMTS

### ARQUITECTURA DE RED

En este apartado hablaremos a la par de GSM-GPRS y UMTS, ambas arquitecturas son muy similares, de hecho el Core prácticamente no cambia, en la parte de acceso en GSM encontraremos que se denomina BSS y en UMTS es el RNS. 3GPP usa el término “tierras públicas de redes de telefonía móvil” (Public Land Mobile Network PLMN) para una red de tierras de telecomunicaciones. La infraestructura PLMN se divide lógicamente en accesos a red (AN) y una red central (CN). La siguiente figura muestra la arquitectura de PLMN (denominada para GSM) con la variante en acceso para el caso de UMTS. En el Anexo 1 se despliega un mejor esquema de la red GSM/UMTS con todo y pila de protocolos e interfaces.

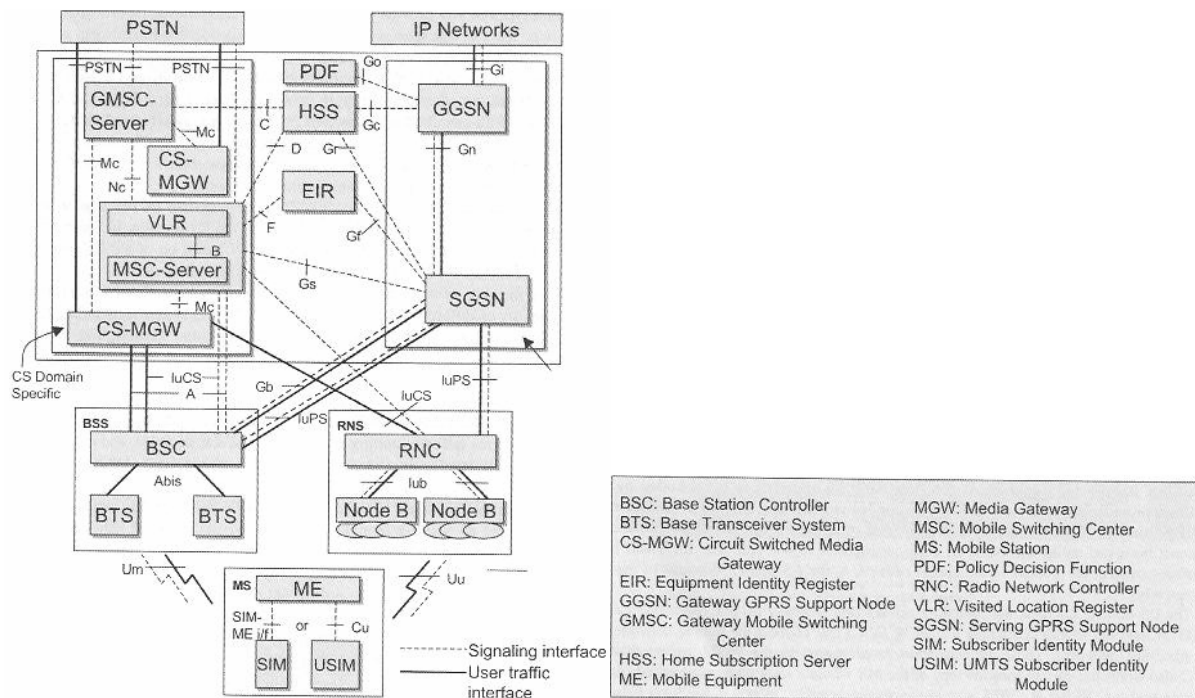


Figura 1.4: Configuración PLMN básica en GSM/UMTS

La Red Central (de ahora en adelante CN por sus siglas en ingles Core Network) consiste principalmente de un dominio de conmutación de circuitos (CS) y de un dominio de conmutación de paquete (PS). Estos dos dominios difieren en la forma en que manejan los datos. El dominio CS ofrece conmutación de circuitos para el tráfico de usuarios y es típicamente usado para servicios de tiempo real y de conversación, como servicios de voz y de videoconferencia. El dominio PS tiene como finalidad de principio a fin los servicios de paquete de datos como transferencia de archivos, navegación en Internet y correo electrónico.



La red central tiene una función lógica llamada *Home Subscriber Service (HSS)*, esta consiste en necesitar diferentes bases de datos para el sistema 3G, incluyendo el *Home Location Register (HLR)*, *Domain Name Service (DNS)*, e información de suscripción y seguridad. El manejo de red es provisto por el *Network Management Subsystem (NMS)*. La terminal del usuario es llamada estación móvil (*Mobile Station MS*), la cual lógicamente consiste de un equipo móvil. El RNC consiste de un controlador de red de radio que controla los recursos de radio en una red de acceso. El RNC realiza el proceso relacionado a la macrodiversidad y provee una transferencia fácil.

El dominio CS contiene los centros de cambio que conectan a la red móvil y las redes de línea fija. Estos son análogos para los intercambios en PSTN.

El dominio PS provee GPRS (General Packet Radio Service, por sus siglas en inglés), este dominio consiste de los nodos de apoyo del GPRS. Existen dos tipos de nodos de apoyo del GPRS: 1) nodo de soporte GPRS de entrada (Gateway GPRS Support Node GGSN) y 2) Nodo de soporte al servicio GPRS (Serving GPRS Support Node SGSN). El SGSN maneja el tráfico de datos del usuario, incluyendo funciones como la autenticación y autorización inicial, control de admisión, recolección de datos y cargos, manejo de radio, la portación de paquetes de creación, así como el manejo de movilidad y ruteo. El GGSN es frecuentemente localizado en el filo del dominio PS y maneja el tráfico del paquete de datos a la red UMTS de afuera hacia adentro y viceversa. Entre todos estos elementos funcionales, se define una serie de interfaces, la más característica de las cuales es la interfaz entre el equipo de usuario UF y los nodos B puesto que será la que defina la capacidad del acceso y el verdadero cuello de la botella de la red.

| Interfaz | Descripción                              |
|----------|--|
| Uu       | Interfaz entre el UE y el nodo B         |
| Iub      | Interfaz entre el nodo B y el RNC        |
| Iur      | Interfaz de conexión entre RNC distintos |
| Iu       | Interfaz entre RNC y UMSC                |

Tabla 1.1 Descripción de las interfaces de UMTS

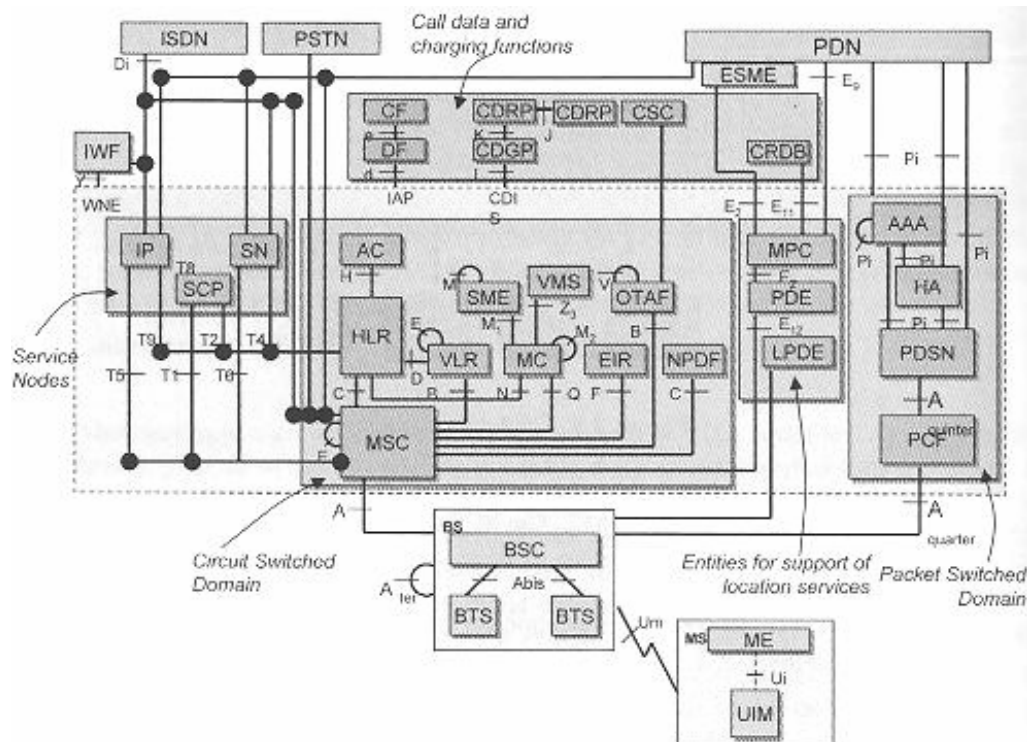
La interfaz Uu está basada en el acceso radio CDMA que presenta dos modos de funcionamiento (UTRA- FDD y UTRA –TDD) y en una nueva interfaz, la denominada IU, que conecta el subsistema de radio con la red de transporte.



## 1.2.2 CDMA2000 1xEV-DO

### ARQUITECTURA DE RED

Los sistemas CDMA2000 y el UMTS difieren marcadamente en como manejan la conmutación de tráfico de paquetes en el centro de la red. La siguiente figura representa la arquitectura estándar del diagrama fraccionado en diferentes dominios del CDMA2000. Aunque la arquitectura del CDMA2000 no es igual, este fraccionamiento hace la comparación con el UMTS más fácil.



- ISDN: Integrated Services Digital Network
- PSTN: Public Switched Telephone Network
- IWF: Interworking Function
- SCP: Service Control Points
- IP: Intelligent Peripherals
- SN: Service Nodes
- AC: Authentication Center
- HLR: Home Location Register
- MSC: Mobile Switching Center
- VLR: Visitor Location Register
- SME: Short Message Entity
- VMS: Voice Mail System
- OTAF: Over-The-Air Activation Function
- EIR: Equipment Identity Register
- BSC: Base Station Controller
- BTS: Base Transceiver Station
- ME: Mobile equipment
- UIM: User Identity Module
- AAA: Authentication, Authorization, and Accounting
- HA: Home Agent
- PDSN: Packet Data Service Node
- PCF: Packet Control Function

Figura 1.5 Configuración red CDMA2000

Para esta comparación con la arquitectura de red UMTS, se consideran dos dominios principales: Un dominio CS (que se encuentra en el centro de la figura que es idéntica a la conmutación de circuitos de la arquitectura celular del 2G) y un dominio PS. Así, las principales diferencias entre UMTS y CDMA2000 desde la perspectiva de la arquitectura recaen en el dominio PS. El segundo consiste en el paquete de control de función (PCF), nodo de apoyo de paquete de datos (PDSN) y en la autorización, autenticación y contabilidad (AAA).

La red de acceso desvía la conmutación de tráfico de paquete al PDSN. El PDSN termina el control de enlace lógico para todos los paquetes de datos y adicionalmente actúa como el agente externo o ruteador de acceso dependiendo de la configuración de red y si la red utiliza IPv4 o IPv6 para dar apoyo a la base IP móvil con *Mobile IP*. El PDSN también hace interfaz con el subsistema AAA para la realización de AAA para paquetes de acceso con HA y otro PDSN para apoyar la movilidad usando IP móvil.

Los servicios en el dominio CS en la arquitectura del CDMA2000 se basan en la Red Inalámbrica Inteligente (Wireless Intelligent Network WIN) (estándares TR-45.2 1997,2001). Como lo muestra la figura siguiente:

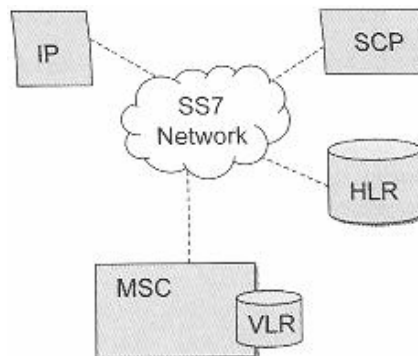


Figura 1.6 Componentes WIN con un solo HLR

### 1.2.3 Wireless LAN (Wi-Fi)

#### ARQUITECTURA

Una red 802.11 genérica está dividida en celdas llamadas BBS (Basic Service Set), que son zonas de cobertura gobernadas por una estación base o punto de acceso (AP Access Point). Para conseguir que los dispositivos de cada BBS puedan comunicarse entre sí, es necesario que los AP se conecten a través del sistema troncal de distribución (Distribution System). Esta es la estructura básica de una WLAN. Sin embargo, varios segmentos de esta se agrupan en una estructura jerárquica superior llamada ESS (Extended Service Set).

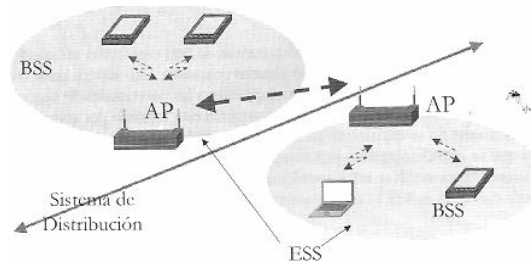


Figura 1.7 Componentes de una red IEEE 802.11

## TOPOLOGÍAS

En una red WLAN se pueden distinguir dos tipos de configuraciones diferentes, en función de que se utilicen puntos de acceso o no. La configuración más sencilla son las redes ad-hoc, también conocidas como configuración P2P (Peer-to-Peer), en las que las terminales móviles se comunican directamente empleando para ello una tarjeta adaptadora para comunicaciones inalámbricas. La única limitación es que los dispositivos se encuentren dentro de sus respectivas áreas de cobertura.

La otra alternativa deriva de la extensión del concepto de cobertura celular típico de las redes de telefonía móvil. En este caso, la estación base recibe el nombre de punto de acceso y hace las veces de repetidor inalámbrico. Un único punto de acceso puede soportar un pequeño grupo de usuarios.



Figura 1.8 Configuración ad-hoc

Otra posibilidad es conectar varios segmentos de red a través de un radio enlace. Estos enlaces pueden ser punto a punto o punto a multipunto. En el primer caso, se utilizan antenas directivas que, bien en RF o bien en la banda infrarroja, soportan el canal de comunicación entre los dos extremos. Por el contrario, en los enlaces punto a multipunto, las antenas tienen un ancho de haz mucho más amplio.

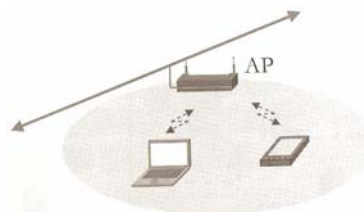


Figura 1.9 Topología con punto de acceso



## PILA DE PROTOCOLOS

El estándar 802.11, como cualquier protocolo 802.x, especifica los requisitos para el nivel físico y el subnivel de MAC.

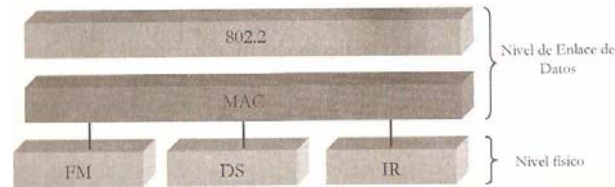


Figura 1.10 Pila de protocolos IEEE 802.11

Existen tres niveles físicos: FHSS en la banda de 2,4 GHz, DSSS también en la banda 2, 4GHz y el último en la banda infrarroja. Sobre el nivel físico, se encuentra el nivel de MAC, encargado de funciones tales como la fragmentación, el arbitrio del acceso al medio compartido o la retransmisión de paquetes.

## APLICACIONES

Además de las redes corporativas inalámbricas, la tecnología WLAN resulta muy adecuada en *hotspots*, lugares públicos de acceso a Internet basados en WiFi. Por otra parte, otra de las nuevas tendencias tecnológicas es la integración de voz y datos en una única infraestructura. Este tipo de aplicaciones también está gozando de gran éxito y todo parece indicar que la voz sobre WiFi nace de la conjunción de ambas.

## HOT SPOT

Un hotspot o isla digital es un área en la que existe conectividad inalámbrica basada en puntos de acceso WiFi y en la que se concentran cierto número de usuarios inalámbricos (aeropuertos, hoteles, centros comerciales) y se proporciona un servicio de acceso que, generalmente, es la conexión a Internet aunque existen otros como el acceso VPN a la red corporativa. La siguiente figura muestra una red de islas digitales en la que sus usuarios pueden conectarse todos con todos y con el exterior.

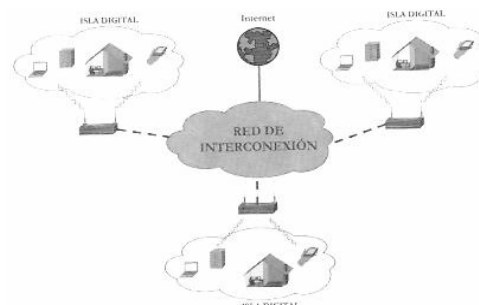


Figura1.11 Mar de islas digitales

## 1.2.4 WiMAX

WiMAX, acrónimo de Worldwide Interoperability for Microwave Access (Interoperabilidad Mundial para Acceso por Microondas), es una norma de transmisión por ondas de radio de última generación orientada al denominado bucle local inalámbrico (en inglés se utiliza el término "última milla" para delimitar el alcance de la comunicación inalámbrica) que permite la recepción de datos por microondas y retransmisión por ondas de radio (protocolo 802.16 MAN - Metropolitan Area NetWork, Red de Área Metropolitana) proporcionando acceso compartido con varios repetidores de señal superpuestos, ofreciendo total cobertura en áreas de hasta 48 Km. de radio y a velocidades de hasta 70 Mbps, utilizando tecnología que no requiere visión directa con las estaciones base (a diferencia de las microondas). WiMax es un concepto parecido a Wi-Fi pero con mayor cobertura y ancho de banda, se sitúa en un rango intermedio de cobertura entre las demás tecnologías de acceso de corto alcance y ofrece velocidades de banda ancha para un área metropolitana. La arquitectura de una red WiMAX se muestra en la siguiente figura:

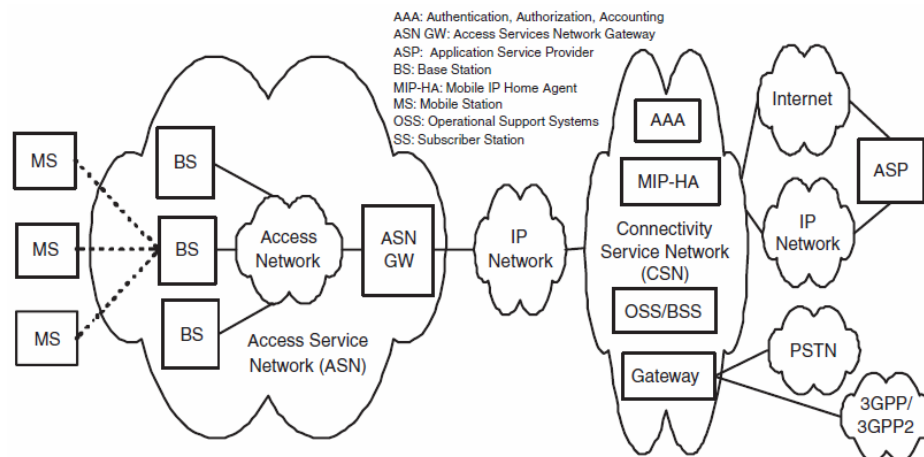


Figura1.12 Arquitectura de red WiMAX

### CARACTERÍSTICAS DE WiMAX

- Una característica importante del estándar es que define una capa MAC que soporta múltiples especificaciones físicas (PHY)
- Mayor productividad a rangos más distantes (hasta 50 km) alcanzando velocidades a esta distancia de 70 Mbps
  - Mejor tasa de bits/segundo/HZ en distancias largas
- Sistema escalable
  - Fácil adición de canales: maximiza las capacidades de las células.
  - Anchos de banda flexibles que permiten usar espectros licenciados y exentos de licencia



- Cobertura
  - Soporte de mallas basadas en estándares y antenas inteligentes.
  - Servicios de nivel diferenciados: E1/T1 para negocios, mejor esfuerzo para uso doméstico
- Coste y riesgo de investigación
  - Los equipos WiMAX-CertifiedFF (certificación de compatibilidad) permiten a los operadores comprar dispositivos de más de un vendedor

## ESTÁNDARES

Integra la familia de estándares IEEE 802.16 y el estándar HyperMAN del organismo de estandarización europeo ETSI. El estándar inicial 802.16 se encontraba en la banda de frecuencias de 10-66 GHz y requería torres con Línea De Vista (LOS por sus siglas en inglés). La nueva versión 802.16a, ratificada en marzo de 2003, utiliza una banda del espectro más estrecha y baja, de 2-11 GHz, facilitando su regulación. Además, como ventaja añadida, no requiere de torres donde exista enlaces del tipo LOS sino únicamente del despliegue de estaciones base (BS) formadas por antenas emisoras/receptoras con capacidad de dar servicio a unas 200 estaciones suscriptoras (SS) que pueden dar cobertura y servicio a edificios completos. Su instalación es muy sencilla y rápida (culminando el proceso en dos horas) y su precio competitivo en comparación con otras tecnologías de acceso inalámbrico como Wi-Fi: entre 5.000 euros y 25.000 euros.

Esta tecnología de acceso transforma las señales de voz y datos en ondas de radio dentro de la citada banda de frecuencias. Está basada en OFDM, y con 256 subportadoras puede cubrir un área de 48 km permitiendo la conexión sin línea vista, es decir, con obstáculos interpuestos, con capacidad para transmitir datos a una tasa de hasta 75 Mbps con una eficiencia espectral de 5.0 bps/Hz y dará soporte para miles de usuarios con una escalabilidad de canales de 1,5 MHz a 20 MHz. Este estándar soporta niveles de servicio (SLAs) y calidad de servicio (QoS).

### *WIBRO: IEEE 802.16e*

Lo que ocurría en la práctica es que pocos se atrevían a invertir en WiMAX bajo el único estándar aprobado hasta ahora, el 802.16d, que sólo sirve para aquellos terminales que están en un punto fijo.

El 7 de diciembre de 2005, el IEEE aprobó el estándar del WiMAX MÓVIL, el 802.16e, que permite utilizar este sistema de comunicaciones inalámbricas con terminales en movimiento. Muchos fabricantes de hardware y operadores estaban esperando a esta decisión para empezar a desplegar redes de WiMAX. Ahora ya diseñan infraestructuras mixtas fijo-móvil, que son mas “jugosas económicamente”. Esta iniciativa ha empezado sus despliegues comerciales en el 2006.

## CAPITULO 2

# Aspectos de redes “Networking”

### 2.1 Terminología de Networking

#### 2.1.1 Redes de datos

Las redes de datos se desarrollaron como consecuencia de aplicaciones comerciales diseñadas para microcomputadores. Por aquel entonces, los microcomputadores no estaban conectados entre sí como sí lo estaban las terminales de computadores *mainframe*, por lo cual no había una manera eficaz de compartir datos entre varios computadores. Se tornó evidente que el uso de disquetes para compartir datos no era un método eficaz ni económico para desarrollar la actividad empresarial. La red a pie creaba copias múltiples de los datos. Cada vez que se modificaba un archivo, había que volver a compartirlo con el resto de sus usuarios. Si dos usuarios modificaban el archivo, y luego intentaban compartirlo, se perdía alguno de los dos conjuntos de modificaciones. Las empresas necesitaban una solución que resolviera con éxito los tres problemas siguientes:

- Cómo evitar la duplicación de equipos informáticos y de otros recursos
- Cómo comunicarse con eficiencia
- Cómo configurar y administrar una red

Las empresas se dieron cuenta de que la tecnología de networking podía aumentar la productividad y ahorrar gastos. Las redes se agrandaron y extendieron casi con la misma rapidez con la que se lanzaban nuevas tecnologías y productos de red. A principios de la década de 1980 networking se expandió enormemente, aun cuando en sus inicios su desarrollo fue desorganizado.

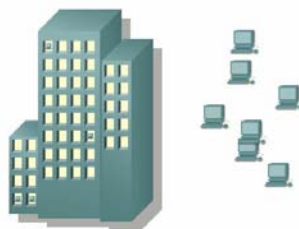


Figura 2.1 Redes de datos



Figura 2.2 Redes de datos

A mediados de la década de 1980, las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software distintas. Cada empresa dedicada a crear hardware y software para redes utilizaba sus propios estándares corporativos. Estos estándares individuales se desarrollaron como consecuencia de la competencia con otras empresas. Por lo tanto, muchas de las nuevas tecnologías no eran compatibles entre sí. Se tornó cada vez más difícil la comunicación entre redes que usaban distintas especificaciones. Esto a menudo obligaba a deshacerse de los equipos de la antigua red al implementar equipos de red nuevos.

Una de las primeras soluciones fue la creación de los estándares de Red de área local (LAN - Local Area Network, en inglés). Como los estándares LAN proporcionaban un conjunto abierto de pautas para la creación de hardware y software de red, se podrían compatibilizar los equipos provenientes de diferentes empresas. Esto permitía la estabilidad en la implementación de las LAN.

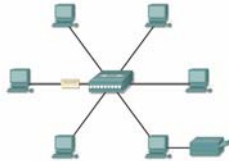


Figura 2.3 Red LAN

En un sistema LAN, cada departamento de la empresa era una especie de isla electrónica. A medida que el uso de los computadores en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes.

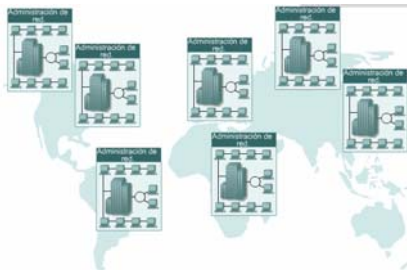


Figura 2.4 Redes LAN insuficientes

Lo que se necesitaba era una forma de que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa sino también de una empresa a otra. La solución fue la creación de redes de área metropolitana (MAN) y redes de área amplia (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, permitieron que las empresas se comunicaran entre sí a través de grandes distancias. La Figura resume las dimensiones relativas de las LAN y las WAN.

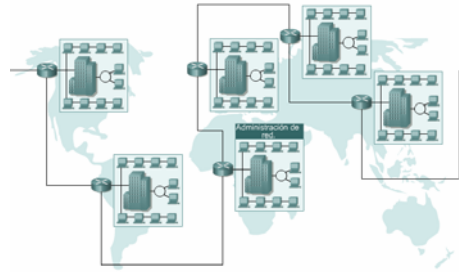


Figura 2.5 Interconexión de Redes LAN para dar origen a las Redes WAN

| Distancia entre las CPU    | Ubicación de las CPU                                  | Nombre   |
|----------------------------|---|--|
| 0.1 m                      | Placa de circuito impreso/Asistente personal de datos | Motherboard Red de área personal (PAN)                   |
| 1.0 m                      | Milímetro Mainframe                                   | Red del sistema de la computadora                        |
| 10 m                       | Habitación  | Red de área local (LAN) Su aula                          |
| 100 m                      | Edificio  | Red de área local (LAN) Su escuela                       |
| 1000 m = 1 km              | Campus  | Red de área local (LAN) Universidad de Stanford          |
| 100,000 m = 100 km         | País  | Red de área amplia (WAN) Cisco Systems, Inc.             |
| 1,000,000 m = 1,000 km     | Continente  | Red de área amplia (WAN) África                          |
| 10,000,000 m = 10,000 km   | Planeta   | Wide Area Network (WAN) The Internet                     |
| 100,000,000 m = 100,000 km | Earth-moon system                                     | Red de área amplia (WAN) Tierra y satélites artificiales |

Figura 2.6 Dimensiones relativas de las LAN y las WAN

## 2.1.2 Dispositivos de networking

Los equipos que se conectan de forma directa a un segmento de red se denominan dispositivos. Estos dispositivos se clasifican en dos grandes grupos. El primer grupo está compuesto por los dispositivos de usuario final. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás dispositivos que brindan servicios directamente al usuario. El segundo grupo está formado por los dispositivos de red. Los dispositivos de red son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

Los dispositivos de usuario final que conectan a los usuarios con la red también se conocen con el nombre de hosts. Estos dispositivos permiten a los usuarios compartir, crear y obtener información. Los dispositivos host pueden existir sin una red, pero sin la red las capacidades de los hosts se ven sumamente limitadas. Los dispositivos host están físicamente conectados con los medios de red mediante una tarjeta de interfaz de red (NIC). Utilizan esta conexión para realizar las tareas de

envío de correo electrónico, impresión de documentos, escaneado de imágenes o acceso a bases de datos. Un NIC es una placa de circuito impreso que se coloca en la ranura de expansión de un bus de la motherboard de un computador, o puede ser un dispositivo periférico. También se denomina adaptador de red. Las NIC para computadores portátiles o de mano por lo general tienen el tamaño de una tarjeta PCMCIA. Cada NIC individual tiene un código único, denominado dirección de control de acceso al medio (MAC). Esta dirección se utiliza para controlar la comunicación de datos para el host de la red. Hablaremos más sobre la dirección MAC más adelante. Tal como su nombre lo indica, la NIC controla el acceso del host al medio.

No existen símbolos estandarizados para los dispositivos de usuario final en la industria de networking. Son similares en apariencia a los dispositivos reales para permitir su fácil identificación.



Figura 2.7 Dispositivos de Networking

Los dispositivos de red son los que transportan los datos que deben transferirse entre dispositivos de usuario final. Los dispositivos de red proporcionan el tendido de las conexiones de cable, la concentración de conexiones, la conversión de los formatos de datos y la administración de transferencia de datos.

Algunos ejemplos de dispositivos que ejecutan estas funciones son los repetidores, hubs, puentes, switches y routers. Todos los dispositivos de red que aquí se mencionan, se tratarán con mayor detalle más adelante en el curso. Por ahora se brinda una breve descripción general de los dispositivos de networking.

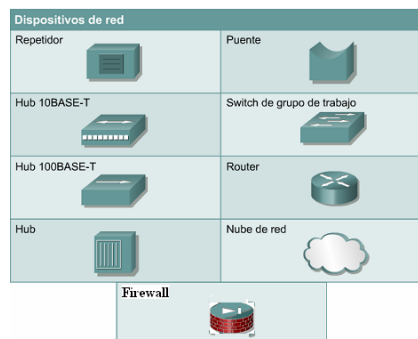


Figura 2.8 Dispositivos de Networking



Un repetidor es un dispositivo de red que se utiliza para regenerar una señal. Los repetidores regeneran señales analógicas o digitales que se distorsionan a causa de pérdidas en la transmisión producidas por la atenuación. Un repetidor no toma decisiones inteligentes acerca del envío de paquetes como lo hace un router o puente.

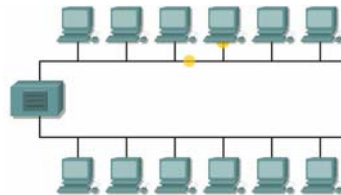


Figura 2.9 Repetidor

Los hubs concentran las conexiones. En otras palabras, permiten que la red trate un grupo de hosts como si fuera una sola unidad. Esto sucede de manera pasiva, sin interferir en la transmisión de datos. Los hubs activos no sólo concentran hosts, sino que además regeneran señales.

Los puentes convierten los formatos de transmisión de datos de la red además de realizar la administración básica de la transmisión de datos. Los puentes, tal como su nombre lo indica, proporcionan las conexiones entre LAN. Los puentes no sólo conectan las LAN, sino que además verifican los datos para determinar si les corresponde o no cruzar el puente. Esto aumenta la eficiencia de cada parte de la red.

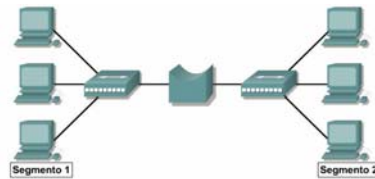


Figura 2.10 Puente

Los switches de grupos de trabajo agregan inteligencia a la administración de transferencia de datos. No sólo son capaces de determinar si los datos deben permanecer o no en una LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos. Otra diferencia entre un puente y un switch es que un switch no convierte formatos de transmisión de datos.

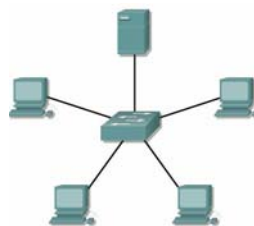


Figura 2.11 Switch



Los routers poseen todas las capacidades indicadas arriba. Los routers pueden regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias. Ninguno de los demás dispositivos puede proporcionar este tipo de conexión.

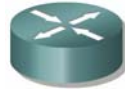


Figura 2.12 Router

Un firewall (o contrafuegos) es una estructura arquitectónica que existe entre el usuario y el mundo exterior para proteger la red interna de los intrusos. En la mayoría de los casos, los intrusos provienen de la Internet mundial y de las miles de redes remotas que interconecta. Normalmente, un firewall de red se compone de varias máquinas diferentes que funcionan al mismo tiempo para impedir el acceso no deseado e ilegal.

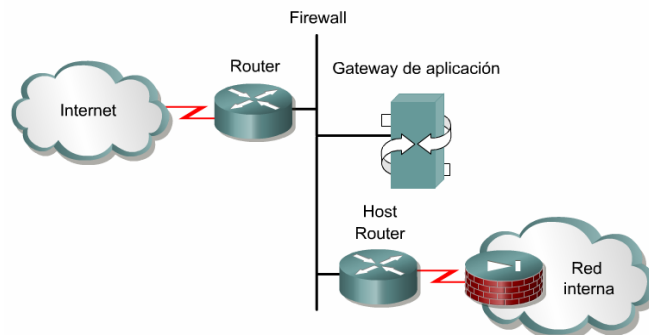


Figura 2.13 Firewall

En esta arquitectura, el router conectado a Internet, es decir el router exterior, obliga todo el tráfico entrante a pasar por el gateway de la aplicación. El router conectado a la red interna, es decir el router interior, acepta los paquetes provenientes sólo del gateway de aplicación. En efecto, el gateway controla la entrega de servicios basados en red que entran y salen de la red interna. Por ejemplo, sólo ciertos usuarios pueden estar autorizados a comunicarse con Internet o sólo a ciertas aplicaciones se les puede permitir establecer conexiones entre un host interior y exterior. Si la única aplicación que se permite es el correo electrónico, entonces sólo se permiten paquetes de correo electrónico a través del router. Esto protege el gateway de aplicación y evita que se supere su capacidad con paquetes que de otra manera se descartarían.

Se deben utilizar ACL (Listas de control de Acceso) en los routers firewall, que a menudo se sitúan entre la red interna y una red externa, como Internet. Esto permite el control del tráfico entrante o saliente de alguna parte específica de la red interna.

El router firewall proporciona un punto de aislamiento, de manera que el resto de la estructura interna de la red no se vea afectada.

Los ACL son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router o firewall. Estas listas le informan al router o firewall qué tipo de paquetes aceptar o rechazar. La aceptación y rechazo se pueden basar en ciertas condiciones específicas. Las ACL permiten la administración del tráfico y aseguran el acceso hacia y desde una red. Es posible crear ACL en todos los protocolos de red enrutados, por ejemplo: el Protocolo de Internet (IP) y el Intercambio de paquetes de internetwork (IPX).

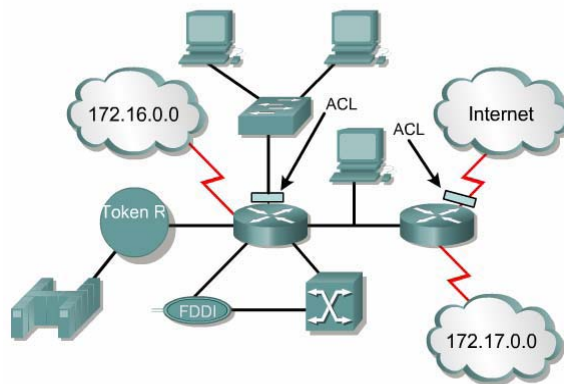


Figura 2.14 ACL

Estas son las razones principales para crear las ACL:

- Limitar el tráfico de red y mejorar el rendimiento de la red. Al restringir el tráfico de video, por ejemplo, las ACL pueden reducir ampliamente la carga de la red y en consecuencia mejorar el rendimiento de la misma.
- Brindar control de flujo de tráfico. Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Por ejemplo, las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Por ejemplo, al Host A se le permite el acceso a la red de Recursos Humanos, y al Host B se le niega el acceso a dicha red.
- Se debe decidir qué tipos de tráfico se envían o bloquean en las interfaces del router. Permitir que se enrute el tráfico de correo electrónico, pero bloquear todo el tráfico de telnet.
- Permitir que un administrador controle a cuáles áreas de la red puede acceder un cliente.
- Analizar ciertos hosts para permitir o denegar acceso a partes de una red. Otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos, tales como FTP o HTTP.

### 2.1.3 Topología de red

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos. Las topologías físicas más comúnmente usadas son las siguientes:

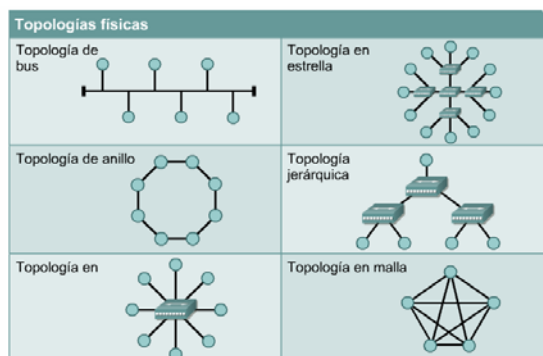


Figura 2.15 Topologías Físicas

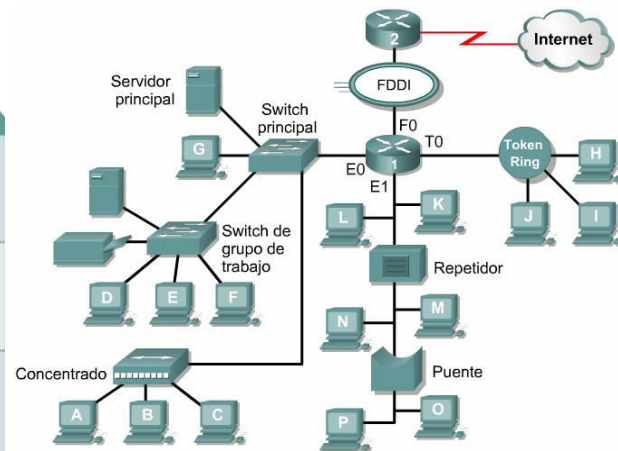


Figura 2.16 Combinación de Topologías físicas

- Una topología de bus usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.
- La topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.
- La topología en estrella conecta todos los cables con un punto central de concentración.
- Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.
- Una topología jerárquica es similar a una estrella extendida. Pero en lugar de conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
- La topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente. Como se puede observar en el gráfico, cada host tiene sus propias conexiones con los demás hosts. Aunque la Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

La topología broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada. Ethernet funciona así, tal como se explicará en el curso más adelante.

La segunda topología lógica es la transmisión de tokens. La transmisión de tokens controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos distribuida por fibra (FDDI). Arcnet es una variación de Token Ring y FDDI. Arcnet es la transmisión de tokens en una topología de bus.

El diagrama en la Figura 2.16 anterior muestra diferentes topologías conectadas mediante dispositivos de red. Muestra una LAN de complejidad moderada que es típica de una escuela o de una pequeña empresa. Tiene muchos símbolos, y describe varios conceptos de networking que lleva cierto tiempo aprender.

### 2.1.4 Protocolos de red

Los conjuntos de protocolos son colecciones de protocolos que posibilitan la comunicación de red desde un host, a través de la red, hacia otro host. Un protocolo es una descripción formal de un conjunto de reglas y convenciones que rigen un aspecto particular de cómo los dispositivos de una red se comunican entre sí.

Los protocolos determinan el formato, la sincronización, la secuenciación y el control de errores en la comunicación de datos. Sin protocolos, el computador no puede armar o reconstruir el formato original del flujo de bits entrantes desde otro computador.

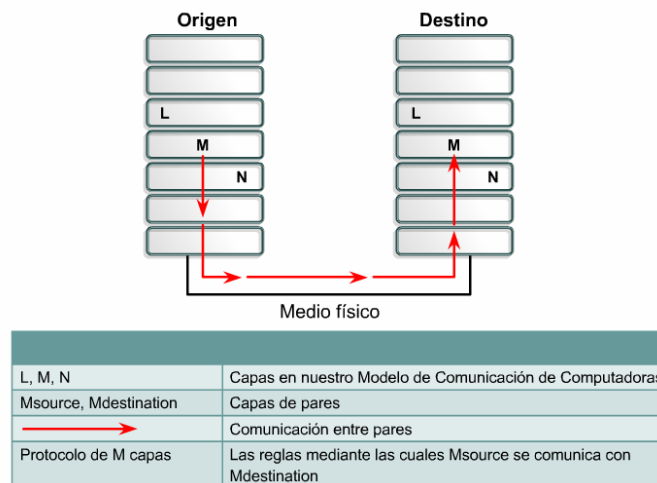


Figura 2.17 Protocolos de red

Los protocolos controlan todos los aspectos de la comunicación de datos, que incluye lo siguiente:

- Cómo se construye la red física
- Cómo los computadores se conectan a la red
- Cómo se formatean los datos para su transmisión
- Cómo se envían los datos
- Cómo se manejan los errores

Estas normas de red son creadas y administradas por una serie de diferentes organizaciones y comités entre ellos se incluyen el Instituto de Ingeniería Eléctrica y Electrónica (IEEE), el Instituto Nacional Americano de Normalización (ANSI), la Asociación de la Industria de las Telecomunicaciones (TIA), la Asociación de Industrias Electrónicas (EIA) y la Unión Internacional de Telecomunicaciones (UIT), antiguamente conocida como el Comité Consultivo Internacional Telegráfico y Telefónico (CCITT).

### 2.1.5 Redes de área local (LAN)

Las LAN constan de los siguientes componentes:

- Computadores
- Tarjetas de interfaz de red
- Dispositivos periféricos
- Medios de networking
- Dispositivos de networking

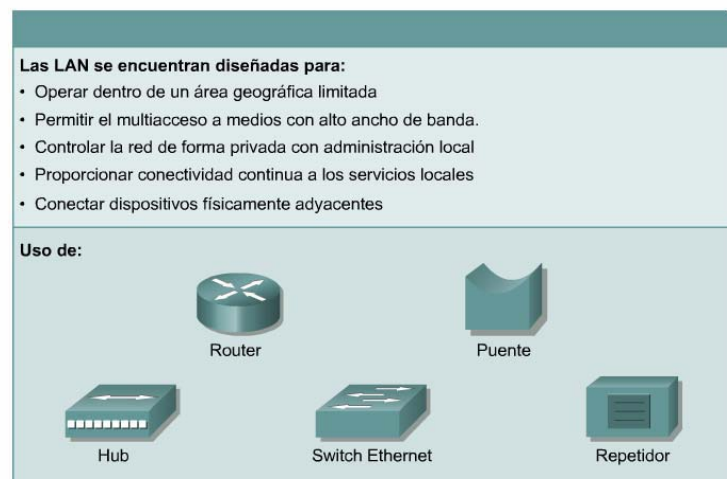


Figura 2.18 Funciones de la Red LAN

Las LAN permiten a las empresas aplicar tecnología informática para compartir localmente archivos e impresoras de manera eficiente, y posibilitar las comunicaciones internas. Un buen ejemplo de esta tecnología es el correo

electrónico. Los que hacen es conectar los datos, las comunicaciones locales y los equipos informáticos.

Algunas de las tecnologías comunes de LAN son:

- Ethernet
- Token Ring
- FDDI

## 2.1.6 Redes de área amplia (WAN)

Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes. Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona. Networking de área amplia también dio lugar a una nueva clase de trabajadores, los empleados a distancia, que no tienen que salir de sus hogares para ir a trabajar.

Las WAN están diseñadas para realizar lo siguiente:

- Operar entre áreas geográficas extensas y distantes
- Posibilitar capacidades de comunicación en tiempo real entre usuarios
- Brindar recursos remotos de tiempo completo, conectados a los servicios locales
- Brindar servicios de correo electrónico, World Wide Web, transferencia de archivos y comercio electrónico



Figura 2.19 Funciones de la red WAN

Algunas de las tecnologías comunes de WAN son:

- Módems
- Red digital de servicios integrados (RDSI)
- Línea de suscripción digital (DSL - Digital Subscriber Line)
- Frame Relay
- Series de portadoras para EE.UU. (T) y Europa (E): T1, E1, T3, E3
- Red óptica Síncrona (SONET)

### 2.1.7 Redes de área metropolitana (MAN)

La MAN es una red que abarca un área metropolitana, como, por ejemplo, una ciudad o una zona suburbana. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común. Por ejemplo, un banco con varias sucursales puede utilizar una MAN. Normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando tecnologías de puente inalámbrico enviando haces de luz a través de áreas públicas

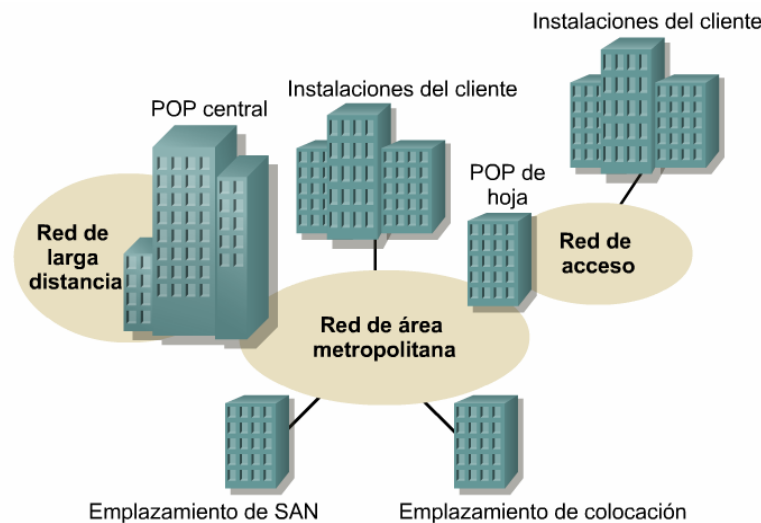


Figura 2.20 Redes de área Metropolitana MAN

### 2.1.8 Red privada virtual (VPN)

Una VPN es una red privada que se construye dentro de una infraestructura de red pública, como la Internet global. Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un router VPN en la sede.



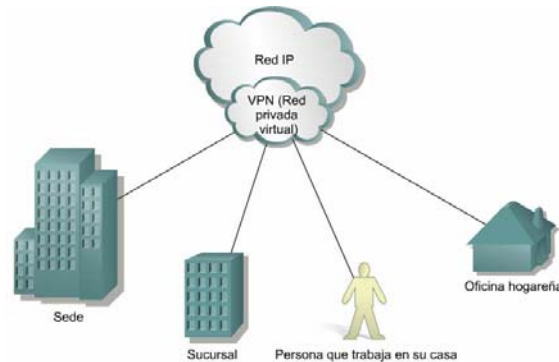


Figura 2.21 Redes Privadas Virtuales

### Ventajas de las VPN

Los productos Cisco admiten la más reciente tecnología de VPN. La VPN es un servicio que ofrece conectividad segura y confiable en una infraestructura de red pública compartida, como la Internet. Las VPN conservan las mismas políticas de seguridad y administración que una red privada. Son la forma más económica de establecer una conexión punto-a-punto entre usuarios remotos y la red de un cliente de la empresa.

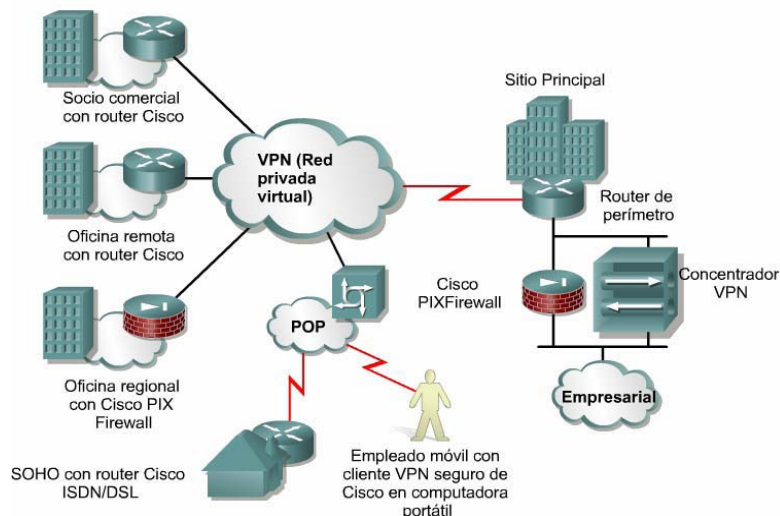


Figura 2.22 Arquitectura de las redes Privadas Virtuales

A continuación se describen los tres principales tipos de VPN:

- **VPN de acceso:** Las VPN de acceso brindan acceso remoto a un trabajador móvil y una oficina pequeña/oficina hogareña (SOHO), a la sede de la red interna o externa, mediante una infraestructura compartida. Las VPN de acceso usan tecnologías analógicas, de acceso telefónico, RDSI, línea de suscripción digital (DSL), IP móvil y de cable para brindar conexiones seguras a usuarios móviles, empleados a distancia y sucursales.



- **Redes internas VPN:** Las redes internas VPN conectan a las oficinas regionales y remotas a la sede de la red interna mediante una infraestructura compartida, utilizando conexiones dedicadas.

Las redes internas VPN difieren de las redes externas VPN, ya que sólo permiten el acceso a empleados de la empresa.

- **Redes externas VPN:** Las redes externas VPN conectan a socios comerciales a la sede de la red mediante una infraestructura compartida, utilizando conexiones dedicadas. Las redes externas VPN difieren de las redes internas VPN, ya que permiten el acceso a usuarios que no pertenecen a la empresa.

### 2.1.9 Redes internas y externas

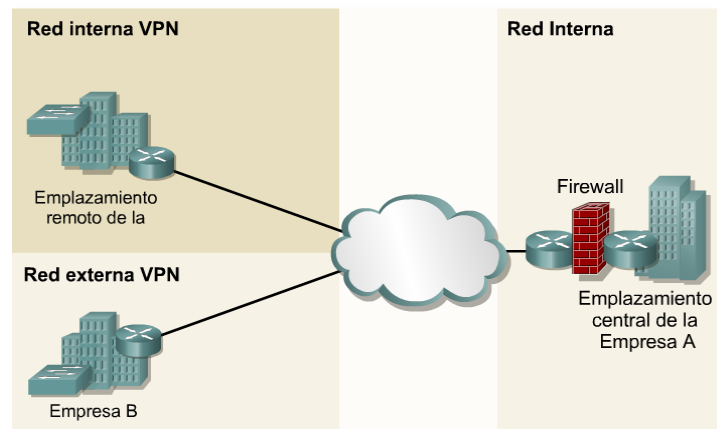


Figura 2.23 Redes internas y externas

Una de las configuraciones comunes de una LAN es una red interna, a veces denominada "intranet". Los servidores de Web de red interna son distintos de los servidores de Web públicos, ya que es necesario que un usuario público cuente con los correspondientes permisos y contraseñas para acceder a la red interna de una organización. Las redes internas están diseñadas para permitir el acceso por usuarios con privilegios de acceso a la LAN interna de la organización. Dentro de una red interna, los servidores de Web se instalan en la red. La tecnología de navegador se utiliza como interfaz común para acceder a la información, por ejemplo datos financieros o datos basados en texto y gráficos que se guardan en esos servidores. Las redes externas hacen referencia a aplicaciones y servicios basados en la red interna, y utilizan un acceso extendido y seguro a usuarios o empresas externas. Este acceso generalmente se logra mediante contraseñas, identificaciones de usuarios, y seguridad a nivel de las aplicaciones. Por lo tanto, una red externa es la extensión de dos o más estrategias de red interna, con una interacción segura entre empresas participantes y sus respectivas redes internas.

## 2.2 Modelos de networking

### 2.2.1 Uso de capas para analizar problemas en un flujo de materiales

El concepto de capas se utiliza para describir la comunicación entre dos computadores. La figura muestra un conjunto de preguntas relacionadas con flujo, que se define como el movimiento de objetos físicos o lógicos, a través de un sistema. Estas preguntas muestran cómo el concepto de capas ayuda a describir los detalles del proceso de flujo. Este proceso puede referirse a cualquier tipo de flujo, desde el flujo del tráfico en un sistema de autopistas, al flujo de datos a través de una red. La figura muestra varios ejemplos de flujo, y formas en las que se puede desglosar el proceso de flujo en detalles o en capas.

| Red             | Qué fluye   | Distintas formas                           | Reglas   | Dónde   |
|-----------------|-------------|--|--|---|
| Agua            | Agua        | Caliente, fría, potable, servida           | Reglas de acceso (abrir o cerrar grifos); vaciar el agua del inodoro; no echar ciertas cosas en las cañerías | Caños   |
| Autopista       | Vehículos   | Camiones, autos, motocicletas y bicicletas | Leyes de tránsito y reglas de cortesía   | Rutas y autopistas                                |
| Servicio postal | Objetos     | Cartas (información escrita); paquetes     | Reglas para el empaquetado y franqueo  | Buzones, oficinas, camiones, aviones, carteros    |
| Teléfono        | Información | Idiomas hablados                           | Reglas de acceso al teléfono y reglas de cortesía  | Cables telefónicos, ondas electromagnéticas, etc. |

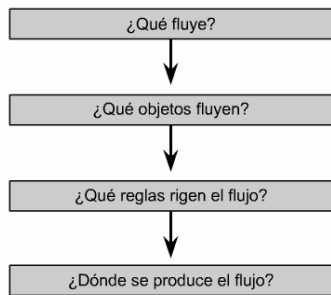


Figura 2.24 Ejemplos de flujo

La conversación entre dos personas es un buen ejemplo para aplicar un enfoque en capas para analizar el flujo de información. En una conversación, cada persona que desea comunicarse comienza creando una idea. Luego se toma una decisión respecto de cómo comunicar la idea correctamente. Por ejemplo, una persona podría decidir si hablar, cantar o gritar, y qué idioma usar. Finalmente, la idea es comunicada. Por ejemplo, la persona crea el sonido que transmite el mensaje.

Se puede desglosar este proceso en distintas capas aplicables a todas las conversaciones. La capa superior es la idea que se comunicará. La capa intermedia es la decisión respecto de cómo se comunicará la idea. La capa inferior es la creación del sonido que transmitirá la comunicación.

El mismo método de división en capas explica cómo una red informática distribuye la información desde el origen al destino. Cuando los computadores envían información

a través de una red, todas las comunicaciones se generan en un origen y luego viajan a un destino.

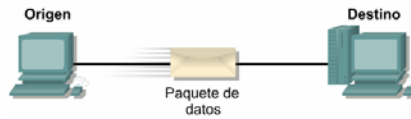


Figura 2.25 Comunicación Origen-Destino

Generalmente, la información que se desplaza por una red recibe el nombre de datos o paquete. Un paquete es una unidad de información, lógicamente agrupada, que se desplaza entre los sistemas de computación. A medida que los datos atraviesan las capas, cada capa agrega información que posibilita una comunicación eficaz con su correspondiente capa en el otro computador.

Los modelos OSI y TCP/IP se dividen en capas que explican cómo los datos se comunican de un computador a otro. Los modelos difieren en la cantidad y la función de las capas. No obstante, se puede usar cada modelo para ayudar a describir y brindar detalles sobre el flujo de información desde un origen a un destino.

## 2.2.2 Uso de capas para describir la comunicación de datos

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo. Un protocolo es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente. Por ejemplo, al pilotar un avión, los pilotos obedecen reglas muy específicas para poder comunicarse con otros aviones y con el control de tráfico aéreo. Un protocolo de comunicaciones de datos es un conjunto de normas, o un acuerdo, que determina el formato y la transmisión de datos.

La Capa 4 del computador de origen se comunica con la Capa 4 del computador de destino. Las normas y convenciones utilizadas para esta capa reciben el nombre de protocolos de la Capa 4. Es importante recordar que los protocolos preparan datos en forma lineal. El protocolo en una capa realiza un conjunto determinado de operaciones sobre los datos al prepararlos para ser enviados a través de la red. Los datos luego pasan a la siguiente capa, donde otro protocolo realiza otro conjunto diferente de operaciones.

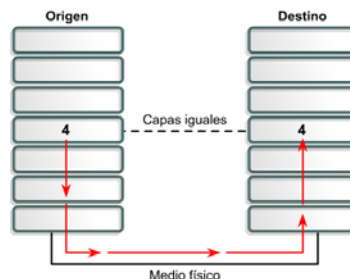


Figura 2.26 Flujo de información de capa en capa

Una vez que el paquete llega a su destino, los protocolos deshacen la construcción del paquete que se armó en el extremo de origen. Esto se hace en orden inverso. Los protocolos para cada capa en el destino devuelven la información a su forma original, para que la aplicación pueda leer los datos correctamente.

### 2.2.3 Modelo OSI

En sus inicios, el desarrollo de redes sucedió con desorden en muchos sentidos. A principios de la década de 1980 se produjo un enorme crecimiento en la cantidad y el tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de usar tecnología de networking, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red.

Para mediados de la década de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de networking privadas o propietarias. "Propietario" significa que una sola empresa o un pequeño grupo de empresas controlan todo uso de la tecnología. Las tecnologías de networking que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes.

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional de Normalización (ISO) investigó modelos de networking como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. En base a esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes. El modelo de referencia de Interconexión de Sistemas Abiertos (OSI) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

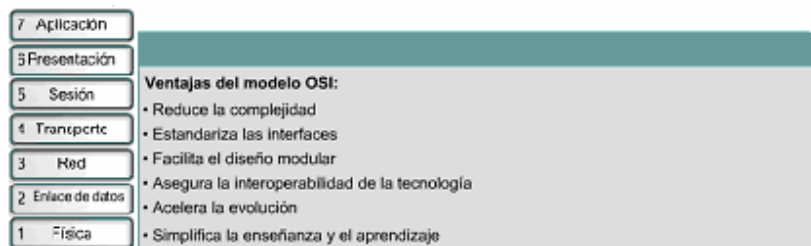


Figura 2.27 Modelo OSI



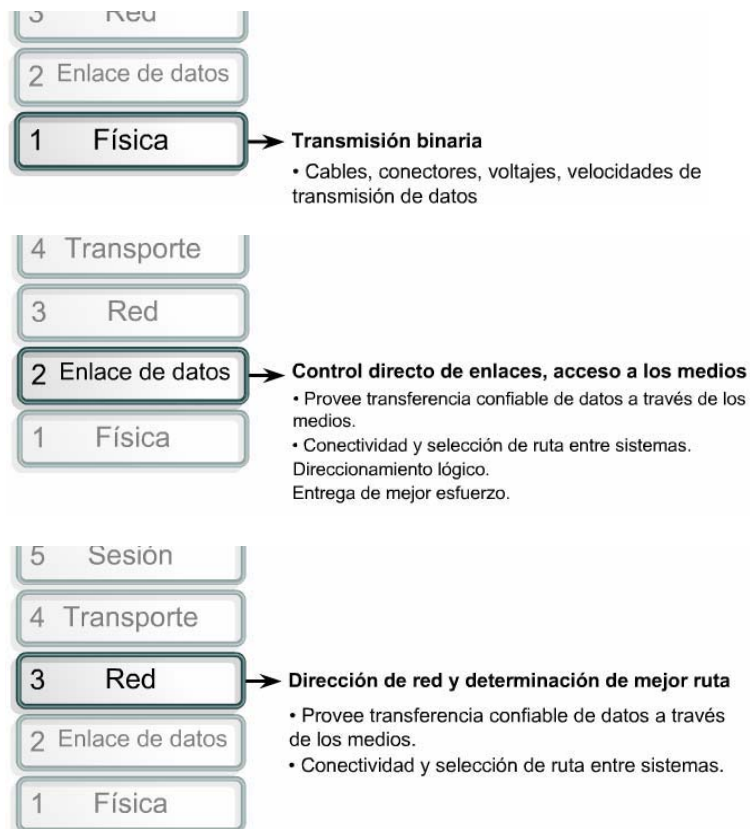
El modelo de referencia OSI se ha convertido en el modelo principal para las comunicaciones por red.

Aunque existen otros modelos, la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia de OSI. Esto es en particular así cuando lo que buscan es enseñar a los usuarios a utilizar sus productos. Se considera la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

## 2.2.4 Las capas del modelo OSI

El modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. El modelo de referencia OSI explica de qué manera los paquetes de datos viajan a través de varias capas a otro dispositivo de una red, aun cuando el remitente y el destinatario poseen diferentes tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. - La división de la red en siete capas permite obtener las siguientes ventajas:



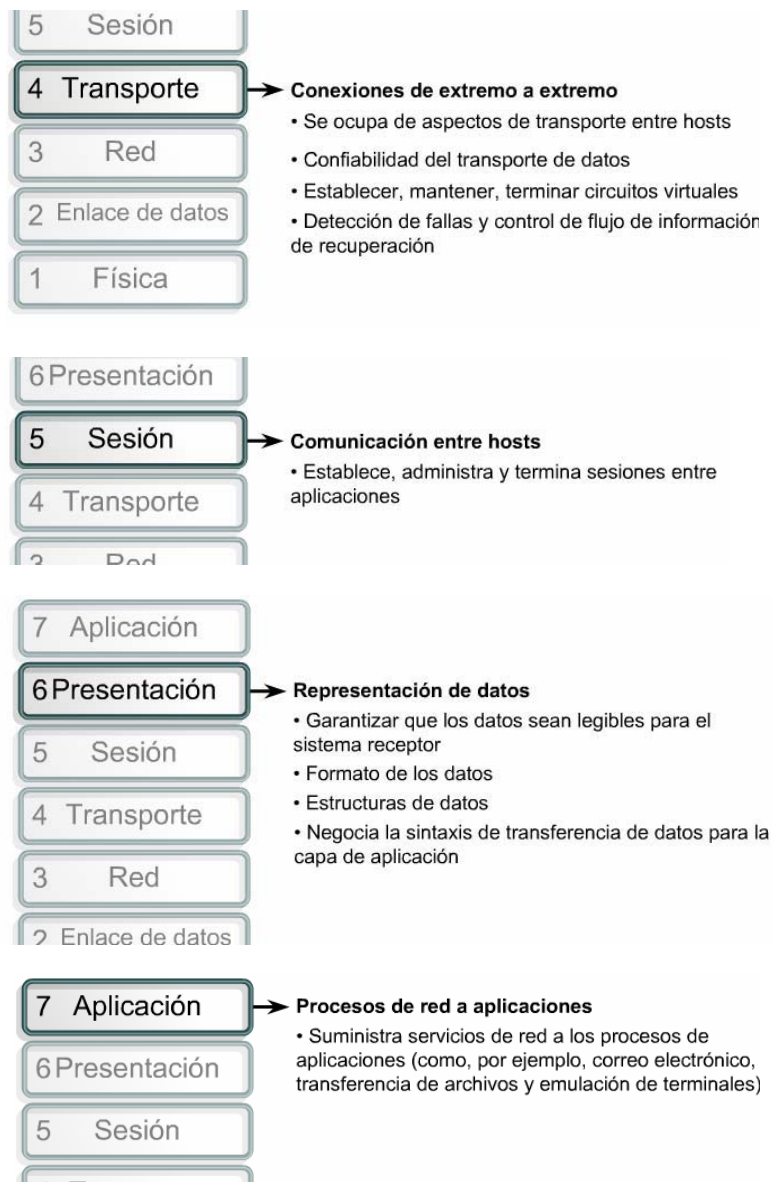


Figura 2.28 Descripción de cada una de las capas del Modelo OSI

- Divide la comunicación de red en partes más pequeñas y fáciles de manejar.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos por diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Evita que los cambios en una capa afecten las otras capas.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

## 2.2.5 Comunicaciones de par a par

Para que los datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa par en el lugar destino. Esta forma de comunicación se conoce como de par-a-par. Durante este proceso, los protocolos de cada capa intercambian información, denominada unidades de datos de protocolo (PDU). Cada capa de comunicación en el computador origen se comunica con un PDU específico de capa, y con su capa par en el computador destino, como lo ilustra la figura.

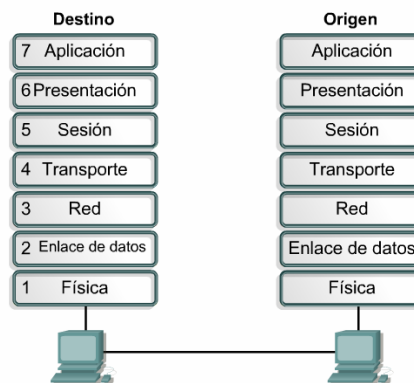


Figura 2.29 Comunicación de par a par

Los paquetes de datos de una red parten de un origen y se envían a un destino. Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego le puede agregar cualquier encabezado e información final que la capa necesite para ejecutar su función.

Posteriormente, a medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, se agregan encabezados e información final adicionales. Después de que las Capas 7, 6 y 5 han agregado su información, la Capa 4 agrega más información. Este agrupamiento de datos, la PDU de la Capa 4, se denomina segmento.

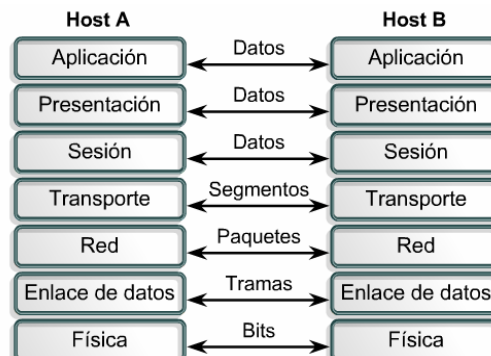


Figura 2.30 PDUs de cada capa





La capa de red presta un servicio a la capa de transporte y la capa de transporte presenta datos al subsistema de internetwork. La tarea de la capa de red consiste en trasladar esos datos a través de la internetwork. Ejecuta esta tarea encapsulando los datos y agregando un encabezado, con lo que crea un paquete (la PDU de la Capa 3). Este encabezado contiene la información necesaria para completar la transferencia, como, por ejemplo, las direcciones lógicas origen y destino.

La capa de enlace de datos suministra un servicio a la capa de red. Encapsula la información de la capa de red en una trama (la PDU de la Capa 2). El encabezado de trama contiene la información (por ejemplo, las direcciones físicas) que se requiere para completar las funciones de enlace de datos. La capa de enlace de datos suministra un servicio a la capa de red encapsulando la información de la capa de red en una trama.

La capa física también suministra un servicio a la capa de enlace de datos. La capa física codifica los datos de la trama de enlace de datos en un patrón de unos y ceros (bits) para su transmisión a través del medio (generalmente un cable) en la Capa 1.

## 2.2.6 Modelo TCP/IP

El estándar histórico y técnico de la Internet es el modelo TCP/IP. El Departamento de Defensa de EE.UU. (DoD) creó el modelo de referencia TCP/IP porque necesitaba diseñar una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear. En un mundo conectado por diferentes tipos de medios de comunicación, como alambres de cobre, microondas, fibras ópticas y enlaces satelitales, el DoD quería que la transmisión de paquetes se realizara cada vez que se iniciaba y bajo cualquier circunstancia. Este difícil problema de diseño dio origen a la creación del modelo TCP/IP.

A diferencia de las tecnologías de networking propietarias mencionadas anteriormente, el TCP/IP se desarrolló como un estándar abierto. Esto significaba que cualquier persona podía usar el TCP/IP. Esto contribuyó a acelerar el desarrollo de TCP/IP como un estándar.

El modelo TCP/IP tiene las siguientes cuatro capas:

- Capa de aplicación
- Capa de transporte
- Capa de Internet
- Capa de acceso a la red

Aunque algunas de las capas del modelo TCP/IP tienen el mismo nombre que las capas del modelo OSI, las capas de ambos modelos no se corresponden de manera exacta. Lo más notable es que la capa de aplicación posee funciones diferentes en cada modelo.



Los diseñadores de TCP/IP sintieron que la capa de aplicación debía incluir los detalles de las capas de sesión y presentación OSI. Crearon una capa de aplicación que maneja aspectos de representación, codificación y control de diálogo.



Figura 2.31 Capas del Modelo TCP/IP

La capa de transporte se encarga de los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo.

TCP es un protocolo orientado a conexión. Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos. Orientado a conexión no significa que existe un circuito entre los computadores que se comunican. Significa que segmentos de la Capa 4 viajan de un lado a otro entre dos hosts para comprobar que la conexión exista lógicamente para un determinado período.

El propósito de la capa Internet es dividir los segmentos TCP en paquetes y enviarlos desde cualquier red. Los paquetes llegan a la red de destino independientemente de la ruta que utilizaron para llegar allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes.

La relación entre IP y TCP es importante. Se puede pensar en el IP como el que indica el camino a los paquetes, en tanto que el TCP brinda un transporte seguro.

El nombre de la capa de acceso de red es muy amplio y se presta a confusión. También se conoce como la capa de host a red. Esta capa guarda relación con todos los componentes, tanto físicos como lógicos, necesarios para lograr un enlace físico. Incluye los detalles de tecnología de networking, y todos los detalles de la capa física y de enlace de datos del modelo OSI.

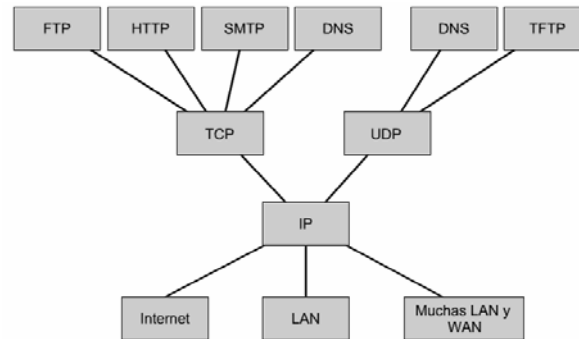


Figura 2.32 Protocolos comunes en el Modelo TCP/IP

La figura ilustra algunos de los protocolos comunes especificados por las capas del modelo de referencia TCP/IP. Algunos de los protocolos de capa de aplicación más comúnmente usados incluyen los siguientes:

- Protocolo de Transferencia de Archivos (FTP)
- Protocolo de Transferencia de Hipertexto (HTTP)
- Protocolo simple de transferencia de correo (SMTP)
- Sistema de denominación de dominios (DNS)
- Protocolo Trivial de Transferencia de Archivos (TFTP)

Los protocolos de capa de transporte comunes incluyen:

- Protocolo para el Control del Transporte (TCP)
- Protocolo de Datagrama de Usuario (UDP)

El protocolo principal de la capa Internet es:

- Protocolo Internet (IP)

La capa de acceso de red se refiere a cualquier tecnología en particular utilizada en una red específica. Independientemente de los servicios de aplicación de red que se brinden y del protocolo de transferencia que se utilice, existe un solo protocolo de Internet, IP. Esta es una decisión de diseño deliberada. IP sirve como protocolo universal que permite que cualquier computador en cualquier parte del mundo pueda comunicarse en cualquier momento.

Comparando el modelo OSI con los modelos TCP/IP, surgen algunas similitudes y diferencias.

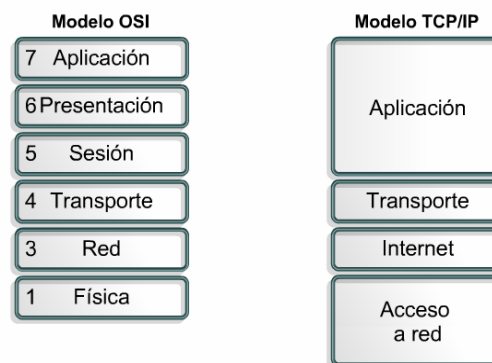


Figura 2.33 Comparación gráfica del modelo OSI con el TCP/IP



Las similitudes incluyen:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Ambos modelos deben ser conocidos por los profesionales de networking.
- Ambos suponen que se conmutan paquetes. Esto significa que los paquetes individuales pueden usar rutas diferentes para llegar al mismo destino. Esto se contrasta con las redes conmutadas por circuito, en las que todos los paquetes toman la misma ruta.

Las diferencias incluyen:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en la capa de acceso de red.
- TCP/IP parece ser más simple porque tiene menos capas.
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, por lo general las redes no se desarrollan a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

Aunque los protocolos TCP/IP representan los estándares en base a los cuales se ha desarrollado la Internet, este currículum utiliza el modelo OSI por los siguientes motivos:

- Es un estándar genérico, independiente de los protocolos.
- Es más detallado, lo que hace que sea más útil para la enseñanza y el aprendizaje.
- Al ser más detallado, resulta de mayor utilidad para el diagnóstico de fallas.

Los profesionales de networking tienen distintas opiniones con respecto al modelo que se debe usar. Dada la naturaleza de esta industria, es necesario familiarizarse con ambos. A lo largo de todo el currículum se hará referencia a ambos modelos, el OSI y el TCP/IP. Se hará énfasis en lo siguiente:

- TCP como un protocolo de Capa 4 OSI
- IP como un protocolo de Capa 3 OSI
- Ethernet como una tecnología de Capa 2 y Capa 1

Hay que recordar que hay una diferencia entre un modelo y un protocolo. Se utilizará el modelo OSI para describir protocolos TCP/IP.

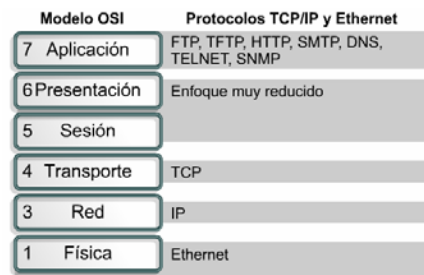


Figura 2.34 Protocolos TCP/IP y Ethernet en el Modelos OSI

## 2.2.7 Proceso detallado de encapsulamiento

Todas las comunicaciones de una red parten de un origen y se envían a un destino. La información que se envía a través de una red se denomina datos o paquetes de datos. Si un computador (host A) desea enviar datos a otro (host B), en primer término los datos deben empaquetarse a través de un proceso denominado encapsulamiento.

El encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tránsito de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información.

Para ver cómo se produce el encapsulamiento, examine la forma en que los datos viajan a través de las capas como lo ilustra la figura 2.35. Una vez que se envían los datos desde el origen, viajan a través de la capa de aplicación y recorren todas las demás capas en sentido descendente. El empaquetamiento y el flujo de los datos que se intercambian experimentan cambios a medida que las capas realizan sus funciones para los usuarios finales. Como lo muestra la figura 2.36, las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos:

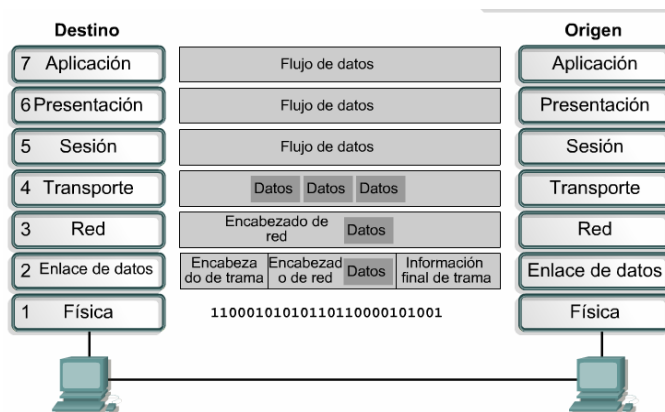


Figura 2.35 Pasos para encapsular los datos

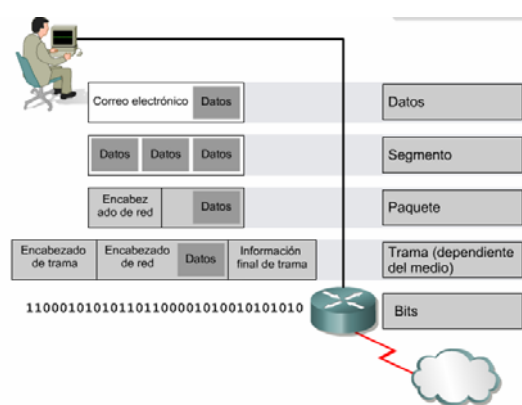


Figura 2.36 Pasos para encapsular los datos

- 1. Crear los datos.** Cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer la internetwork.
- 2. Empaquetar los datos para ser transportados de extremo a extremo.** Los datos se empaquetan para ser transportados por la internetwork. Al utilizar segmentos, la función de transporte asegura que los hosts de mensaje en ambos extremos del sistema de correo electrónico se puedan comunicar de forma confiable.
- 3. Agregar la dirección de red IP al encabezado.** Los datos se colocan en un paquete o datagrama que contiene un encabezado de paquete con las direcciones lógicas de origen y de destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.

4. **Agregar el encabezado y la información final de la capa de enlace de datos.** Cada dispositivo de la red debe poner el paquete dentro de una trama. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

5. **Realizar la conversión a bits para su transmisión.** La trama debe convertirse en un patrón de unos y ceros (bits) para su transmisión a través del medio. Una función de temporización permite que los dispositivos distinguan estos bits a medida que se trasladan por el medio. El medio en la internetwork física puede variar a lo largo de la ruta utilizada. Por ejemplo, el mensaje de correo electrónico se puede originar en una LAN, atravesar el backbone de una universidad y salir por un enlace WAN hasta llegar a su destino en otra LAN remota.

## 2.3 MEDIOS FÍSICOS DE TRANSMISIÓN DE DATOS

El medio físico viene a ser básicamente el "cable" que permite la comunicación y transmisión de datos, y que define la transmisión de bits a través de un canal. Esto quiere decir que debemos asegurarnos que cuando un punto de la comunicación envía un bit 1, este se reciba como un bit 1, no como un bit 0.

Para conectar físicamente una red se utilizan diferentes medios de transmisión.

A continuación veremos cómo se trabaja con los medios de transmisión en las redes LAN, en donde por lo general se utilizan cables.

### 2.3.1 El cableado de la red

El cable es el medio a través del cual fluye la información a través de la red. Hay distintos tipos de cable de uso común en redes LAN. Una red puede utilizar uno o más tipos de cable, aunque el tipo de cable utilizado siempre estará sujeto a la topología de la red, el tipo de red que utiliza y el tamaño de esta.

Estos son los tipos de cable más utilizados en redes LAN:

#### *CABLE DE PAR TRENZADO SIN APANTALLAR*

Este tipo de cable es el más utilizado. Tiene una variante con apantallamiento pero la variante sin apantallamiento suele ser la mejor opción para una PYME.

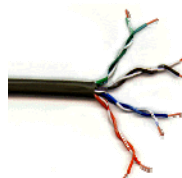


Figura 2.37 Cable UTP



La calidad del cable y consecuentemente la cantidad de datos que es capaz de transmitir varían en función de la categoría del cable. Las categorías van desde el cable de teléfono, que solo transmite la voz humana, a el cable de categoría 5 capaz de transferir 100Megabytes por segundo.

| Tipo        | Uso                     |
|-------------|-------------------------|
| Categoría 1 | Voz (Cable de teléfono) |
| Categoría 2 | Datos a 4 Mbps          |
| Categoría 3 | Datos a 10 Mbps         |
| Categoría 4 | Datos a 20 Mbps/16 Mbps |
| Categoría 5 | Datos a 100 Mbps        |

Tabla 2.1 Categorías UTP

La diferencia entre las distintas categorías es la tirantez. A mayor tirantez mayor capacidad de transmisión de datos. Se recomienda el uso de cables de Categoría 3 o 5 para la implementación de redes en PYMES (pequeñas y medianas empresas). Es conveniente sin embargo utilizar cables de categoría 5 ya que estos permitirán migraciones de tecnologías 10Mb a tecnología 100 Mb.

### *CONECTOR UTP*

El estándar para conectores de cable UTP es el RJ-45. Se trata de un conector de plástico similar al conector del cable telefónico. Las siglas RJ se refieren al estándar Registered Jack, creado por la industria telefónica. Este estándar define la colocación de los cables en su pin correspondiente.

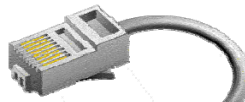


Figura 2.38. Conector RJ-45

### *CABLE DE PAR TRENZADO APANTALLADO*

Una de las desventajas del cable UTP es que es susceptible a las interferencias eléctricas. Para entornos con este problema existe un tipo de cable UTP que lleva apantallamiento, esto es, protección contra interferencias eléctricas.

### *CABLE COAXIAL*

El cable coaxial contiene un conductor de cobre en su interior. Este va envuelto en un aislante para separarlo de un apantallado metálico con forma de rejilla que aísla el cable de posibles interferencias externas.



Figura 2.39 Cable Coaxial

Aunque la instalación del cable coaxial es más complicada que la del UTP, este tiene un alto grado de resistencia a las interferencias. Por otra parte también es posible conectar distancias mayores que con los cables de par trenzado. Existen dos tipos de cable coaxial, el fino y el grueso conocidos como thin coaxial y thick coaxial.

Con frecuencia se pueden escuchar referencias al cable coaxial fino como thinnet o 10Base2. Esto hace referencia a una red de tipo Ethernet con un cableado coaxial fino, donde el 2 significa que el mayor segmento posible es de 200 metros, siendo en la práctica reducido a 185 m. El cable coaxial es muy popular en las redes con topología de BUS. Con frecuencia se pueden escuchar referencias al cable coaxial grueso como thicknet o 10Base5. Esto hace referencia a una red de tipo Ethernet con un cableado coaxial grueso, donde el 5 significa que el mayor segmento posible es de 500 metros.

El cable coaxial grueso tiene una capa plástica adicional que protege de la humedad al conductor de cobre. Esto hace de este tipo de cable una gran opción para redes de BUS extensas, aunque hay que tener en cuenta que este cable es difícil de doblar.

### *CONECTOR PARA CABLE COAXIAL*

El más usado es el conector BNC. BNC son las siglas de Bayone-Neill-Concelman. Los conectores BNC pueden ser de tres tipos: normal, terminadores y conectores en T.



Figura 2.40 Conector BNC

### *CABLE DE FIBRA ÓPTICA*

El cable de fibra óptica consiste en un centro de cristal rodeado de varias capas de material protector. Lo que se transmite no son señales eléctricas sino luz con lo que se elimina la problemática de las interferencias. Esto lo hace ideal para entornos en los que haya gran cantidad de interferencias eléctricas. También se utiliza mucho en la conexión de redes entre edificios debido a su inmunidad a la humedad y a la exposición solar.

Con un cable de fibra óptica se pueden transmitir señales a distancias mucho mayores que con cables coaxiales o de par trenzado. Además, la cantidad de información capaz de transmitir es mayor por lo que es ideal para redes a través de



las cuales se desee llevar a cabo videoconferencia o servicios interactivos. El coste es similar al cable coaxial pero las dificultades de instalación y modificación son mayores. En algunas ocasiones escucharemos 10BaseF como referencia a este tipo de cableado.

### CARACTERÍSTICAS DE LA FIBRA ÓPTICA

El aislante exterior está hecho de teflón o PVC. Fibras Kevlar ayudan a dar fuerza al cable y hacer más difícil su ruptura.

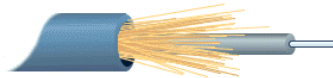


Figura 2.41 Cable de fibra óptica

Se utiliza un recubrimiento de plástico para albergar a la fibra central. El centro del cable está hecho de cristal o de fibras plásticas.

### CONECTORES PARA FIBRA ÓPTICA

El conector de fibra óptica más utilizado es el conector ST. Tiene una apariencia similar a los conectores BNC. También se utilizan, cada vez con más frecuencia conectores SC, de uso mas fácil

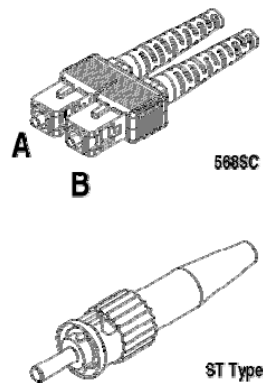
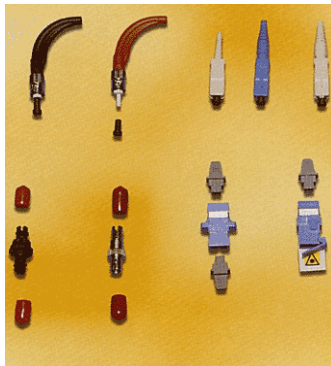


Figura 2.42 Conectores y adaptadores para la fibra óptica

| Especificación | Tipo de Cable   | Longitud Máxima |
|----------------|-----------------|-----------------|
| 10BaseT        | U T P           | 100 mts.        |
| 10Base2        | Coaxial Delgado | 185 mts.        |
| 10Base5        | Coaxial Grueso  | 500 mts.        |
| 10BaseF        | Fibra Óptica    | 2000 mts.       |

Tabla 2.2 Resumen de tipos de cables



### 2.3.2 Redes LAN sin cableado

No todas las redes se implementan sobre un cableado. Existen redes que utilizan señales de radio de alta frecuencia o haces infrarrojos para comunicarse. Cada punto de la red tiene una antena desde la que emite y recibe. Para largas distancias se pueden utilizar teléfonos móviles o satélites.

Este tipo de conexión está especialmente indicada para su uso con portátiles o para edificios viejos en los que es imposible instalar un cableado.

Las desventajas de este tipo de redes es sus altos costes, su susceptibilidad a las interferencias electromagnéticas y la baja seguridad que ofrecen. Además son más lentas que las redes que utilizan cableado.

Hemos visto los medios más comunes de transmisión de datos en las redes LAN, ahora veremos los medios mas comunes en las redes WAN

### 2.3.3 Medios inalámbricos en las redes WAN

Para redes de área extendida (WAN), los medios físicos de transmisión comunes son:

#### *COMUNICACIÓN POR MICROONDAS*

Microondas se llaman las ondas de radio que van de una antena parabólica a otra, sirven básicamente para comunicaciones de vídeo o telefónicas. La movilidad que pueden caracterizar estos equipos y el ahorro económico que produce el hecho de no tender cable a cada sitio en que quiera enviarse o recibir la información hace de esta técnica una de las más usadas para comunicaciones móviles.

Uno de los inconvenientes de la transmisión vía microondas es que las comunicaciones se ven afectadas por el estado del clima.

#### *COMUNICACIÓN POR SATÉLITE*

Los satélites de comunicación son enormes repetidores de microondas localizados en el cielo. Están constituidos por uno o más dispositivos recepto-transmisores, cada uno de los cuales capta y re-transmite la señal de microondas. El flujo dirigido hacia abajo puede ser muy amplio y cubrir una parte significativa de la superficie de la tierra, o bien puede ser estrecho y cubrir un área de cientos de kilómetros de diámetro.

Los satélites de comunicación tienen varias propiedades que son completamente diferentes de las que presentan los enlaces terrestres punto a punto. Por ejemplo, aún cuando las señales que van o vienen del satélite viajan a la velocidad de la luz (300.000 Km/s), éstas introducen un retardo substancial al recorrer la distancia total como consecuencia del tiempo que tarda la información en ir y venir.

## 2.4 Dirección de Internet

### 2.4.1 Direccionamiento IP

Para que dos sistemas se comuniquen, se deben poder identificar y localizar entre sí. Aunque las direcciones de la Figura no son direcciones de red reales, representan el concepto de agrupamiento de las direcciones. Este utiliza A o B para identificar la red y la secuencia de números para identificar el host individual.

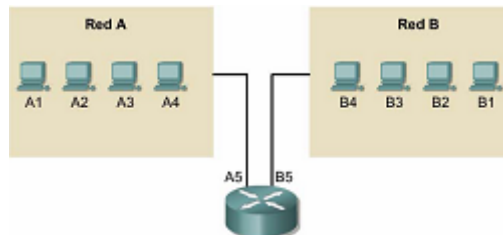


Figura 2.43 Ejemplos de direcciones en redes

Un computador puede estar conectado a más de una red. En este caso, se le debe asignar al sistema más de una dirección. Cada dirección identificará la conexión del computador a una red diferente. No se suele decir que un dispositivo tiene una dirección sino que cada uno de los puntos de conexión (o interfaces) de dicho dispositivo tiene una dirección en una red. Esto permite que otros computadores localicen el dispositivo en una determinada red. La combinación de letras (dirección de red) y el número (dirección del host) crean una dirección única para cada dispositivo conectado a la red. Cada computador conectado a una red TCP/IP debe recibir un identificador exclusivo o una dirección IP. Esta dirección, que opera en la Capa 3, permite que un computador localice otro computador en la red. Todos los computadores también cuentan con una dirección física exclusiva, conocida como dirección MAC. Estas son asignadas por el fabricante de la tarjeta de interfaz de la red. Las direcciones MAC operan en la Capa 2 del modelo OSI.

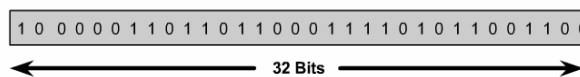


Figura 2.44 Secuencia de bits en una dirección IP

Una dirección IP es una secuencia de unos y ceros de 32 bits. La Figura muestra un número de 32 bits de muestra. Para que el uso de la dirección IP sea más sencillo, en general, la dirección aparece escrita en forma de cuatro números decimales separados por puntos. Por ejemplo, la dirección IP de un computador es 192.168.1.2. Otro computador podría tener la dirección 128.10.2.1. Esta forma de escribir una dirección se conoce como formato decimal punteado. En esta notación, cada dirección IP se escribe en cuatro partes separadas por puntos. Cada parte de la dirección se conoce como octeto porque se compone de ocho dígitos binarios. Por

ejemplo, la dirección IP 192.168.1.8 sería 11000000.10101000.00000001.00001000 en una notación binaria. La notación decimal punteada es un método más sencillo de comprender que el método binario de unos y ceros. Esta notación decimal punteada también evita que se produzca una gran cantidad de errores por transposición, que sí se produciría si sólo se utilizaran números binarios. El uso de decimales separados por puntos permite una mejor comprensión de los patrones numéricos. Tanto los números binarios como los decimales de la Figura representan a los mismos valores, pero resulta más sencillo apreciar la notación decimal punteada. Este es uno de los problemas frecuentes que se encuentran al trabajar directamente con números binarios. Las largas cadenas de unos y ceros que se repiten hacen que sea más probable que se produzcan errores de transposición y omisión.

|  |
|--|
| Binario: 11000000.10101000.00000001.00001000 y 11000000.10101000.00000001.00001001 |
| Decimal: 192.168.1.8 y 192.168.1.9   |

Figura 2.45 Conversión binario-decimal

Resulta más sencillo observar la relación entre los números 192.168.1.8 y 192.168.1.9, mientras que 11000000.10101000.00000001.00001000 y 11000000.10101000.00000001.00001001 no son fáciles de reconocer. Al observar los binarios, resulta casi imposible apreciar que son números consecutivos.

## 2.4.2 Direcciones IP reservadas

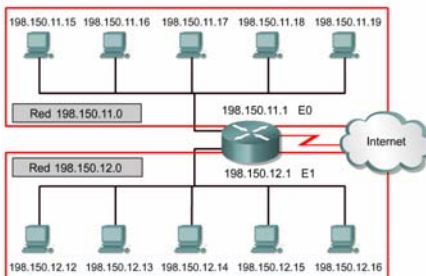


Figura 2.46 Direcciones IP reservadas

Ciertas direcciones de host son reservadas y no pueden asignarse a dispositivos de la red. Estas direcciones de host reservadas incluyen:

- **Dirección de red:** Utilizada para identificar la red en sí.

En la Figura, la sección que está identificada en el casillero superior representa la red 198.150.11.0. Los datos enviados a cualquier host de dicha red (198.150.11.1-198.150.11.254) se verá desde afuera de la red del área local con la dirección 198.159.11.0. Los números del host sólo tienen importancia cuando los datos se encuentran en una red de área local. La LAN contenida en el casillero inferior recibe el mismo tratamiento que la LAN superior, sólo que el número de la red es 198.150.12.0.

- **Dirección de broadcast:** Utilizada para realizar el broadcast de paquetes hacia todos los dispositivos de una red.

En la Figura, la sección que se identifica en el casillero superior representa la dirección de broadcast 198.150.11.255. Todos los hosts de la red leerán los datos enviados a la dirección de broadcast (198.150.11.1- 198.150.11.254). La LAN contenida en el casillero inferior recibe el mismo tratamiento que la LAN superior, sólo que la dirección de broadcast es 198.150.12.255.

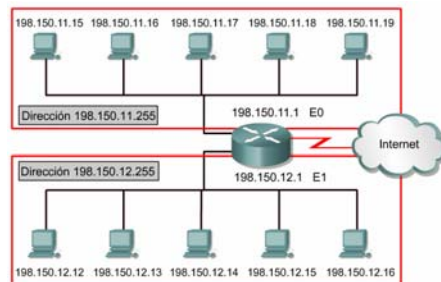


Figura 2.47 Direcciones IP reservadas

La dirección IP que tiene ceros binarios en todas las posiciones de bits de host queda reservada para la dirección de red. Tomando como ejemplo una red Clase A, 113.0.0.0 es la dirección IP de la red, conocida como el ID (identificador) de la red, que contiene el host 113.1.2.3. Un Router usa la dirección IP de red al enviar datos por Internet.

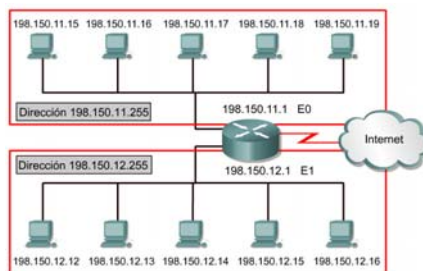


Figura 2.48 Direcciones IP reservadas

### 2.4.3 Introducción a la división en subredes

La división en subredes es otro método para administrar las direcciones IP. Este método, que consiste en dividir las clases de direcciones de red completas en partes de menor tamaño, ha evitado el completo agotamiento de las direcciones IP. Resulta imposible hablar sobre el TCP/IP sin mencionar la división en subredes. Como administrador de sistemas, es importante comprender que la división en subredes constituye un medio para dividir e identificar las redes individuales en toda la LAN. No siempre es necesario subdividir una red pequeña.

Sin embargo, en el caso de redes grandes a muy grandes, la división en subredes es necesaria. Dividir una red en subredes significa utilizar una máscara de subred para dividir la red y convertir una gran red en segmentos más pequeños, más eficientes y administrables o subredes. Un ejemplo sería el sistema telefónico de los EE.UU. que se divide en códigos de área, códigos de intercambio y números locales.

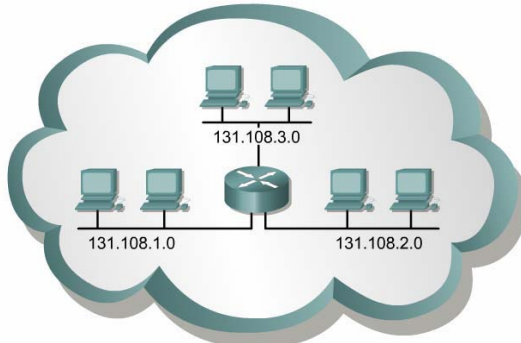


Figura 2.49 División de subred

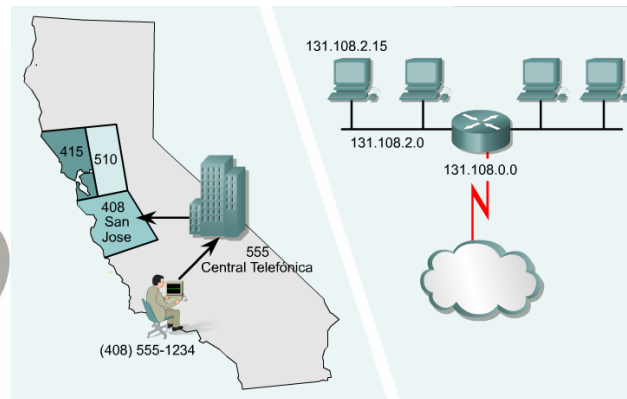


Figura 2.50 Administrador en la subred

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

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

Para crear una dirección de subred, un administrador de red pide prestados bits del campo de host y los designa como campo de subred. El número mínimo de bits que se puede pedir es dos. Al crear una subred, donde se solicita un sólo bit, el número de la red suele ser red .0. El número de broadcast entonces sería la red .255. El número máximo de bits que se puede pedir prestado puede ser cualquier número que deje por lo menos 2 bits restantes para el número de host.

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

Figura 2.51 Relación de subredes por valor de ultimo octeto





## 2.5 Mecanismos de la división en subredes

### 2.5.1 Clases de direcciones IP de red

Las clases de direcciones IP ofrecen de 256 a 16,8 millones de Hosts, como se vio con anterioridad en este módulo. Para administrar de forma eficiente un número limitado de direcciones IP, todas las clases pueden subdividirse en subredes más pequeñas. La Figura ofrece una descripción de la división entre redes y Hosts.

| Clase A | Red | Host |   |   |
|---------|-----|------|---|---|
| Octeto  | 1   | 2    | 3 | 4 |

| Clase B | Red |   | Host |   |
|---------|-----|---|------|---|
| Octeto  | 1   | 2 | 3    | 4 |

| Clase C | Red |   |   | Host |
|---------|-----|---|---|------|
| Octeto  | 1   | 2 | 3 | 4    |

| Clase D | Host |   |   |   |
|---------|------|---|---|---|
| Octeto  | 1    | 2 | 3 | 4 |

Figura 2.52 Clases de direcciones IP

### 2.5.2 Introducción y razones para realizar subredes

Para crear la estructura de subred, los bits de host se deben reasignar como bits de subred. Este proceso es a veces denominado "pedir bits prestados". Sin embargo, un término más preciso sería "prestar" bits. El punto de inicio de este proceso se encuentra siempre en el bit del Host del extremo izquierdo, aquel que se encuentra más cerca del octeto de red anterior.

Las direcciones de subred incluyen la porción de red Clase A, Clase B o Clase C además de un campo de subred y un campo de Host. El campo de subred y el campo de Host se crean a partir de la porción de Host original de la dirección IP entera. Esto se hace mediante la reasignación de bits de la parte de host a la parte original de red de la dirección. La capacidad de dividir la porción de Host original de la dirección en nuevas subredes y campos de Host ofrece flexibilidad de direccionamiento al administrador de la red.

Además de la necesidad de contar con flexibilidad, la división en subredes permite que el administrador de la red brinde contención de broadcast y seguridad de bajo nivel en la LAN. La división en subredes ofrece algo de seguridad ya que el acceso a las otras subredes está disponible solamente a través de los servicios de un Router. Además, el uso de listas de acceso puede ofrecer seguridad en el acceso. Estas





listas pueden permitir o negar el acceso a la subred, tomando en cuenta varios criterios, de esta manera brindan mayor seguridad. Más tarde se estudiarán las listas de acceso. Algunos propietarios de redes Clases A y B han descubierto que la división en subredes crea una fuente de ingresos para la organización a través del alquiler o venta de direcciones IP que anteriormente no se utilizaban.

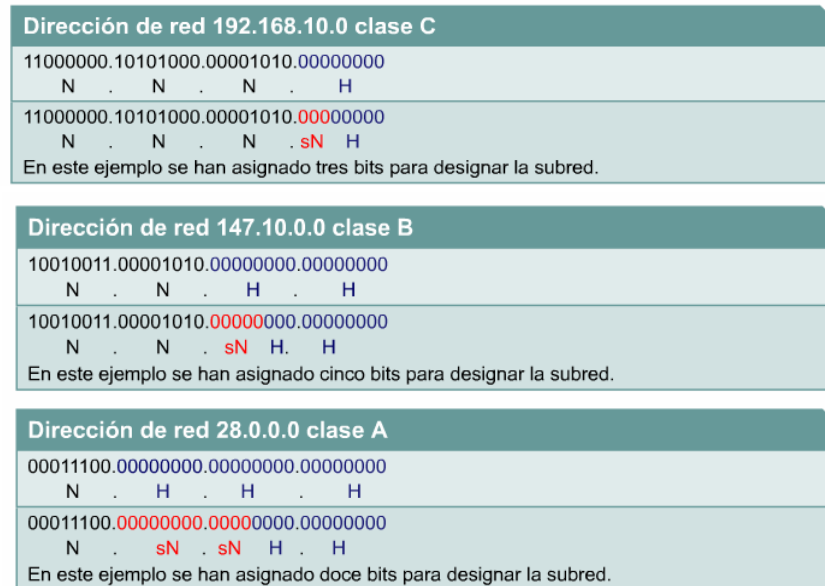


Figura 2.53 Cadenas de bits en las distintas clases de direcciones IP

Una LAN se percibe como una sola red sin conocimiento de su estructura de red interna. Esta visión de la red hace que las tablas de enrutamiento sean pequeñas y eficientes. Dada una dirección de nodo local 147.10.43.14 de la subred 147.10.43.0, el mundo exterior sólo puede ver la red mayor que se anuncia, la 147.10.0.0. Esto tiene su razón en que la dirección de la subred local 147.10.43.0 sólo es válida dentro de la LAN donde se aplica el subneteo.

### 2.5.3 Cómo establecer la dirección de la máscara de subred

La selección del número de bits a utilizar en el proceso de división en subredes dependerá del número máximo de Hosts que se requiere por subred. Es necesario tener una buena comprensión de la matemática binaria básica y del valor de posición de los bits en cada octeto para calcular el número de subredes y Hosts creados cuando se pide bits prestados.

| Bits pedidos | 1   | 2  | 3  | 4  | 5 | 6 | 7 | 8 |
|--------------|-----|----|----|----|---|---|---|---|
| Valor        | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

Figura 2.54 Relación de bits prestados por hosts resultantes



Es posible que los últimos dos bits del último octeto nunca se asignen a la subred, sea cual sea la clase de dirección IP. Estos bits se denominan los dos últimos bits significativos. El uso de todos los bits disponibles para crear subredes, excepto los dos últimos, dará como resultado subredes con sólo dos Hosts utilizables. Este es un método práctico de conservación de direcciones para el direccionamiento de enlace serial de Routers. Sin embargo, para una LAN que está en funcionamiento, puede que esto origine gastos prohibitivos en equipos.

|                           |     |     |     |     |     |     |     |     |
|---------------------------|-----|-----|-----|-----|-----|-----|-----|-----|
| Formato de barra diagonal | /25 | /26 | /27 | /28 | /29 | /30 | N/A | N/A |
| Máscara                   | 128 | 192 | 224 | 240 | 248 | 252 | 254 | 255 |
| Bits pedidos              | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   |
| Valor                     | 128 | 64  | 32  | 16  | 8   | 4   | 2   | 1   |

Figura 2.55 Relación de bits prestados por máscara de red

La máscara de subred da al Router la información necesaria para determinar en qué red y subred se encuentra un Host determinado. La máscara de subred se crea mediante el uso de 1s binarios en los bits de red. Los bits de subred se determinan mediante la suma de los valores de las posiciones donde se colocaron estos bits. Si se pidieron prestados tres bits, la máscara para direcciones de Clase C sería 255.255.255.224. Esta máscara se puede representar con una barra inclinada seguida por un número, por ejemplo /27. El número representa el número total de bits que fueron utilizados por la red y la porción de subred.

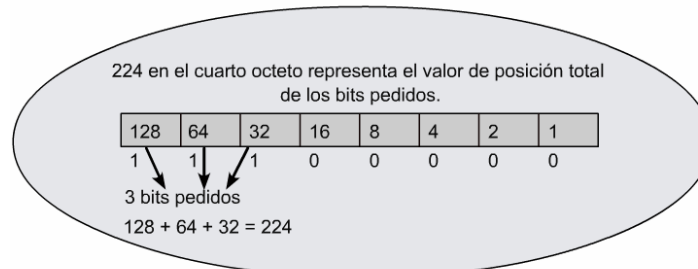


Figura 2.56 Bits prestados

Para determinar el número de bits que se deberán utilizar, el diseñador de redes calcula cuántos Hosts necesita la subred más grande y el número de subredes necesarias. Como ejemplo, la red necesita 30 Hosts y cinco subredes. Una manera más fácil de calcular cuántos bits reasignar es utilizar la tabla de subredes. Al consultar la fila denominada "Hosts Utilizables", se ve en la tabla que para 30 Hosts se requieren tres bits. La tabla también muestra que esto crea seis subredes utilizables, que satisfacen los requisitos de este esquema. La diferencia entre las direcciones válidas y el total es el resultado del uso de la primera dirección como el ID de la subred y de la última como la dirección de broadcast para cada subred.



El tomar prestados el número adecuado de bits para obtener un número determinado de subredes y de hosts por subred puede generar el desperdicio de direcciones válidas en algunas subredes. La habilidad de usar estas direcciones no la proporciona un enrutamiento con distinción de clase. Sin embargo, el enrutamiento sin distinción de clase, el cual se cubrirá más adelante en el curso, permite el uso de estas direcciones.

| Formato de barra diagonal       | /25 | /26 | /27 | /28 | /29 | /30 | No es aplicable | No es aplicable |
|---------------------------------|-----|-----|-----|-----|-----|-----|-----------------|-----------------|
| Máscara                         | 128 | 192 | 224 | 240 | 248 | 252 | 254             | 255             |
| Bits pedidos                    | 1   | 2   | 3   | 4   | 5   | 6   | 7               | 8               |
| Valor                           | 128 | 64  | 32  | 16  | 8   | 4   | 2               | 1               |
| Subredes totales                |     | 4   | 8   | 16  | 32  | 64  |                 |                 |
| Subredes que se pueden utilizar |     | 2   | 6   | 14  | 30  | 62  |                 |                 |
| Hosts totales                   |     | 64  | 32  | 16  | 8   | 4   |                 |                 |
| Hosts que se pueden utilizar    |     | 62  | 30  | 14  | 6   | 2   |                 |                 |

Figura 2.57 Relación bits-mascara-hosts

El método que se utilizó para crear la tabla de subred puede usarse para resolver todos los problemas con subredes. Este método utiliza la siguiente fórmula:

- El número de subredes que se pueden usar es igual a dos a la potencia del número de bits asignados a subred, menos dos. La razón de restar dos es por las direcciones reservadas de ID de red y la dirección de broadcast.

**(2 potencia de bits prestados) – 2 = subredes utilizables**

$$(2^3) - 2 = 6$$

- Número de Hosts utilizables = dos elevado a la potencia de los bits restantes, menos dos (direcciones reservadas para el ID de subred y el broadcast de subred)

**(2 potencia de los bits restantes del Host) – 2 = Hosts utilizables**

$$(2^5) - 2 = 30$$



## 2.5.4 Aplicación de la máscara de subred

Una vez que la máscara está establecida, puede utilizarse para crear el esquema de subred. La tabla de la Figura es un ejemplo de subredes y direcciones que se crean al asignar tres bits al campo de la subred. Esto creará ocho subredes con 32 Hosts por subred. Comience desde cero (0) al asignar números a las subredes. La primera subred es siempre llamada subred cero.

| Subred N | ID de subred   | Rango de hos | ID de broadcast |
|----------|----------------|--------------|-----------------|
| 0        | 192.168.10.0   | .1--.30      | 192.168.10.31   |
| 1        | 192.168.10.32  | .33--.62     | 192.168.10.63   |
| 2        | 192.168.10.64  | .65--.94     | 192.168.10.95   |
| 3        | 192.168.10.96  | .97--.126    | 192.168.10.127  |
| 4        | 192.168.10.128 | .129--.158   | 192.168.10.159  |
| 5        | 192.168.10.160 | .161--.190   | 192.168.10.191  |
| 6        | 192.168.10.192 | .193--.222   | 192.168.10.223  |
| 7        | 192.168.10.224 | .225--.254   | 192.168.10.255  |

Figura 2.58 Ejemplo de subred

Al llenar la tabla de subred, tres de los campos son automáticos, otros requieren de cálculos. El ID de subred de la subred 0 equivale al número principal de la red, en este caso 192.168.10.0. El ID de broadcast de toda la red es el máximo número posible, en este caso 192.168.10.255. El tercer número representa el ID de subred para la subred número siete. Este número consiste en los tres octetos de red con el número de máscara de subred insertado en la posición del cuarto octeto. Se asignaron tres bits al campo de subred con un valor acumulativo de 224. El ID de la subred siete es 192.168.10.224. Al insertar estos números, se establecen puntos de referencia que verificarán la exactitud cuando se complete la tabla.

| Formato de barra diagonal       | /25 | /26 | /27 | /28 | /29 | /30 | No es aplicable | No es aplicable |
|---------------------------------|-----|-----|-----|-----|-----|-----|-----------------|-----------------|
| Máscara                         | 128 | 192 | 224 | 240 | 248 | 252 | 254             | 255             |
| Bits pedidos                    | 1   | 2   | 3   | 4   | 5   | 6   | 7               | 8               |
| Valor                           | 128 | 64  | 32  | 16  | 8   | 4   | 2               | 1               |
| Subredes totales                |     | 4   | 8   | 16  | 32  | 64  |                 |                 |
| Subredes que se pueden utilizar |     | 2   | 6   | 14  | 30  | 62  |                 |                 |
| Hosts totales                   |     | 64  | 32  | 16  | 8   | 4   |                 |                 |
| Hosts que se pueden utilizar    |     | 62  | 30  | 14  | 6   | 2   |                 |                 |

Figura 2.59 Relación bits-mascara-hosts

Al consultar la tabla de subredes o al utilizar la fórmula, los tres bits asignados al campo de la subred darán como resultado 32 Hosts en total, asignados a cada subred. Esta información da el número de pasos de cada ID de subred. El ID de cada subred se establece agregando 32 a cada número anterior, comenzando con cero. Observe que el ID de la subred tiene ceros binarios en la porción de Host.

El campo de broadcast es el último número en cada subred, y tiene unos binarios en la porción de Host. La dirección tiene la capacidad de emitir broadcast sólo a los miembros de una sola subred. Ya que el ID de subred para la subred cero es 192.168.10.0 y hay un total de 32 Hosts, el ID de broadcast será 192.168.10.31 Comenzando con el cero, el trigésimo segundo número secuencial es el 31. Es importante recordar que cero (0) es un número real en el mundo de networking.

El resultado de la columna ID de broadcast puede completarse usando el mismo proceso que fue utilizado para la columna ID de la subred. Simplemente agregue 32 al ID de broadcast anterior de la subred. Otra opción es comenzar por el final de la columna y calcular hacia arriba restando uno al ID de subred anterior.



## CAPITULO 3

# Arquitectura de una red celular 3G CDMA2000

### 3.1 Introducción

Como ya se vio en el primer capítulo **CDMA** es un modo de acceso múltiple implementado por la Modulación de Espectro Disperso. Diferente a FDMA y TDMA, en ambos la información del usuario es separada en términos de tiempo y frecuencia, CDMA puede transmitir la información de múltiples usuarios en un canal al mismo tiempo. Es decir, se permite la interferencia mutua entre usuarios. La clave es que cada información antes de la transmisión debe ser modulada por diferentes códigos secuenciales de espectro disperso para la señal de banda ancha, entonces todas las señales deben ser mezcladas y enviadas. La señal mezclada debe ser demodulada por diferentes secuencias de códigos de espectro disperso en los diferentes receptores. Debido a que todos los códigos secuenciales de espectro disperso son ortogonales, solo la información que fue demodulada por el mismo código secuencial del espectro disperso puede ser revertido en la señal mezclada.

Entre las razones para el desarrollo de CDMA2000 EV encontramos las siguientes:

- Voz: baja velocidad, simétrico, ráfagas de baja velocidad
- Datos: ráfagas de alta velocidad, asimétrico, requerimientos BER bajos

El proceso de evolución de CDMA2000 EV ha sido el siguiente:

Fase 1: 1XEV-DO ( solo datos/ Datos optimizados)

Proporciona el soporte de servicios de paquetes de datos en lugar de servicios de voz en tiempo real.

Fase 2: 1XEV-DV ( voz y datos)

Proporciona servicios de paquetes de datos en tiempo no real y servicios de voz en tiempo real

Para el caso que estudiaremos, el sistema trabajará en la frecuencia de los 450 MHz cuyos rangos en la banda clase 5 los encontramos en la siguiente tabla





CDMA Band Class 5 (450 MHz)

| Block Designator | CDMA Channel Validity | CDMA Channel Number | Transmit Frequency Band |                |                |                |
|------------------|-----------------------|---------------------|-------------------------|----------------|----------------|----------------|
|                  |                       |                     | Mobile station          |                | Base Station   |                |
| A (4.5 MHz)      | Not Valid             | 121 - 125           | 453.000                 | 453.100        | 463.000        | 463.100        |
|                  | <b>Cond. Valid</b>    | <b>126 - 145</b>    | <b>453.125</b>          | <b>453.600</b> | <b>463.125</b> | <b>463.600</b> |
|                  | <b>Valid</b>          | <b>146 - 275</b>    | <b>453.625</b>          | <b>456.850</b> | <b>463.625</b> | <b>466.850</b> |
|                  | Not Valid             | 276 - 300           | 456.875                 | 457.475        | 466.875        | 467.475        |
| A' (0.5 MHz)     | Not Valid             | 101 - 120           | 452.500                 | 452.975        | 462.500        | 462.975        |
| B (4.5 MHz)      | Not Valid             | 81 - 105            | 452.000                 | 452.600        | 462.000        | 462.600        |
|                  | <b>Valid</b>          | <b>106 - 235</b>    | <b>452.625</b>          | <b>455.850</b> | <b>462.625</b> | <b>465.850</b> |
|                  | Not Valid             | 236 - 260           | 455.875                 | 456.475        | 465.875        | 466.475        |
| C (4.8 MHz)      | Not Valid             | 1 - 25              | 450.000                 | 450.600        | 460.000        | 460.600        |
|                  | <b>Valid</b>          | <b>26 - 168</b>     | <b>450.625</b>          | <b>454.175</b> | <b>460.625</b> | <b>464.175</b> |
|                  | Not Valid             | 169 - 193           | 454.200                 | 454.800        | 464.200        | 464.800        |
| D (4.2 MHz)      | Not Valid             | 539 - 563           | 411.675                 | 412.275        | 421.675        | 422.275        |
|                  | <b>Valid</b>          | <b>564 - 681</b>    | <b>412.300</b>          | <b>415.225</b> | <b>422.300</b> | <b>425.225</b> |
|                  | Not Valid             | 682 - 706           | 415.250                 | 415.850        | 425.250        | 425.850        |
| E (4.5 MHz)      | Not Valid             | 692 - 716           | 415.500                 | 416.100        | 425.500        | 426.100        |
|                  | <b>Valid</b>          | <b>717 - 846</b>    | <b>416.125</b>          | <b>419.350</b> | <b>426.125</b> | <b>429.350</b> |
|                  | Not Valid             | 847 - 871           | 419.375                 | 419.975        | 429.375        | 429.975        |
| F (4.5 MHz)      | Not Valid             | 1792 - 1822         | 479.000                 | 479.600        | 489.000        | 489.600        |
|                  | <b>Valid</b>          | <b>1823 - 1985</b>  | <b>479.620</b>          | <b>482.860</b> | <b>489.620</b> | <b>492.860</b> |
|                  | Not Valid             | 1986 - 2016         | 482.880                 | 483.480        | 492.880        | 493.480        |
| G (4.76 MHz)     | Not Valid             | 1235 - 1265         | 455.230                 | 455.830        | 465.230        | 465.830        |
|                  | <b>Valid</b>          | <b>1266 - 1442</b>  | <b>455.850</b>          | <b>459.370</b> | <b>465.850</b> | <b>469.370</b> |
|                  | Not Valid             | 1443 - 1473         | 459.390                 | 459.990        | 469.390        | 469.990        |
| H (4.42 MHz)     | Not Valid             | 1039 - 1069         | 541.310                 | 451.910        | 551.310        | 461.910        |
|                  | <b>Valid</b>          | <b>1070 - 1229</b>  | <b>451.930</b>          | <b>455.110</b> | <b>461.930</b> | <b>465.110</b> |
|                  | Not Valid             | 1230 - 1260         | 455.130                 | 455.730        | 465.130        | 465.730        |

Figura 3.1 Rangos en la banda clase 5 en CDMA2000

### 3.2 Técnicas y Tecnologías CDMA2000

CDMA utiliza varios principios para su funcionamiento. Por ejemplo, la ortogonalidad de una señal es importante para que el sistema funcione, ya que los códigos Walsh usados en CDMA son una secuencia de señales ortogonales. Para saber que tanto es ortogonal o no una señal con respecto a otra ubicamos su correlación en el espectro del tiempo.

La correlación es medida de manera similar con alguna señal arbitraria. Esto es multiplicando las señales y sumando (integrando) el resultado sobre ventanas de tiempo definidas. La correlación es 100% cuando las funciones son paralelas. La correlación es 0% cuando las funciones son ortogonales.

Para la propagación de la señal, a cada símbolo se le aplica XOR con todos los chips en la secuencia ortogonal (como mencionamos, el sistema CDMA utiliza la secuencia Walsh) asignada a cada usuario. El resultado de la secuencia es procesado y transmitido sobre todo el canal físico con los demás símbolos propagados. En esta figura, se utiliza un código de 4 dígitos. El producto de los símbolos de usuario y el código propagado es una secuencia de dígitos que deben ser transmitidos a 4 veces la velocidad de la señal binaria original codificada.



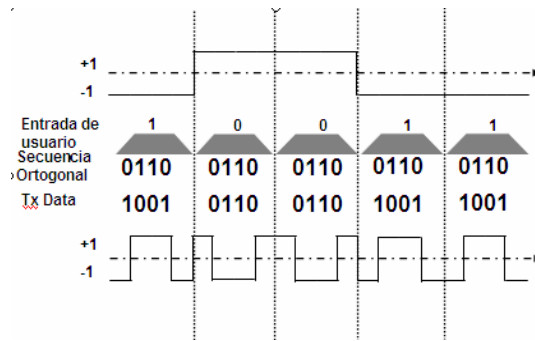


Figura 3.2 Secuencia de código de 4 dígitos WALSH

El receptor "des-dispersa" los chips utilizando el mismo código Walsh que se ocupó en el transmisor. Note que bajo condiciones sin ruido, los símbolos o dígitos son completamente recuperados sin error alguno. En realidad, el canal no es libre de ruido, pero el sistema CDMA emplea técnicas de corrección de error para eliminar los efectos de ruido y mejorar el desempeño del sistema.

Cuando se utiliza una secuencia Walsh equivocada para la "des-dispersión", la correlación resultante produce un promedio cero. Esta es una muestra clara de las ventajas de la propiedad de ortogonalidad de los códigos Walsh. Si un código equivocado es erróneamente utilizado por el usuario destino o algún otro usuario intenta decodificar la señal recibida, el resultado de la correlación es siempre cero debido a la propiedad de ortogonalidad de las secuencias Walsh.

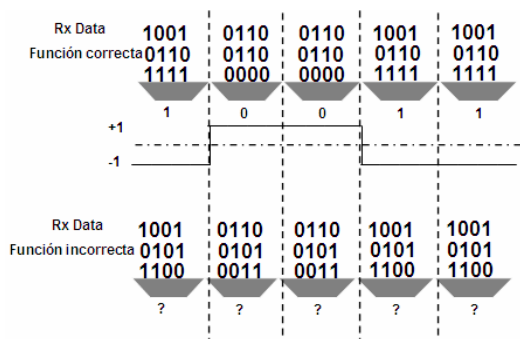


Figura 3.3 Correlación en la ortogonalidad de la secuencia WALSH

El código Walsh es generado a partir de un proceso inicializado con una semilla de 0, en forma de matriz o bloque se va complementando por el número inverso correspondiente, es decir donde hay ceros se pondrán unos y viceversa, tal como lo muestra la figura:

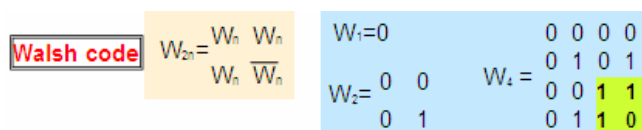


Figura 3.4 Inicialización del código WALSH

Podemos partir para una mejor comprensión del funcionamiento de CDMA con lo que es el flujo de señal en esta tecnología:

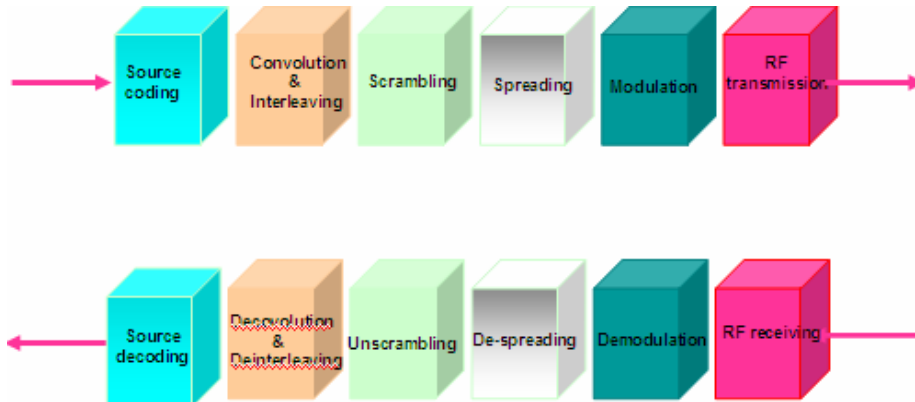
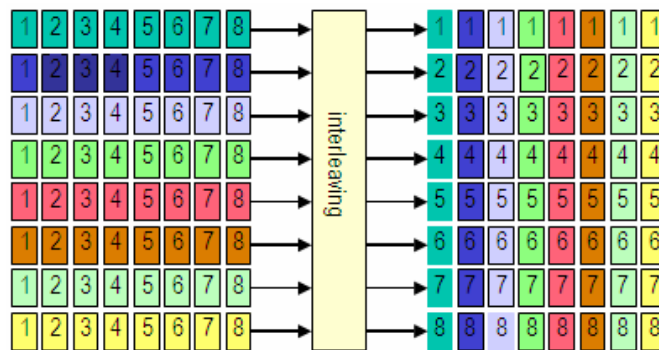


Figura 3.5 Flujo de señal de CDMA

- 1) Los códigos fuente pueden incrementar la eficiencia de la transmisión.
- 2) La codificación de canal (Convolución e Interleaving) puede hacer la transmisión más confiable.



Dirección del flujo de datos  
 →  
 Figura 3.6 Interleaving

En la figura se puede ver que los datos son leídos fila por fila dentro del interleaver para la transmisión, leídos columna por columna a la salida (este proceso es llamado interleaving) y propagados después de otro proceso de modulación.

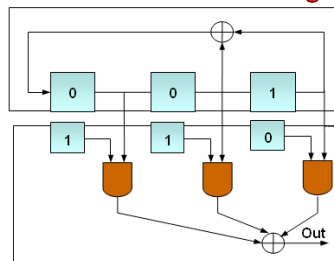
Entonces, los datos ingresan al interleaver en el receptor fila por fila y son leídos columna por columna (este proceso es llamado de-interleaving). Actualmente, se considera que en el curso de la propagación, cuando dos filas de datos son transmitidas, consecutivamente ocurren errores en los códigos en el 2o, 3o y 4o bits como resultado del desvanecimiento u otras razones, como se muestra en la figura en el lado izquierdo.

Si los datos originales han sido transmitidos después del interleaving, el segundo bit de la fila 2, el segundo bit de la fila 3 y el segundo bit de la fila 4 deben haber sido errores en el código después de que se obtuvo la salida columna por columna en el receptor.

Debido a que los códigos de corrección de errores pueden procesar fácilmente códigos de error discretos, la parte de recepción puede recuperar fácilmente las señales después del de-interleave en señales originales por medio de la corrección de errores, pero no siempre se puede obtener la recuperación de estas señales como resultado de errores de código consecutivos. Así mismo, el interleave puede superar el rápido desvanecimiento causado durante la transmisión de señales en el aire. Las funciones del código interleave rara vez corrigen errores por causa de bajo desvanecimiento, a causa del bajo desvanecimiento puede resultar en errores de códigos consecutivos, si en toda la trama hay errores. Así mismo, ocurrirán errores consecutivos después del de-interleaving. La figura muestra la forma más simple de interleave y el interleave en las aplicaciones actuales son mucho más complejos.

3) El Scrambling puede hacer la transmisión segura.

### Secuencia de Scrambling (M)



- 2 puntos son importantes aquí:
  - ⇒ Máximo número de cambios de registro (N)
  - ⇒ Mascara
- El periodo de la frecuencia de salida es  $2^N-1$  bits
- Solo la secuencia de offset cambia cuando la mascara cambia
- PN soporta Secuencia de ruido pseudoaleatoria

Figura 3.7 Scrambling

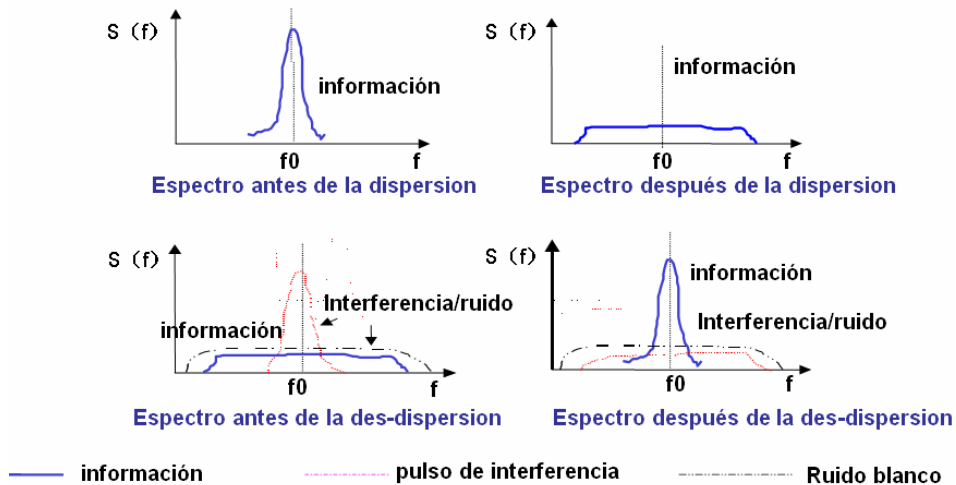
En el sistema CDMA, la información del usuario es encriptada por medio de scrambling. El código scramble usado aquí es de secuencia M. La figura muestra un generador de secuencia M que consta de flip-flops y una mascara. El periodo de la salida es  $2^N-1$  (donde N es el número de registros). Es decir, la secuencia de los registros asume el estado inicial cada  $2^N-1$  códigos a la salida. En el sistema CDMA, existen dos clases de secuencias M, una es long code con un periodo  $2^{42}-1$  y la otra es short code periodo  $2^{15}-1$ . Para scrambling se utiliza long code mientras que para demodulación subsecuente se utiliza short code.

Se puede ver que para diferentes mascarar, a la salida de un registro de corrimiento secuencial se obtienen diferentes secuencias  $M$ , a las cuales llamamos diferentes fases. Actualmente, diferentes mascarar en CDMA son asignadas a diferentes usuarios, los cuales son habilitados para obtener diferentes secuencias  $M$ .

4) El Spreading puede incrementar la capacidad de controlar la interferencia.

### Dispersión y Des-dispersión

La mejora de la velocidad de la información en el dominio del tiempo se refiere a que la información en el dominio del espectro es dispersada



$S(f)$  es la densidad de energía.

Figura 3.8 Dispersión y Des-dispersión

Los sistemas tradicionales de comunicación de radio transmiten datos utilizando el mínimo de ancho de banda requerido para llevarlos como una señal de banda angosta. Los sistemas de Espectro Disperso de Secuencia Directa (Direct-Sequence Spread Spectrum) mezclan sus entradas de datos con una secuencia rápida de propagación y transmiten una señal en banda ancha, como es nuestro caso de CDMA.

La secuencia propagada es independientemente regenerada en el receptor y mezclada con la señal de banda ancha entrante para recuperar los datos originales. La unión da una ganancia sustancial proporcional al ancho de banda de la señal de espectro disperso. La ganancia puede ser usada para incrementar el desempeño del sistema y también el rango, o permitir múltiples códigos de usuarios, o ambos. Una cadena de bits digital enviada sobre un enlace de radio requiere un ancho de banda definido para que sea exitosamente transmitido y recibido.

5) A través de la modulación, las señales transferirán las señales de radio desde las señales digitales.



Por otro lado, CDMA se caracteriza por las técnicas utilizadas en los siguientes tres aspectos

a) Control de Potencia:

En un sistema inalámbrico, hay un problema muy conocido llamado problema far/near (lejos/cerca). La distribución del suscriptor es aleatoria. Algunos móviles pueden estar cerca de la estación base, mientras otros pueden estar lejos de ella. Como resultado, las trayectorias perdidas y multi-trayectorias ambientales afectan las señales de diferentes móviles que muestran una gran variabilidad. Si cada móvil transmite a la misma potencia, la estación base puede recibir una señal muy fuerte de un móvil cercano, junto con otra señal de uno que este distante; y la señal débil podría ser opacada por la fuerte.

Para controlar este problema, cada móvil no puede enviar señales con la misma potencia. La tecnología que controla la potencia se llama control de potencia. El propósito del control de potencia es asegurar que todas las señales lleguen a la estación base aproximadamente al mismo nivel. Este requerimiento hace que el control de potencia en dirección inversa sea extremadamente crítico y demandante.

Existen varios tipos de control de potencia, solo los mencionaremos ya que la explicación de cada uno de ellos rebasa los objetivos de este trabajo:

- Reverse power control
  - ⇒ Loop abierto de power control
  - ⇒ Loop cerrado de power control
    - Loop interno de power control: 800 Hz
    - Loop externo de power control
- Forward power control
  - ⇒ Modo de transmisión de mensajes:
    - Umbrales de transmisión
    - Transmisión periodica
  - ⇒ Loop power control

b) Traspaso o HandOff:

En el sistema inalámbrico, existe handoff (o handover), en el sistema CDMA como ya se mencionó en el capítulo 1, existen tres tipos de traspaso o handoff que son: hard handoff ,soft handoff y softer handoff.

- Soft handoff
  - ⇒ Es el proceso para establecer un link con un sector antes de romper el link con el sector que da el servicio



- Softer handoff
  - ⇒ Como el soft handoff, pero el handoff ocurre entre multi-sectores en la misma base station
- Hard handoff
  - ⇒ Hard handoff ocurre cuando 2 sectores no se sincronizan o no están en la misma frecuencia. Interrupción en la voz o en los datos ocurre pero esto no interrumpe la comunicación del usuario

c) Diversidad y RAKE:

La diversidad se refiere a que después de recibir dos o mas señales de entrada con desvanecimiento mutuamente no correlacionado al mismo tiempo, el sistema demodula estas señales y las agrega. Así mismo, el sistema puede recibir mas señales y controlar el desvanecimiento.

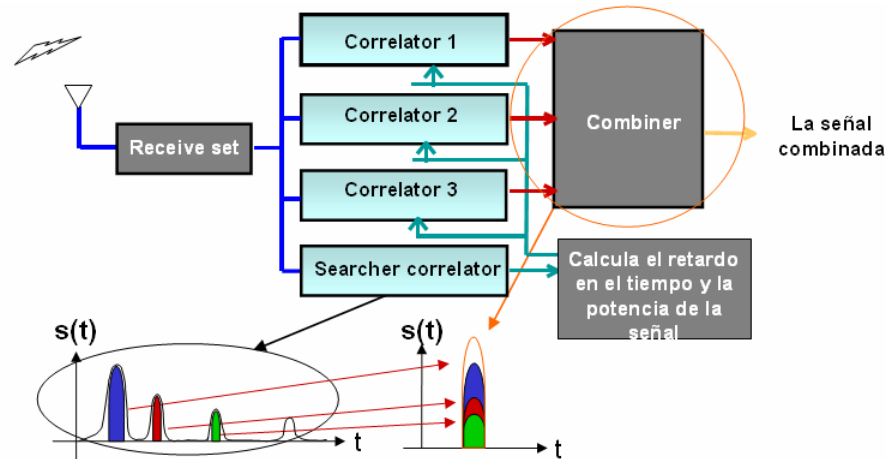
Un canal de comunicación móvil es un canal de desvanecimiento multi-trayectoria y alguna señal transmitida alcanza a recibir la terminal por medio de múltiples trayectorias de transmisión, tales como transmisión directa, reflexión, difusión, etc. Además, con el movimiento del móvil, la amplitud de la señal retarda y su fase en varias trayectorias de transmisión varía con el tiempo y espacio. Por consiguiente los niveles de señales recibidas son fluctuantes e inestables y estas señales multi-trayectoria, tenderán al desvanecimiento. La media del campo de fuerza del desvanecimiento Rayleigh tiene cambios relativamente suaves y es llamado “desvanecimiento lento”. Y esto conforma una distribución normal.

La diversidad tecnológica es una manera eficiente de controlar el desvanecimiento. Puede ser seleccionado en términos de la frecuencia, tiempo y espacio, la diversidad incluye diversidad en frecuencia, tiempo y espacio.

El receptor RAKE es una técnica la cual utiliza diversos correladores en banda base para procesos individuales de los componentes de la señal multi-trayectoria. Las salidas de diferentes correladores son combinadas para lograr la mejora de confiabilidad y desempeño.

Cuando los sistemas CDMA fueron diseñados para los sistemas celulares, las señales con amplio ancho de banda inherentes con sus funciones Walsh ortogonales fueron naturales para la implementacion del receptor RAKE. En CDMA, el ancho de banda es mayor que el ancho de banda coherente del celular. Así mismo, cuando los componentes de la multi-trayectoria son resueltos en el receptor, las señales desde cada toma en la línea de retardo son no correlacionadas con las demás. El receptor puede combinarlas utilizando esquemas. El sistema CDMA entonces utiliza características multitrayectoria del canal como ventaja para mejorar la operación del sistema. Un receptor RAKE utiliza múltiples correladores para separar y detectar el componente multi-trayectoria M mas fuerte en el enlace.

En el sistema CDMA, el enlace hacia adelante utiliza un receptor tridente, y el enlace inverso utiliza uno de cuatro vías. La detección y medición de los parámetros de la multi-trayectoria son desempeñados por un correlador.



Antenas RAKE ayudan al multipath y mejoran el desempeño de la recepción del sistema

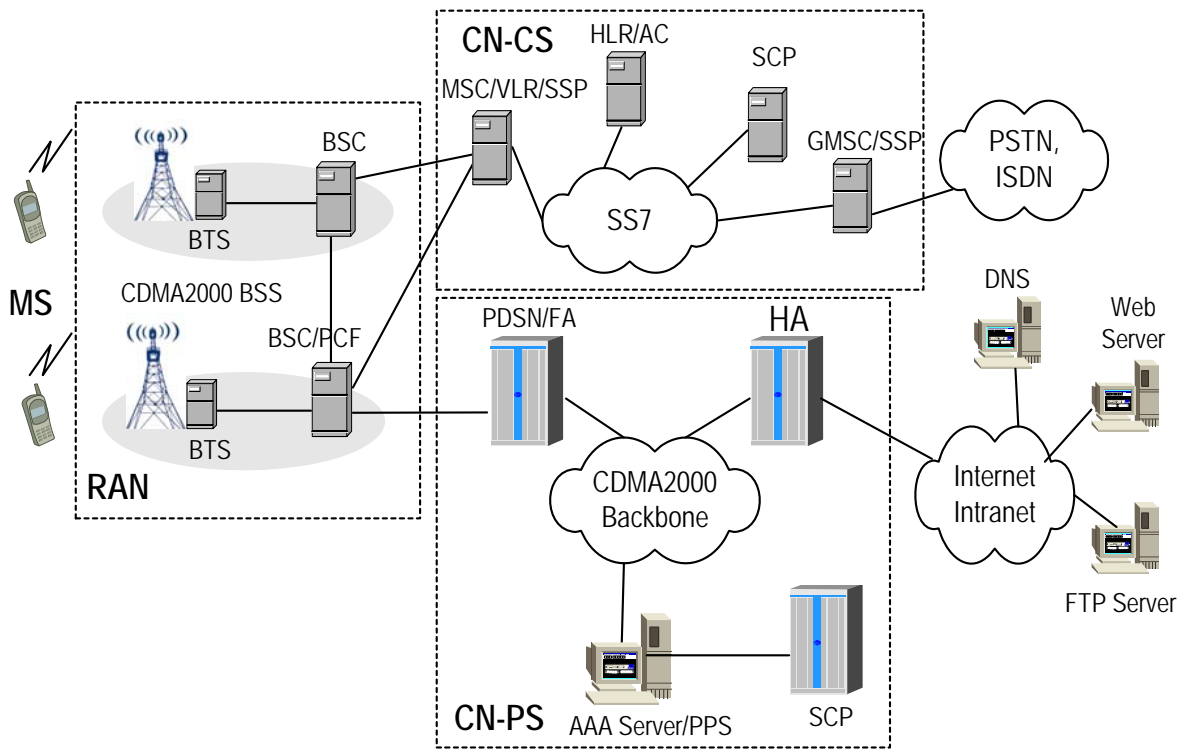
Figura 3.9 Principio del receptor RAKE

### 3.3 Arquitectura de la red CDMA2000

Como uno de los principales estándares en tecnología 3G, CDMA2000 soporta altas tasas de transmisión de paquetes de bits además del tradicional servicio de llamada de voz. Como se muestra en la figura 4-1 una red CDMA2000 principalmente consiste en lo siguiente:

- Estación Móvil (EM o MS por sus siglas en inglés): Una EM es el dispositivo móvil de un usuario, que es capaz de hacer y recibir llamadas vía un interfaz de aire. Para proporcionar servicio de datos, la EM establece un enlace lógico con el PS.
- Red de Acceso por Radio (RAR o RAN por sus siglas en inglés): La RAR maneja todas las funciones inalámbricas.
- Red Central (CN Core Network en inglés) - Conmutación de Circuito (RC- CC o por sus siglas en inglés CN-CS): El dominio CC proporciona servicios de tipo de circuito, conectando la Red Telefónica Pública (PSTN) u otras redes de CS externas
- Red Central – Conmutación de Paquetes (RC- CP o por sus siglas en inglés CN-PS): El dominio CP proporciona servicios de paquetes de datos, conectando la Internet u otras Redes de Datos Públicas. (PDNs).





MS: Mobile Station  
Estación Móvil

CN-CS: Core Network-Circuit Switching  
Comutación de Paquetes - Red Central  
BSS: Base Station Subsystem  
Subsistema de Estación Base  
BSC: Base Station Controller  
Controlador de Estación Base  
PDSN: Packet Data Serving Node  
Nodo de Servicio de Paquetes de Datos

HA: Home Agent  
Agente local domestico  
PPS: PrePaid Server  
Servidor de Prepago

RAN: Radio Access Network  
Red de Acceso de Radio

CN-PS: Core Network-Packet Switching  
Comutación de paquetes – Red Central  
BTS: Base Transceiver Station  
Estación Transreceptora base  
PCF: Packet Control Function  
Función de Control de Paquetes

FA: Foreign Agent  
Agente extranjero  
AAA: Authentication, Authorization,  
Accounting Server  
Servidor Autenticación, Autorización y  
Contabilidad  
SCP: Service Control Node  
Nodo de Control de Servicio

Figura 3.10 Arquitectura de un sistema de red CDMA2000



## CAPITULO 4

# Arquitectura y Funcionamiento del PDSN9660 (Nodo de Servicio de Paquetes de Datos)

### 4.1 EI PDSN en la red CDMA2000

El Nodo de Servicio de Paquetes de Datos (de ahora en adelante PDSN por sus siglas en ingles) proporciona el acceso a Internet, intranets y a los servidores para estaciones móviles que utilizan una Red de Acceso de Radio CDMA2000 (RAN). Actuando como una compuerta de acceso (Gateway). El PDSN proporciona acceso IP simple e IP móvil, soporte de un agente extranjero (FA) y el transporte de paquetes para las redes privadas virtuales. Actúa como cliente de los servidores de Autenticación, Autorización, y Contabilidad (o por sus siglas en inglés AAA) y provee a las estaciones móviles de una entrada a la red IP.

La Red Central de Conmutación de Paquetes (CN-PS) en el dominio CDMA2000 consiste de las siguientes entidades de red: el PDSN/FA, HA, servidor AAA PPS, SCP, etcétera. Esta solución permite a una EM tener acceso a la Red de Datos de Paquete Externa (PDN) en el modo IP simple o IP móvil, realizando servicios de paquete y servicios de tarificación (incluyendo las modalidades pospago y prepago).

Las principales características de las entidades de red en la CN-PS son las siguientes:

#### I. PDSN

El nodo de servicio de paquetes de datos (PDSN) es un dispositivo de entrada entre el PDN y el sistema de comunicación CDMA2000 móvil, que permite a una EM tener acceso a la red IP y provee a la EM el servicio de paquete de datos. Las funciones del PDSN son las descritas a continuación:

- Sirve como un dispositivo de entrada (gateway). Puede establecer y terminar sesiones PPP entre el PDSN y la EM dejando a la EM tener acceso al PDN. Este papel es similar al del Servidor de Acceso de Red (NAS por sus siglas en inglés) en la tradicional red de marcado o dialup.



- Provee acceso de IP simple. El PDSN es responsable de asignar una dirección IP a una EM (o pide al AAA hacerlo).
- Provee acceso IP móvil. Para hacer esto, la funcionalidad de FA es integrada al PDSN. De este modo, el PDSN/FA sirve tanto como dispositivo de entrada como un FA de la red a la cual la MS tiene acceso.
- Cliente AAA para el servicio de postpago. Esta a cargo de recopilar la información de la tarificación del servicio de paquetes y de enviar dicha información al servidor AAA.
- Cliente de prepago para el servicio prepago. Es responsable de solicitar cuotas para los usuarios y supervisar el uso de estas.

## II. HA

El Agente Local ó Domestico (o Home Agent por sus siglas en ingles HA) es una nueva entidad que soporta IP móvil. De hecho, esto es un ruteador mejorado, que es añadido con la función de mantener la información de ubicación. Las funciones principales del HA son las siguientes:

- Enviar de mensajes de anuncio, ayudando a una EM a saber si esta en la red local
- Manejar el registro de las solicitudes de una EM y contestarlas; así como establecer los Registros de Movilidad Fijados (Mobility Binding Records) entre la dirección de la ES local y la dirección del encargado actual
- Agencia y reenvío. El HA anuncia la accesibilidad de la dirección local de la EM para que de este modo todos los paquetes destinados a la dirección local de la EM se redirijan a la red local. Después de encapsular los paquetes destinados a la EM, el HA los envía al PDSN/FA. Finalmente, los paquetes son reenviados a la EM por el PDSN/FA.

## III. AAA Server

El Servidor de Autenticación, Autorización y Contabilidad (Servidor AAA) es principalmente usado para la autenticación, la autorización y la tarificación (contabilidad) de acuerdo al protocolo de Servicio de Usuario de Marcado de Autenticación Remota (Remote Authentication Dial In User Service, RADIUS por sus siglas en ingles). Las funciones principales del servidor AAA son las siguientes:

- Provee la Autenticación y Autorización a un usuario móvil. Esto puede diferenciar al usuario de servicio prepago y el usuario de servicio



postpago así como la autenticación y autorización de diferentes usuarios.

- Para usuarios de servicio postpago, este lleva la Tarificación.
- Para usuarios de servicio prepagados, el servidor AAA reenvía todos los cobros por lo usado y actualiza las solicitudes al PPS.

#### **IV. PPS**

El servidor de prepago (PPS) es una entidad recién añadida que soporta el servicio de pago por adelantado. Este pide al Nodo de Control (SCP) identificar el estado de cuenta de un usuario de servicio de pre-pago (pago por adelantado) y escoge una política de pre-pago para la sesión según sea la capacidad del PDSN. Las funciones principales del PPS son las siguientes:

- Provee la conversión de las tarifas. Puede convertir el dinero invertido en tiempo aire o descarga de datos de acuerdo a ciertas reglas asignadas al cliente de prepago y de acuerdo a las cuotas establecidas.
- Mantiene el uso de las cuotas de dinero solicitadas por el SCP. Cuando la cuota asignada es usada en su totalidad, el PPS debe solicitar la cuota de dinero adicional del SCP.
- Cuando el servicio de pre-pago ha terminado, el PPS devuelve la cuota de dinero restante al SCP y deduce el dinero usado por el usuario.

El sistema de servicio de pre-pago de algunos proveedores integra tanto el módulo AAA como el módulo PPS en la misma entidad física.

#### **V. SCP**

El SCP es también una entidad recién añadida sobre todo para soportar el servicio de pre-pago. La información de la cuenta de un suscriptor de servicio de pre-pago es grabada o guardada sobre el SCP. Las funciones del SCP son las siguientes:

- Manejar una cuenta unificada de un suscriptor de servicio de pre-pago. El gasto de un suscriptor sobre diferentes servicios es deducido de la cuenta unificada.
- Distribuir el dinero disponible a un suscriptor y deducir el dinero usado de la cuenta.
- Recibir la información de unidades de dinero enviadas por el PPS y añadir estas unidades de dinero a la cuenta del suscriptor.



En nuestro caso estudiado, la plataforma de hardware del PDSN9660 es en base a un Ruteador de Conmutación Universal (USR) del proveedor en cuestión. El USR es un dispositivo compacto, basado en normas de industria probadas. El software del PDSN9660 estudiado es desarrollado sobre la Plataforma de Ruteo Versátil (VRP), hereda las tecnologías básicas de las comunicaciones de datos, como la tecnología de ruteo integrada, la Calidad de Servicio IP (QoS), la Red Virtual Privada (VPN) y la tecnología de seguridad, además se amplían y mejoran las funciones basadas en los usos de comunicación inalámbricos.

Basado tanto en la plataforma de hardware que es dada por el USR, la alta fiabilidad así como en la gran capacidad en el manejo de datos, y la plataforma de software que integra a la perfección tecnologías de comunicación inalámbricas y tecnologías de comunicaciones de datos, el PDSN9660 provee soluciones ideales y flexibles para operadores de red con tecnología de comunicaciones de datos inalámbricas CDMA2000

## 4.2 Normas Compatibles y Protocolos por el PDSN9660

La red de datos CDMA2000 está basada en la tecnología IP. Por lo tanto, la red de datos de paquete CDMA2000 se adapta a los protocolos RFC definidos por IETF.

A continuación se presentan todas las normas CDMA2000 especiales así como los protocolos RFC, soportados por el PDSN9660.

### a) Normas especiales para CDMA2000

- TIA/EIA/IS-2001-A
- TIA/EIA/IS-2001-B
- TIA/EIA/IS-835
- TIA/EIA/IS-878
- TIA/EIA/IS-707-A
- TSB115 (PN-4286)
- A.S0001-A\_v2.0 (3GPP2 Standards and Protocols)
- P.S0001-A\_v3.0 (3GPP2 Standards and Protocols)
- P.S0001-B\_v1.0 (3GPP2 Standards and Protocols)
- X.S0011-0060-C (3GPP2 Standards and Protocols)

### b) Protocolos IETF

- RFC 768 User Datagram Protocol (UDP)
- RFC 791 Internet Protocol (IP)
- RFC 793 Transmission Control Protocol (TCP)
- RFC 826 Ethernet Address Resolution Protocol



- RFC 1144 Compressing TCP/IP Headers for Low-Speed Serial Links
- RFC 1256 ICMP Router Discovery Messages
- RFC1332 The PPP Internet Control Protocol (IPCP)
- RFC 1334 PAP Authentication Protocols
- RFC 1570 PPP LCP Extensions
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1662 PPP in HDLC Framing
- RFC 1701 Generic Routing Encapsulation (GRE)
- RFC 1702 Generic Routing Encapsulation over IPv4 Networks
- RFC 1962 The PPP Compression Control Protocol (CCP)
- RFC 1974 PPP Stac LZS Compression Protocol
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2002 IP Mobility Support
- RFC 2003 IP Encapsulation within IP
- RFC 2004 Minimal Encapsulation within IP
- RFC 2005 Applicability Statement for IP Mobility Support
- RFC 2006 The Definitions of Managed Objects for IP Mobility Support Using SMIv2
- RFC 2118 Microsoft Point-To-Point Compression (MPPC) Protocol
- RFC 2138 Remote Authentication Dial In User Service (RADIUS)
- RFC 2139 RADIUS Accounting
- RFC 2290 Mobile-IPv4 Configuration Option for PPP IPCP
- RFC 2344 Reverse Tunneling for Mobile IP
- RFC 2394 IP Payload Compression Using DEFLATE
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 The Internet Key Exchange (IKE)
- RFC 2475 Architecture for Differentiated Services
- RFC 2486 The Network Access Identifier
- RFC 2597 Assuring Forwarding PHB Group
- RFC 2661 Layer Two Tunneling Protocol "L2TP"
- RFC 2794 Mobile IP Network Access Identifier Extension for IPv4
- RFC 2865 Remote Authentication Dial In User Service (RADIUS)
- RFC 2866 RADIUS Accounting
- RFC 3012 Mobile IPv4 Challenge/Response Extensions
- RFC 3024 Reverse Tunneling for Mobile IP, revised

## 4.3 Arquitectura del sistema

### 4.3.1 Configuración de Hardware

El sistema del PDSN9660 se integra por los siguientes componentes: Gabinete, Switch para LAN, Ruteador AR28-80 y Firewall Eudemon200. Estos son montados en el gabinete N68-22 del proveedor en cuestión. El bosquejo del gabinete N68-22 se muestra en la figura 4.1 y la configuración típica del gabinete se muestra en la figura 4.2.

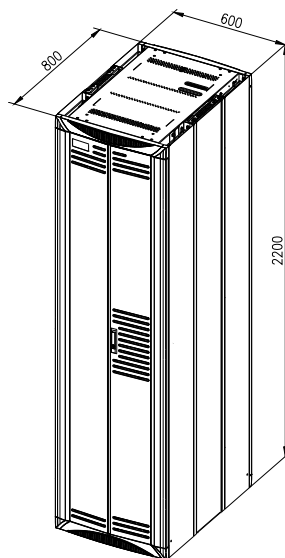


Figura 4.1 Bosquejo del gabinete N68-22 (in mm)

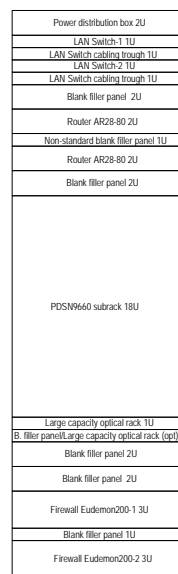


Figura 4.2 Configuración típica del gabinete PDSN9660 (1U=44.45mm)

De estos componentes:

- El subestante del PDSN es obligatorio. Las tarjetas principales de servicios que consiste en la SRU (Unidad de Ruteo), la SPU (Unidad de Procesamiento) y LPU (Unidad de Interfaces) que son insertadas en dicho subestante. Para que la fiabilidad del sistema sea mejorada, le recomiendan que dos SRU y dos SPU sean configurados. Ellos trabajan en el modo activo/de espera. Diferentes tipos de tarjeta de interfaz (LPU) pueden ser configurados según exigencias reales conectadas a una red.
- El ruteador AR28-80 es opcional. Cuando los tipos de las interfaces de un LPU del PDSN9660 no cumplen con las necesidades requeridas para conectarse a una red (por ejemplo, el modo E1 es usado para





conectar la red con el PCF), se pueden usar las interfaces y las funciones del ruteador AR28-80 para encontrar dichas necesidades. Si un usuario necesita la función de NAT, pero el ruteador del cual salen los datos no proporciona tal función, se puede usar la función NAT que es proporcionada por un ruteador AR28-80 o un Eudemon200.

- El LANSWITCH es opcional. En la interconexión real, el canal de control del dispositivo puede ser implantado por el LANSWITCH. Cuando el PDSN9660 se conecta una red con otros dispositivos (por ejemplo, un HA), este puede compartir un solo LANSWITCH
- El Firewall Eudemon200 es opcional. Es un dispositivo de seguridad colocado entre el PDSN9660 Y PDN externo. Si los clientes tienen demandas especiales sobre seguridad pueden comprar otros dispositivos de seguridad de manera personal.
- Para mejorar la fiabilidad de la conexión, se puede configurar dobles LANSWITCHES, dobles ruteadores AR28-80 y dobles Eudemon200s para hacerlos trabajar en el modo activo/de espera.

## TARJETAS

EL arreglo típico de las tarjetas en el PDSN del proveedor en cuestión se muestra en la figura 4.3.

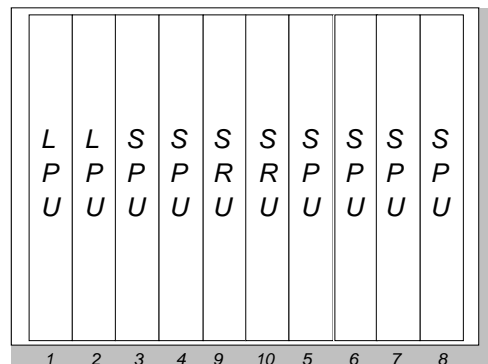


Figura 4.3 Arreglo Típico de tarjetas

SRU: Switching and routing unit.  
Unidad de Ruteo y Conmutación

SPU: Service processing unit.  
Unidad de Procesamiento de Servicio

LPU: Line interface processing unit.  
Unidad de Procesamiento de Interfaces



## I. SRU

El SRU es el núcleo del sistema de control. El SRU trabaja en el modo activo/ de reserva. Todo el sistema del PDSN9660 necesita sólo dos SRU, uno es activo y uno es de reserva. Estos son insertados en ranuras 9 y 10 del subestante del PDSN.

Las funciones principales del SRU son las siguientes:

- La SRU colecta la información del ruteador y genera una tabla de ruteo de acuerdo a la topología de red y el esquema definido por usuario. Luego entrega esta tabla a las tarjetas LPU y SPU.
- La SRU es el agente de Operación y Mantenimiento (O&M) del PDSN9660. Esta controla el sistema PDSN9660 según las órdenes del operador y colecta los parámetros que están corriendo para el operador.
- La SRU es el centro de conmutación de datagramas del PDSN9660. Recibe paquetes del LPU y procesa los paquetes según la información de control llevada por el datagrama, luego esta entrega el datagrama a la SPU para el siguiente proceso. En el sentido inverso, los paquetes habiendo sido procesados por el SPU también deberían ser examinados por la SRU antes de la expedición a la LPU.
- El SRU proporciona señales de reloj SDH muy confiables para la LPU y tiene como salidas dos señales de reloj (2048kHz y 2048kbit/s) para otros dispositivos

## II. SPU

La SPU proporciona todo el servicio que procesa la funcionalidad del PDSN9660. Un PDSN9660 puede ser configurado con hasta tres pares de SPU, cada par mantenido en un modo activo/de reserva, localizado en ranuras de 3/4, 5/6 y 7/8. La capacidad del PDSN depende de la capacidad de procesamiento de las SPU's. La capacidad de tratamiento de un par de SPU es de 100,000 conexiones PPP simultáneas. Así, la capacidad de procesamiento de un PDSN9660 en máxima capacidad es 300,000 conexiones PPP simultáneas.

## III. LPU

La LPU provee de interfaces físicas hacia la red externa (como el PCF, PDN y el servidor AAA), incluyendo los siguientes tipos de interfaces:

- Interface de Fast Ethernet (FE, 10/100Mbit/s)
- Interface Gigabit-Ethernet (GE, 1000Mbit/s)
- Interface Packet Over SDH (POS, 155/622Mbit/s)
- Modo Asíncrono de Transferencia (ATM, 155Mbit/s).

Un PDSN9660 es diseñado con dos LPUs, las cuales están en las ranuras 1 y 2 y son usadas para trabajar junto con dispositivos remotos de una red. Los LPUs puede realizar la redundancia activa/de reserva o la función compartida de carga.

La LPU esta encargada únicamente del reenvío de paquetes de información, no hace ningún tipo de procesamiento. Todo el procesamiento de servicios es realizado por las SPUs. La información de la tabla de ruteo para la LPU es emitida por la SRU.

### 4.3.2 Software

El diseño y la arquitectura del software PDSN9660 es mostrado en la siguiente figura 4.4.

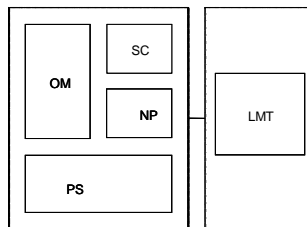


Figura 4.4 Arquitectura del software del PDSN9660

El software del PDSN9660 cuenta con 5 módulos:

- OM (operación y mantenimiento): Su función principal es el control y dirección de la operación y el mantenimiento, incluyendo la configuración, el control de alarmas, el control del funcionamiento del sistema, la resolución de la línea de comandos, etcétera.
- SPR, servicio de procesamiento de red (NSP por sus siglas en inglés “Network Service Process”): Este módulo funciona para reenviar paquetes, reenviando paquetes de una EM a la PDN o paquetes destinados a una EM del PDN.
- SC: (servicio de control): Este módulo procesa toda la información de señalización, como la señalización A11 y la señalización de tarificación.
- PS (servicio de plataforma): Este módulo proporciona el servicio de plataforma de todo el sistema de software del PDSN, incluyendo el establecimiento y el mantenimiento de la conexión PPP, la asignación de direcciones IP, la comunicación al AAA, la seguridad, VPNs, etcétera.
- Terminal de Mantenimiento Local (LMT, Local Maintenance Terminal, por sus siglas en inglés): Este módulo provee a los usuarios interfaces gráficas (GUI, Graphic User Interface)

## 4.4 Protocolos de interfaces

Como se muestra en la figura 4.5, el 3GPP2 define tres interfaces para PDSN incluyendo la interfaz A10, la interfaz A11 y la interfaz Pi.

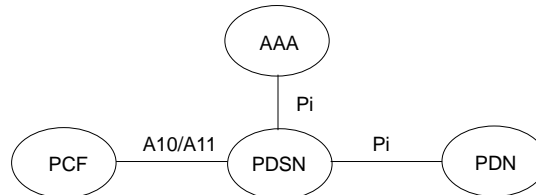


Figura 4.5 Interfaces del PDSN

### - Interfaz A11

La interfaz A11, es el interfaz de señalización entre PDSN y PCF. Un mensaje A11 es usado para crear, mantener y suprimir conexiones A10. Mientras tanto, el PCF entrega parámetros de tarificación mediante un mensaje A11. La pila de protocolos de la interfaz A11 se muestra en la figura 4.6.

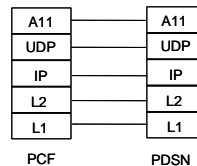


Figura 4.6 Pila de protocolos A11

### - Interfaz A10

La interfaz A10 es usada para transmitir datos del suscriptor entre PCF y PDSN. Como se muestra en la Figura 4.7. La capa mas alta es la capa GRE, que encapsula la capa de datos (PPP) en marcos (frames) de GRE para la transmisión.

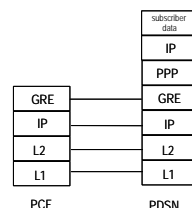


Figura 4.7 Pila de protocolos A10

### - Interfaz Pi

Las interfaces Pi incluyen las interfaces entre el PDSN y todos los nodos de comunicaciones de datos, como la interfaz entre PDSN y AAA, la interfaz entre PDSN y el HA, y la interfaz entre PDSN y otros ruteadores.

El 3GPP2 casi no da ninguna nueva definición para interfaz Pi. Un interfaz Pi es realizada por el empleo directo de los protocolos RFC. Esto ha simplificado enormemente la arquitectura de red.

### - Interfaz entre PDSN y AAA

La pila de protocolos entre el PDSN Y el AAA son definidos en la figura 4.8. Estos son definidos en el RFC 2138 y el RFC 2139. En la red de CDMA2000, esta interfaz es usada para transmitir los datos de autenticación y datos de la tarificación.

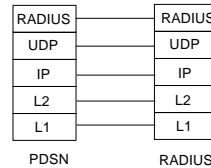


Figura 4.8 Pila de protocolos entre PDSN y AAA

### - Interfaz entre PDSN y PDN

Las interfaces entre PDSN y PDN son interfaces de protocolo IP, como se muestra en la figura 4.9.

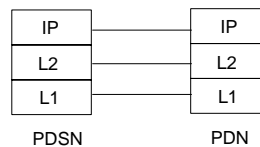


Figura 4.9 Interfaz entre PDSN y PDN

## 4.5 Servicios y funciones

El PDSN es una entidad de red indispensable en la red de CDMA2000. Su función principal es reenviar paquetes entre una red de CDMA2000 y una red de paquetes, es decir, conectar una EM a un PDN externo por PPP para proveer del servicio de datos proveyendo a los paquetes las rutas del siguiente salto

### 4.5.1 Ruteo

Desde punto de vista del PDN, como un dispositivo de entrada entre la red CDMA2000 y el PDN, el PDSN es equivalente a un router, que puede dirigir a todos los usuarios IP en la red de CDMA2000.

El PDSN9660 soporta todos los protocolos de ruteo más populares, incluyendo:

- Static routing
- RIP
- OSPFv2
- IS-IS
- BGP-4
- Routing policies
- Active/Standby routing



## 4.5.2 Interfaz R-P Estardar

Cuando una EM inicia una llamada de datos, una sesión A10 (es decir un canal de datos) es establecido entre el PCF y EL PDSN por el interfaz de Paquete de Radio (R-P). Basado en el canal de datos de este usuario, una conexión PPP es establecida entre el MS y el PDSN. Los paquetes de datos entonces son transmitidos por la conexión PPP.

---

**Nota:**

La interfaz R-P es una interfaz entre la red de acceso de radio y la red central de paquetes. Para ser específico, esto es un interfaz entre el PCF Y EL PDSN. Hay dos tipos de interfaces R-P: A10 y A11.

- A10: Esta es usada para transmitir los datos de los usuarios. La capa superior del protocolo A10 es la capa de GRE, que encapsula la parte superior de los datos PPP en marcos de GRE para la transmisión.
  - A11: Esta es usada transmitir la señalización entre el PDSN Y el PCF para establecer o liberar conexiones A10. Mientras tanto, el PCF también puede entregar parámetros de la tarificación mediante mensajes A11.
- 

El PDSN9660 soporta la interfaz R-P definida el protocolo A.S0001-A protocol y provee las siguientes funciones:

- Establecimiento o supresión de conexiones A10: El PDSN9660 soporta conexiones A10 iniciadas por el PCF. Tanto el PCF como el PDSN9660 pueden suprimir activamente conexiones A10.
- Actualizar conexiones A10 periódicamente: El PCF envía mensajes de registro A11 de vez en cuando para pedir la actualización de las conexiones A10; el PDSN9660 corresponde dichas actualizaciones de igual forma a través de mensajes.
- Establecimiento y mantenimiento del túnel GRE: Establece el túnel GRE entre el PCF Y EL PDSN9660 y mantiene el túnel.
- Negociación PPP: Basado en la RFC1661, EL PDSN9660 establece, mantiene o termina sesiones PPP de las Estaciones Móviles (EMs).
- Soporta el cambio entre PCFs: Cuando una EM se mueve y cambia de una BSC a otra, el PDSN9660 permite la conmutación entre PCFs y mantiene las sesiones PPP en la EM .



### 4.5.3 IP Simple e IP Móvil

El PDSN9660 puede hacer que una EM pueda acceder al PDN externo. Esto puede ser posible mediante dos accesos: el IP simple y el IP móvil

#### *IP SIMPLE*

Por la modalidad de acceso simple IP, cuando una EM inicia un servicio de paquetes, el PDSN asigna una dirección IP a la EM durante la conexión PPP que está siendo establecida. Cuando el servicio de paquetes es terminado, la dirección IP es liberada.

Es fácil habilitar la modalidad de acceso IP simple. La dirección IP de una EM es asignada sólo cuando es necesario. Por consiguiente, la demanda de la cantidad de direcciones IP es pequeña. Sin embargo, el modo IP simple sólo apoya los servicios de paquete que son iniciados por una EM. Si esto cambia de un PDSN al otro, la EM tiene que interrumpir el servicio de paquete actualmente en curso y establecer una conexión PPP con el nuevo PDSN.

Bajo el modo de IP simple, el CN- PS tiene dos principales entidades de red, el PDSN y el servidor AAA. El flujo de servicio básico que el PDSN ejecuta en el modo IP simple es el siguiente:

- 1) Un suscriptor móvil manda una petición de servicio de paquetes, estableciendo un enlace PPP a través de la RAN, la EM y el PDSN9660.
- 2) El PDSN9660 se comunica con el servidor AAA para la autenticación del suscriptor móvil.
- 3) Habiendo pasado la autenticación, la EM obtiene una dirección asignada por el PDSN9660 (o del servidor AAA a petición del PDSN9660).
- 4) El PDSN9660 entonces conecta la EM a un PDN externo en el modo IP, colectando la información de tarificación y enviándola al servidor AAA.
- 5) Si el suscriptor por iniciativa propia se desconecta o no hace ninguna operación durante mucho tiempo, el PDSN9660 inicia el proceso para liberar la dirección de IP actualmente sostenida por la EM.

#### *IP MÓVIL*

La IP simple sólo soporta los servicios de paquetes que son inicialmente mandados por una EM. Sin embargo, cuando las EM se mueve de una red a otra (o cambia de un PDSN al otro), el servicio de paquetes existente será interrumpido y la





dirección de IP debe ser asignada de nuevo o renegociada. Para solucionar el problema cada vez más frecuente de la movilidad de una EM, se diseñó la IP Móvil (o MIP).

La tecnología móvil IP es una solución para proporcionar la movilidad sobre la red de IP. Esta solución permite a una EM mantener su comunicación disponible sin interrupción, incluso si la EM cambia de una red a otra ya que hace permanente su dirección IP (dirección local) al unirse con cualquier otra red. Es decir cuando la EM cambia de un PDSN a otro, la dirección IP original y la sesión son mantenidos y el servicio de paquete en curso permanece ininterrumpido.

Bajo la arquitectura IPM, aparte del PDSN y el servidor AAA, el HA es también una de las entidades conectadas a la red. Al mismo tiempo, el PDSN también es integrado con la funcionalidad de FA.

EL flujo del servicio en IPM del PDSN es como sigue:

- 1) Un usuario móvil (MS) manda una petición de servicio de paquete; estableciendo un enlace PPP con el PDSN9660/FA a través de la RAN.
- 2) El PDSN9660/FA envía mensajes de anuncio, declarando sus servicios de FA. Tal mensaje lleva cierta dirección IP de PDSN9660/FA. Esta dirección sirve como el agente externo que cuida la dirección de la EM
- 3) La EM envía la petición de registro al HA por el PDSN9660/FA, advirtiendo el cuidado de la dirección (es decir, la información de la ubicación).
- 4) Mediante la autenticación del mensaje entre el PDSN9660/FA y el servidor AAA, el PDSN9660/FA verifica si la EM es legal o asigna un HA dinámico para ello. Cuando la EM ha pasado la autenticación, el PDSN9660/FA reenviara el mensaje de petición de registro de la EM al HA.
- 5) El HA anuncia la accesibilidad del prefijo de red de la dirección local de la EM para atraer los paquetes destinados a la EM y direccionar a la red local. El HA entrega estos paquetes al PDSN9660/FA vía túnel. Los paquetes originales serán individualizados del túnel en el PDSN9660/FA y reenviados a la EM.
- 6) En la dirección inversa, los paquetes de datos que son enviados de la EM siguen sólo el flujo que expide IP simple; en vez del HA, los paquetes van directamente al nodo destino en el PDN a través del PDSN9660/FA. Sin embargo, si el túnel inverso entre el PDSN9660/FA y el HA ha sido aplicado, los paquetes también pueden alcanzar el HA, llegando ahí son reenviados vía HA.



#### 4.5.4 Agente Extranjero ó Foráneo (FA)

Bajo la arquitectura IPM, el PDSN no sólo sirve como un dispositivo de entrada entre el CDMA2000 y el PDN, también integra la funcionalidad de FA. Esta funcionalidad puede proveer a una EM de un una dirección de cuidado agente externo, esta puede ser responsable de rutear una EM certificada y reenviar los paquetes del HA a través del túnel a la EM.

Las funciones de FA que son soportadas por el PDSN9660 son:

- Enviar anuncios de agente: Enviando los mensajes de anuncio de agente, el FA ayuda a la EM a reconocer si esta fuera de su red local y provee a la EM de la dirección de cuidado del agente externo y de otra información.
- Manejo de mensajes de registro: El FA juzga si el mensaje de registro tiene el contenido legal en los campos de mensaje de registro de una MS. Si es necesario, el FA también puede enviar el mensaje de registro al servidor AAA para la autenticación y expedición del mensaje de registro legal al HA para el negociación.
- Extensión de autenticación: El registro es un proceso vulnerable a ser atacado. Esto exige una autenticación obligatoria a los mensajes de registro entre una MS y el HA. EL PDSN9660/FA soporta la extensión de autenticación de mensajes de registro, incluyendo la autenticación entre una EM y el FA y entre el FA y el HA.
- Soporta tanto la tunelización de envío como la de respuesta: El PDSN9660/FA lleva el tráfico IP entre una EM y el HA vía un túnel. En el túnel de envío (un túnel con el HA es el punto de principio y el FA como el punto final), el FA desencapsula los paquetes IP del HA y luego los envía a la EM. En el túnel de respuesta (un túnel con la FA que es el punto de principio y el HA como el punto de final), el FA encapsula los paquetes de una MS y los envía a la HA vía el túnel. El PDSN9660/FA apoya tres tipos de encapsulación de túnel: encapsulación IP en IP, encapsulación mínima y encapsulación GRE.
- Entrega de Paquete: El FA obtiene los paquetes que son expedidos del HA por el túnel de envío y los entrega a la EM. También puede reenviar los paquetes de una EM a través del procedimiento de IP Simple o vía túnel inverso.

#### 4.5.5 Tarificación o Contabilidad (Accounting)

El PDSN puede coleccionar información de tarificación basándose en la duración del servicio o en el tráfico de datos. Cuando una EM ha pasado la autenticación e inicia el servicio de datos, El PDSN9660 recibirá la información de la tarificación desde el PCF y aquella que es coleccionada por el mismo. Luego convierte esta

información en mensajes llamados Usage Data Record (UDR por sus siglas en ingles) para luego enviarlos al servidor de tarificación vía protocolo de RADIUS. El servidor de tarificación entonces guarda esta información y genera registros de llamada detallados.

Para asegurar la fiabilidad de la tarificación, el PDSN9660 puede guardar y reenviar los mensajes de tarificación. Cuando el PDSN no puede conseguir respuesta del servidor de tarificación, envía de nuevo los mensajes correspondientes para prevenir la pérdida de información. Si se reenvía muchas veces pero el servidor sigue sin responder, el PDSN9660 guarda los registros en su disco duro. Cuando la comunicación al servidor de tarificación se restablece, el PDSN9660 le reenvía los registros que tenga guardados.

#### 4.5.6 PPS

El Servicio de Pre-Pago (o pago por adelantado), PPS por sus siglas en ingles, es una modalidad para que un suscriptor pueda disfrutar del servicio de datos pagando por adelantado una suma del dinero, ya sea que se convierta en tiempo aire o trafico de datos. Bajo PPS, el uso de los recursos (la duración de servicio o el volumen de datos) que es comprado por el suscriptor será descontado de su cuenta en tiempo real.

El sistema de prepago del proveedor en cuestión incluye las entidades siguientes: el PDSN9660, servidor AAA, PPS y SCP.

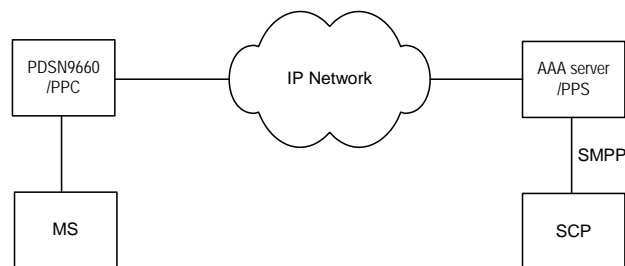


Figura 4.10 Sistema de servicio de prepago del PDSN9660

Como se muestra en la Figura 4.10, la EM es un suscriptor de servicio de pre-pago y el PDSN9660 es un cliente de servicio de pre-pago (PPC). El PDSN9660/PPC interactúa con el servidor PPS a través del AAA. El PDSN9660/PPC proporciona las funciones siguientes:

- Solicitud de cuotas para un suscriptor y la supervisión del uso de dichas cuotas.
- Cuando la cuota de una cuenta se termina, el PDSN envía mensajes al AAA/PPS para terminar la sesión y liberar los recursos involucrados.
- Cambia entre una tarifa y otra.



El sistema PDSN9660 PPS tiene las siguientes características:

- Supervisa que la tarificación este de acuerdo a la duración de la sesión del suscriptor activo
- Supervisa que la tarificación este de acuerdo al volumen de trafico consumido.
- Cambia entre el cargo por tiempo y el cargo por datos transmitidos.
- Distribuye el dinero dividiéndolo en pequeñas partes para el control del suscriptor. Así, muchos usuarios pueden compartir la misma cuenta al mismo tiempo para el servicio de paquetes.

#### 4.5.7 VPN Móvil

La Red Privada Virtual Móvil (MVPN por sus siglas en ingles) es una red de datos móvil en el que los servicios de VPN son dados de alta en base a la red de conmutación de paquetes pública, La MVPN permite que usuarios móviles puedan acceder a la red de alguna empresa con seguridad. Esto puede salvar grandes sumas de dinero usadas en líneas privadas que son muy caras. Además tiene la característica de que es sumamente seguro, confiable y manejable.

Basándose en una red CDMA2000, se puede hacer que una EM tenga acceso a la red privada de una empresa de manera segura y confiable, configurando un túnel privado entre el PDSN y los Gateways de VPN de la empresa en cuestión, solicitando la autenticación del usuario remoto y a través de tecnologías de encriptación de datos en el túnel.

El PDSN9660 soporta las tecnologías de tunelización tales como MPLS, L2TP y GRE. El operador puede proporcionar a los clientes flexibilidad con una solución segura y conveniente estableciendo una VPN.

#### VPN MPLS L3

La MPLS L3 VPN puede proporcionar la tecnología VPN usando MPLS LSP para reenviar los paquetes de datos en de la red central IP siempre y cuando MPLS LSP sea sumamente confiable. MPLS L3 VPN distribuye rutas VPN a través de BGP sobre las redes centrales IP para separar el tráfico entre distintos miembros VPN. EL PDSN9660 soporta MPLS L3 VPN y se basa en la definición de la IETF RFC 2547.

#### VPN L2TP

El túnel L2TP es una especie de tunelización en capa 2. Usa redes de IP para establecer un túnel L2TP y encapsula los datos en PPP. El PDSN9660 tiene la función de Concentrador de Acceso de L2TP (LAC) y soporta la construcción de una VPN a través del túnel L2TP para el transporte paquetes PPP destinados a una EM. El túnel L2TP se basa en la RFC 2661.

## VPN GRE

EL túnel GRE túnel es una especie de túnel de capa 3, que permite la encapsulación de cualquier protocolo de la capa de red sobre otro protocolo de capa de red. El PDSN9660 soporta la tunelización GRE. El Protocolo de red IP puede ser utilizado por GRE para transmitir protocolos de capas superiores a fin de proporcionar la funcionalidad de una VPN. El túnel GRE se ajusta a las definiciones del RFC 1702 y RFC 1701.

La Figura 4.11 muestra un ejemplo de la interconexión de las redes mediante el establecimiento de una VPN entre el PDSN9660 y el PDN con GRE.

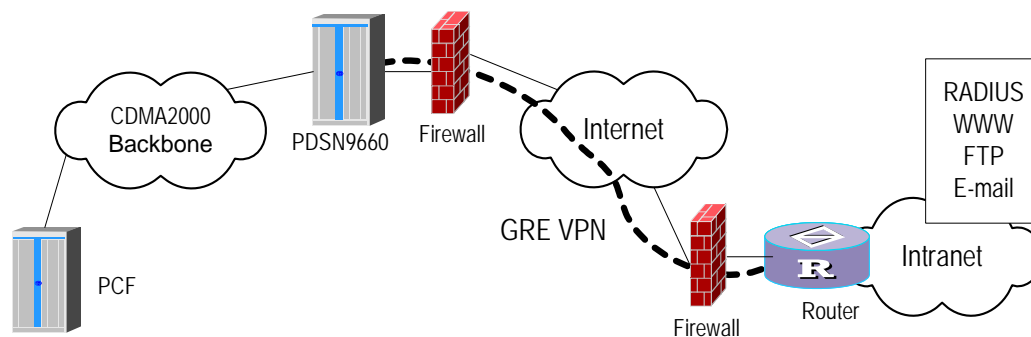


Figura 4.11 El PDSN crea una VPN con GRE

## 4.5.8 Seguridad

En el diseño del PDSN9660 se consideraron la implementación de varias políticas de seguridad

El PDSN9660 soporta los siguientes protocolos de autenticación y seguridad:

- Cuando en la conexión IP Simple, el PDSN9660 lleva a cabo la autenticación y la autorización de una EM interactuando con el servidor AAA. El PDSN9660 admite dos modos de autenticación, PAP y CHAP. La autenticación se lleva a cabo cuando una EM lleva a cabo negociaciones PPP con el PDSN9660.
- Cuando es una conexión IP Móvil, el PDSN9660 necesita llevar a cabo la autenticación para el registro entre la EM y el HA. El PDSN9660/FA soporta la extensión de autenticación del mensaje de registro, incluyendo la autenticación EM - FA y FA - HA.
- El PDSN9660 provee mas de un método de autenticación, tales como el "plain text authentication", MD5 y HMAC-MD5, para protocolos importantes de ruteo como por ejemplo, RIP v2, OSPF, IS-IS y BGP.



### - IPSec

La familia de protocolos de Seguridad en IP (IPSec por sus siglas en ingles) son una serie de protocolos definidos por la IETF. Proporciona alta calidad, interoperables y basados en la criptografía de seguridad para los paquetes de datos IP. Los dos lados de la comunicación realizan el cifrado y la autenticación del origen de datos en la capa IP para garantizar la confidencialidad, la integridad de los datos, y la no repetición de los paquetes cuando se transmiten a través de redes.

El PDSN9660 soporta las siguientes funciones IPSec en las interfaces R-P, Pi , y en todas aquellas interfaces físicas ya sean de operación o de mantenimiento:

- Implementar los algoritmos de autenticación MD5 y SHA-1
- Implementa los algoritmos de encriptación DES, 3DES y AES.
- Soporta dos modos de IPSec: El modo de transmisión o el modo de túnel
- Implementa los protocolos AH y ESP y soporta la vinculación entre el AH y el ESP
- Asocia la seguridad configurada manualmente o la seguridad negociada automáticamente a través de IKE
- Realiza la VPN tipo IPSec vinculando una VRF a la interfaz donde el IPSec se sitúa

Las características antes citadas son ejecutadas por medio de una tarjeta de cifrado de hardware, a fin de garantizar un alto rendimiento.

### - ACL y Filtrado de Paquetes

El PDSN9660 proporciona filtrado de paquetes y mecanismo de ACL, filtrando cada paquete de acuerdo a las condiciones definidas (por ejemplo, comparando si la dirección de la fuente de un paquete, o la dirección de destino del mismo u otros elementos que sean acorde a las normas). Esto puede prevenir eficazmente invasión ilegal o mal intencionados ataques.

### - Reorientación Pi

En general, el PDSN lleva a cabo la búsqueda de rutas a la capa interna de los datagramas IP que se obtienen por desencapsulación de los paquetes de una EM. Si las direcciones en los datagramas están destinadas a otras EM de la mismo PDSN, podría provocar un problema de seguridad: los ataques de datagrama entre los usuarios móviles en el mismo PDSN no pueden ser prohibidos.

La función “reorientación de PI” (o PI redirect en inglés) del PDSN9660 puede resolver el problema anterior. Se solicita al PDSN9660 reorientar los datagramas a Pi en los paquetes de transmisión de los usuarios, incluso si los datagramas están destinados a otros usuarios móviles bajo su misma administración. Después de haber sido filtrados por el firewall que conecta la interfaz Pi, los datagramas son devueltos al PDSN9660 y este los encapsula y retransmite al móvil destino.





#### 4.5.9 Calidad de Servicio (QoS)

CDMA2000 puede proporcionar a los abonados calidad del servicio con distintas prioridades. Al contratar un servicio de datos, el suscriptor elige la calidad del servicio que necesita y esta se guarda en el servidor de autenticación. El PDSN9660 soporta el establecimiento de etiquetas para el QoS. Es decir, el PDSN9660 primero obtiene los parámetros de los abonados del servicio de paquetes QoS del servidor de autenticación. Luego, mapea los parámetros QoS negociados en los servicios diferenciados por prioridad de la red IP y pone esta información en el encabezado del campo ToS o DSCP del datagrama del suscriptor y, por último, envía los datagramas a la PDN externa. Basándose en esto, la red externa implementa IP QoS fin de garantizar la calidad de servicio de los abonados del servicio de paquetes.

Además, como una mejora de router, el PDSN9660 admite las siguientes características QoS, tales como las políticas de tráfico, la modulación del tráfico, la cola de programación y control de la congestión. Ellos son ejecutados por hardware, lo que se traduce en un alto rendimiento.

#### 4.5.10 Múltiples tecnologías de compresión

Los recursos de ancho de banda de una red inalámbrica son limitados. El PDSN9660 admite el método de compresión de encabezado TCP / IP, el método STAC LZS y el método MPPC. Incluso cuando el ancho de banda es el mismo, la compresión puede proporcionar una mayor velocidad de transferencia de datos.

#### 4.5.11 Otros

El PDSN9660 también soporta los siguientes servicios y funciones:

- Muchos modos de asignación de direcciones IP

En el modo de acceso de IP Simple, el PDSN9660 asigna las direcciones IP a las Estaciones Móviles ya sea de su alberca de direcciones IP local o pidiéndola al AAA. La dirección asignada a una EM puede ser una dirección IP pública o privada. Si se trata de una IP privada, es necesario que esta sea transformada por el servidor NAT (firewall en nuestro caso). En el modo de acceso de IP Móvil, la dirección local pública o privada de la EM es asignada por el HA. En caso de tener un túnel con una IP privada, este debe establecerse entre el PDSN9660 y el HA.

- Protocolo de Tiempo de Red (NTP, Network Time Protocol)

Como cliente NTP, el PDSN9660 puede habilitar la sincronización de tiempo de red con un servidor NTP.

- SNMPV1/V2/V3.





## CAPITULO 5

# Implantación y puesta en funcionamiento del PDSN en un Proyecto real de CDMA2000 a 450 Mhz (CDMA450)

Toda la introducción previa abordada en los capítulos 1, 2, 3 y 4 (siendo los últimos dos algo mas relacionado directamente al tema central) es para tener un mejor base y así entender este último capítulo que explica de manera mas específica el proyecto implementado en la red del cliente, tema central de este trabajo. Los siguientes puntos son parte de un documento elaborado con el cliente de titulo, "Premisas de ingeniería". En el se explica de manera concisa, detallada y brevemente la implementación del equipo PDSN en la red CDMA450 del cliente en cuestión.

De igual forma en este capítulo se desglosarán los criterios de Ingeniería del proyecto que permitieron definir la ínter conectividad del Módulo de Servicios de Datos en Paquetes [PDSN 9660], del proveedor en cuestión. Así mismo se mencionan las capacidades y los requerimientos en fuerza, clima y espacio inherentes para la óptima funcionalidad e interoperabilidad de la red del cliente.

### 5.1 Antecedentes del proyecto

Realizar la sustitución del Sistema de Radio RAM (Radio Acceso Múltiple) Analógico por un Sistema en base a la Tecnología CDMA (**A**cceso **M**últiple por **D**ivisión de **C**ódigo), en la banda de los 450 Mhz. Con lo cual se pretende ampliar la cobertura del servicio; pasando de solo tenerlo en Agencias Telefónicas a ofrecerlo a nivel domiciliario, con posibilidad de proporcionar servicio de Acceso a Internet en las poblaciones actualmente RAM ubicado en comunidades rurales.



## 5.2 Premisas en la Cobertura

1. Sustituir al Sistema (obsoleto) de Radio Analógico RAM el cual es empleado en proporcionar servicios de voz a Agencias Telefónicas ubicadas principalmente en el ámbito rural.
2. La sustitución engloba 166 células RAM.
3. La cobertura será a nivel nacional, con la participación de dos proveedores de la tecnología CDMA. El proveedor cuestión cubrirá lo relacionado a las DD. siguientes:
  - Metro Norte
  - Metro Sur
  - Golfo
  - Sureste

NOTA: Se contempla que solo el 10% de los usuarios del Sistema CDMA demanden el servicio de Internet.

## 5.3 Premisas de Ingeniería.

1. El área de Cobertura del proveedor implica a 18 elementos de red RACs, 163 elementos de red BTSS, 1 Gestor M2000 y 1 PDSN.
2. Los RACs deberán ser interconectados al PDSN mediante interfaces FE mediante Anillos de Fibra Óptica.
3. Los RACs han sido ubicados en centrales con acceso a la red de transporte de Larga Distancia.
4. Se deberá cuidar que la conexión entre el RAC y la terminal de transporte de Larga Distancia no exceda los 100 m.
5. El PDSN será ubicado en la central del cliente preferentemente en la Sala de Tx de Larga Distancia, con el objeto de no rebasar los 100 m de una conexión en LAN, que iría entre la terminal de transporte y el propio PDSN.
6. El PDSN tendrá conexión con el Gestor M2000 a través de la RCDT mediante interfaces Et 10/100 Mbps.
7. El PDSN se interconectará al AAA de UniNet mediante una interfaz GE.

## 5.4 Coberturas.

El PDSN 9660 será ubicado en la Central del cliente (Metro Norte), e interconectará a 18 RACS del sistema CDMA450 del proveedor y 163 BTS, los cuales en su conjunto generarán un tráfico de 3.35 Mbps hacia Internet, el cual será cursado por la red de transporte de Larga Distancia.



A continuación se relacionan los RACs, su ubicación y el Ancho de Banda que se prevé será generado por elemento de red (RAC).

| RAC No.      | Ubicación - Nombre              | Usuarios Totales (Voz) | Cantidad de BTS | Ancho de Banda hacia el PDSN (Mbps) |
|--------------|---------------------------------|------------------------|-----------------|-------------------------------------|
| 1            | 1 PACHUCA-REVOLUCION            | 8,448                  | 13              | 0.28                                |
| 2            | 2 POZA RICA-POZA RICA           | 7,793                  | 9               | 0.26                                |
| 3            | 3 PUEBLA-FUERTES                | 7,866                  | 17              | 0.26                                |
| 4            | 4 COATZACOALCOS-PETROLERA       | 2,249                  | 3               | 0.08                                |
| 5            | 5 CORDOBA-CORDOBA               | 7,050                  | 11              | 0.24                                |
| 6            | 6 VERACRUZ-MOCAMBO              | 10,189                 | 10              | 0.34                                |
| 7            | 7 CUAUTITLAN-CUAUTITLAN         | 1,173                  | 3               | 0.04                                |
| 8            | 8 TOLUCA-NEVADO                 | 13,426                 | 17              | 0.45                                |
| 9            | 9 ACAPULCO-HIDALGO              | 1,528                  | 4               | 0.05                                |
| 10           | 10 CHILPANCINGO-CHILPANCINGO    | 3,487                  | 11              | 0.12                                |
| 11           | 11 CUERNAVACA-BORDA             | 593                    | 2               | 0.02                                |
| 12           | 12 TUXTLA GUTIERREZ-TUXTLA GTZ. | 8,523                  | 16              | 0.29                                |
| 13           | 13 TAPACHULA-TAKANA             | 3,234                  | 3               | 0.11                                |
| 14           | 14 OAXACA-BELISARIO             | 6,796                  | 18              | 0.23                                |
| 15           | 15 JUCHITAN-JUCHITAN            | 2,829                  | 5               | 0.10                                |
| 16           | 16 CANCUN-CASCADA               | 770                    | 3               | 0.03                                |
| 17           | 17 VILLAHERMOSA-PASEO           | 8,530                  | 7               | 0.29                                |
| 18           | 18 MERIDA-PLAZA                 | 4,611                  | 11              | 0.16                                |
| <b>TOTAL</b> |                                 | <b>99,095</b>          | <b>163</b>      | <b>3.35</b>                         |

Tabla 5.1 Relación de RACs y Ancho de Banda calculado

## 5.5 Plataforma del Sistema CDMA450.

El propósito es ofrecer conexión vía inalámbrica mediante un subsistema Wireless Local Loop (WLL), a poblaciones rurales, proporcionando terminales inalámbricas de tecnología CDMA enlazadas por medio de Estaciones Remotas hacia un Radio Controlador directamente conectado con centrales de conmutación digital a través de interfaces V5.2 con la posibilidad de migrar hacia un esquema de Red de Siguiete Generación (NGN). Uno de los Nodos de Acceso es el RAC (RAC6610), el cual es un equipo que concentra el tráfico de las BTS (BTS 3606) y permite el acceso de los clientes vía inalámbrica. En la Red Rural la BTS se encuentra ubicada en la capa de acceso para proporcionar los servicios mencionados a los clientes. La solución se basa en tecnología CDMA en la banda de los 450MHz.

Los usuarios de esta tecnología tienen la posibilidad de acceder al servicio de Internet vía su terminal inalámbrica, este tráfico al igual que el de voz es concentrado por el RAC y es enviado al PDSN, el cual a su vez lo enviará al AAA de Uninet y de ahí a la red de Internet.

Diagrama General de la conectividad del Sistema CDMA450.

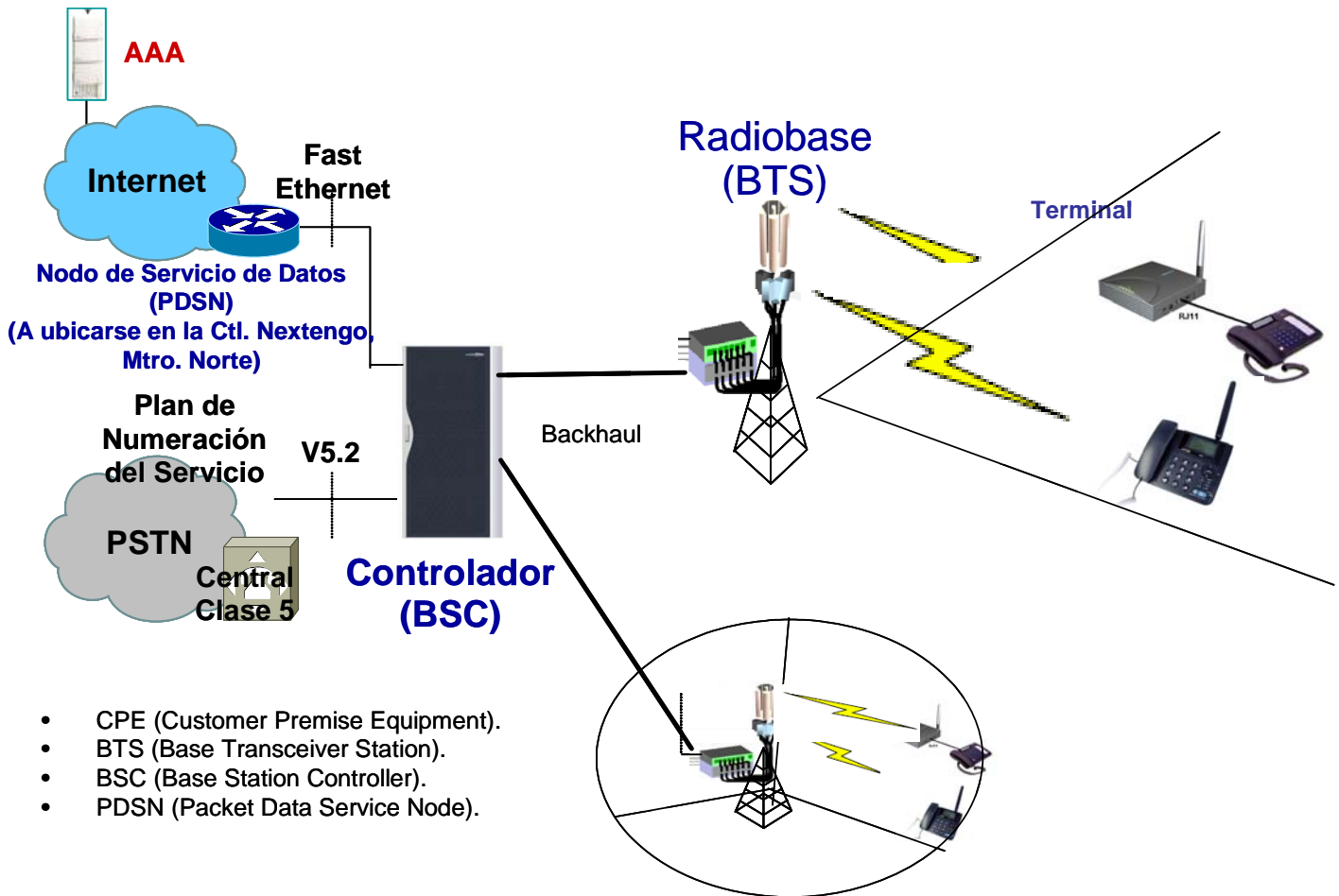


Figura 5.1 Arquitectura General del Sistema CDMA

## 5.6 Conectividad del PDSN en el proyecto CDMA450

El control del acceso a Datos, involucra la funcionalidad de los Sistemas PDSN y AAA, los cuales estarán físicamente ubicados en la Central del cliente y en las instalaciones de Uninet respectivamente.

Para que la solución CDMA pueda operar en la red de Uninet, debe cumplir con diversos requisitos que pueden ser agrupados de la forma siguiente:

- Conectividad
- Direccionamiento
- AAA



### Interfaces

El Módulo PDSN se conectará al Sistema CDMA (RAC) mediante interfaces FE sobre Fibra óptica a través de la red de Transporte de Larga Distancia.

El Módulo PDSN se conectará al AAA de Uninet mediante una interfaz GE sobre UTP, la cual será local, buscando que esta sea en la central del cliente, donde Uninet cuenta con un punto de acceso a su backbone

El Módulo PDSN se conectara al equipo de Gestión M2000 a través de la RCDT mediante interfaces Et de 10/100 Mbps.

El sistema PDSN deberá contar con Una dirección IP, para ser gestionado por el M2000 a través de la RCDT.

### Direccionamiento

Los Equipos que proporcionan la conectividad hacia la red de Uninet (PDSN y AAA), soportan la configuración de albercas (pools) locales de direcciones para la asignación al usuario final. Estas albercas manejan direcciones validas en Internet y direcciones privadas. De la misma forma, el direccionamiento utilizado para la configuración de dichos dispositivos, deben permitir tener un registro del direccionamiento utilizado por el usuario final en los servidores de Radius (AAA).

### AAA [Autenticación, Autorización y Accounting]

Los servicios de AAA (Autenticación, Autorización y Accounting), en la red de Uninet para la validación de usuarios finales es realizada con el protocolo RADIUS, utilizando los puertos estándares para estos servicios (1812 para autenticación y 1813 para Accounting), todos los equipos RAS (Remote Access Server), en nuestro caso el PDSN, cumplen con los RFC 2865 y 2866.

| Características Comunicaciones del elemento de red (PDSN)    |                   |                   |                  |   |
|--|-------------------|-------------------|------------------|---|
| Protocolo de capa 3  | IP [ X ]          | CLNS [ ]          | Otro [ ]         |   |
| Protocolo de capa 4  | UDP [ ]           | TCP [ X ]         | TP [ ]           | Otro [ ]                                      |
| Protocolos de capas superiores                               | SNMP [ ]          | FTP [ X ]         | Telnet[ X ]      | Otro [ ]                                      |
| Tipo de interfaz   | Eth [ X ]         | FasEth [ X ]      | RS-232[ ]        | Otro [ ]                                      |
| Si es RS-232 Pinout en diagrama anexo                        | Bits de datos [ ] | Paridad [ ]       | Bits de paro [ ] | Caracteres<br>Hex [ ]<br>ASCII [ ]<br>Bin [ ] |
|  |                   |                   |                  |   |
| Modo y Velocidad   | Half Duplex [ ]   | Full Duplex [ X ] | 10 Mbps[ ]       | 100 Mbps [ X ]                                |
| Conector fisico de Interfaz<br>(Especifique: macho ó hembra) | RJ-45 [ X ]       | Macho [ ]         | Hembra[ X ]      |   |
|  | DB-25 [ ]         | BNC [ ]           | Otro [ ]         |   |

Tabla 5.2 Comunicación del PDSN [Interfaces y Protocolos]

*Esquema de conectividad del módulo PDSN.*

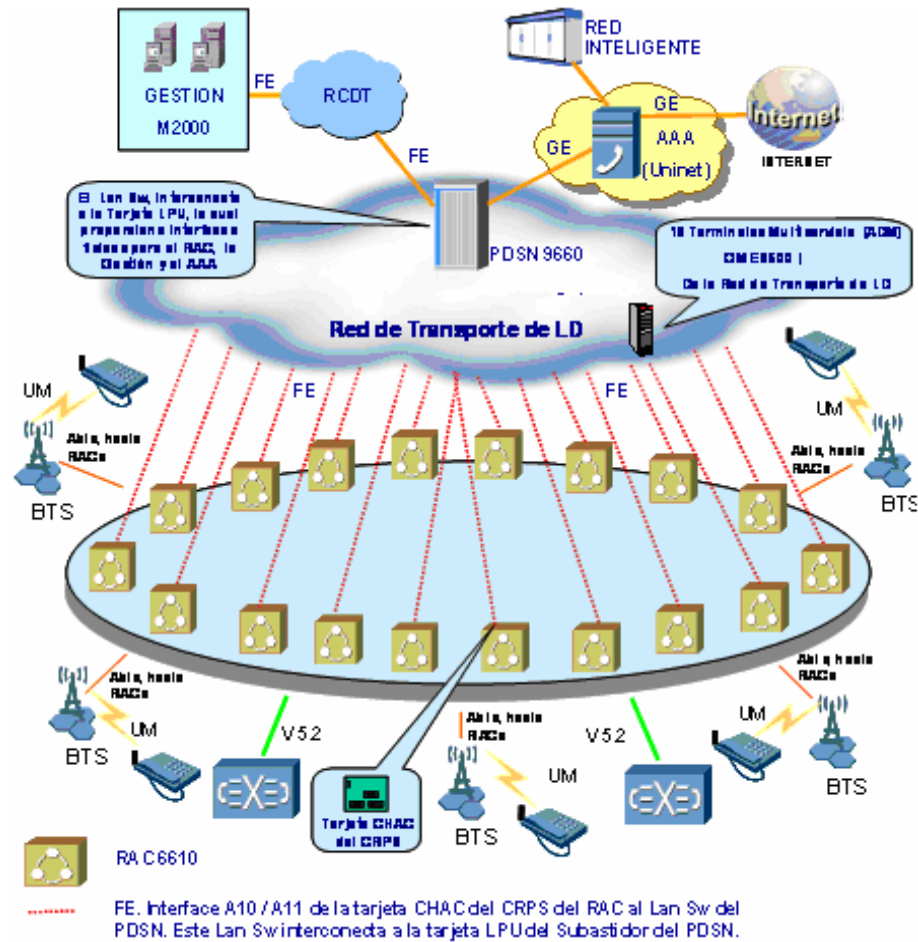


Figura 5.2 Conectividad del Módulo PDSN

## 5.7 Ubicación de los elementos de red

### RACs

En el Anexo 1 se incluye un archivo con la ubicación de los 18 RACs, los cuales tendrán que ser conectados mediante cable UTP categoría 5 hacia las terminales de la Red de Transporte de Larga Distancia.

### Terminales de la Red de Transporte de Larga Distancia.

En el Anexo 2 Se incluye un archivo con la ubicación de las Terminales de Transporte Multi Servicio FE (ADM) en la red de larga distancia, conectados a los



RACs y al PDSN mediante Fibra Óptica (UTP en los extremos). Estas terminales están constituidas por el equipo OME de otra proveedora de equipos de telecomunicaciones importante a nivel mundial

*PDSN 9660 V800r002 – Packet Data Serving Node - Nodo de Servicio de Datos.*

#### Especificaciones Técnicas

El PDSN9660 se encuentra montado en un gabinete del proveedor N68-22. Las dimensiones físicas del gabinete son las siguientes:

- Altura: 2200 mm
- Profundidad (espesor): 800 mm
- Ancho: 600 mm
- Peso: menos de 300 Kg. (gabinete simple)

#### Requerimiento.

- Los bastidores deberán contar con herrajes de sujeción de tipo normal y antisísmico.

#### Fuente de Alimentación

- Entrada de CC: –48 a –60 V CC

#### Consumo Total de Energía

- Menos de 1400 W (gabinete simple)

## 5.8 Instalación del PDSN en la Central del cliente

En cualquier instalación de equipos de telecomunicaciones en centrales del cliente sea el proveedor que sea, uno de los requerimientos básicos para llevar a cabo dicha instalación en la llamada orden de trabajo (OT). En ella se especifican los trabajos a realizar y en caso de que el equipo ya este dando servicio, el impacto que van a tener estos trabajos para el servicio (de hecho, en estos casos lo que se acostumbra es hacer estos trabajos durante la noche en las llamadas “ventanas de mantenimiento”). La siguientes imágenes muestran lo que es una OT real, en este caso la del PDSN en la central telefónica del cliente en cuestión que consistió en tres partes principalmente:

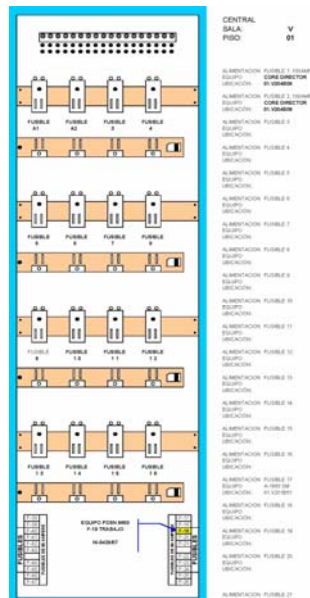




- Especificación de los trabajos a realizar (instalación del equipo y conectividad)

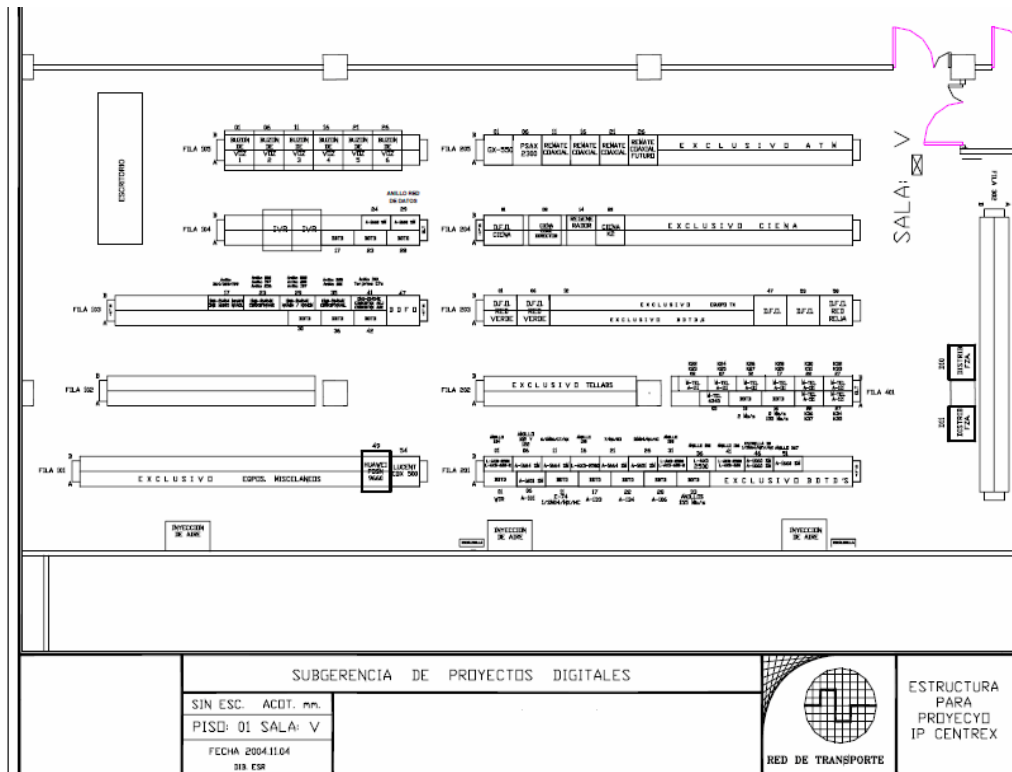
|   |  |
|---|--|
| <b>PROYECTOS</b><br><br>P. C. M.  | Departamento de Proyectos de Sistemas<br>Digitales<br>Wirdep<br><br><b>ORDEN DE TRABAJO</b>      |
| México D.F., a 24 de abril de 2007.<br>Encargado del Trabajo: _____<br>Encargado del Proyecto: _____<br>Proyectista: _____  |  |
| <b>CENTRAL:</b><br>Instalación de equipo PDSN 9660<br>Sirvase efectuar los siguientes trabajos:<br>1.-Instalación, conexión y ajuste de equipo PDSN 9660 _____, en la posición 01.V101B49, de acuerdo a lo indicado en anexo.<br>2.-La alimentación se tomará de los bastidores remotos de fuerza BASTIDOR 10, fusible 19 (Trabajo) y BASTIDOR 11, fusible 19 (Respaldo), de acuerdo a lo indicado en anexos.<br>3.-Aterrizaje del bastidor, con respecto a la barra de Tierra de la fila.<br>4.- Conexión a RCDT.CENTRAL.sw2, FE 0/15(ubicación: 2ºpiso, sala PMCT, fila-210, Serie CSG0838PIH1). IP:10.166.65.10,M:255.255.255.0,GM:10.166.65.254.<br>4.-Antes de iniciar los trabajos, favor de dar aviso al jefe de la central.<br>NOTA. EL EQUIPO PROVIENE DEL DESMONTAJE DE LA SALA L.D. SEGUNDO PISO.<br>Se mandará a construir un tramo de escalerilla aluminio 4" para fuerza (4 mts).<br>Se mandará a construir un tramo de escalerilla aluminio 4" para UTP (6 mts). |  |
| <b>GRUPO: NI-0428/07</b>  |  |
| <b>Materiales y mano de obra.</b>   |  |
| Clase de trabajo  | Cuenta   |
| <b>Instalación de Equipo PDSN 9660</b><br><br>TRABAJO EMPEZADO .... DE _____<br>TRABAJO TERMINADO ...DE _____<br>DE.....ENCARGADO   | Al terminar el trabajo Deberá ser inspeccionado por el encargado de Mantenimiento.<br>Autorizó : |

- Especificación de la alimentación del equipo





- Ubicación física y exacta (sala, fila, lado, bastidor) del equipo



Como se puede ver en las tres figuras de la Orden de Trabajo de especifica de manara detallada la instalación e interconexión del equipo PDSN de manera muy clara, este documento es elemental para la realización de cualquier trabajo dentro de una central del cliente.

## 5.9 Interconexión entre el PDSN y RAC's.

El PDSN es el equipo con el que se realizan las sesiones de datos de las terminales. El PDSN se comunica con el servidor AAA para validar y autenticar al usuario. Dependiendo de la sesión (si es prepago o pospago) se podrá comunicar con red inteligente para realizar el cobro.

Los RAC's utilizan puertos Fast ethernet para comunicarse con el PDSN. Debido a que la conexión entre estos dos equipos se realizará a través de la red SDH de Larga distancia, se encapsulará el tráfico ethernet saliente de los RAC's en SDH para transportarlo hacia el PDSN. Por cada RAC se utilizará un lada enlace con capacidad de VC12 (2Mbps) punto a punto. Al ser transportado el tráfico por anillos SDH, no se utilizan anillos RPR (Resilient Packet Ring).



Para identificar el tráfico de cada RAC, se asignó una VLAN para cada uno de estos equipos. El equipo PDSN podrá identificar cada VLAN (utilizando el protocolo IEEE 802.1q). Para cada división se ha asignado un rango de VLAN's. El número más significativo de la VLAN indica el proveedor de la tecnología CDMA. El número 2 corresponde al proveedor en cuestión.

El segundo número más significativo indica la división a la que le corresponde el RAC. En la siguiente tabla se muestra los números asignados a cada división.

| Número Proveedor | Número asignado | División    |
|------------------|-----------------|-------------|
| 2                | 0               | Golfo       |
| 2                | 1               | Metro Sur   |
| 2                | 2               | Metro Norte |
| 2                | 3               | Sureste     |

Tabla 5.3 Números asignados por división

Los dos números menos significativos indican la ubicación del RAC. Conforme se instalen más RAC's se asignará un número consecutivo al último RAC instalado. El primer RAC asignado a una Dirección Divisional deberá ser el número 01.

En la tabla 2 se muestra la VLAN asignada a cada una de las 18 RAC's del proveedor.

| Ubicación-Nombre Central     | División    | Usuarios     | AB hacia PDSN (Mbps) | Cantidad BTS | VLAN |
|------------------------------|-------------|--------------|----------------------|--------------|------|
| PACHUCA- REVOLUCION          | Golfo       | 8448         | 2                    | 13           | 2001 |
| POZA RICA- POZA RICA         | Golfo       | 7793         | 2                    | 9            | 2002 |
| PUEBLA- FUERTES              | Golfo       | 7866         | 2                    | 17           | 2003 |
| COATZACOALCOS- PETROLERA     | Golfo       | 2249         | 2                    | 3            | 2004 |
| CORDOBA- CORDOBA             | Golfo       | 7050         | 2                    | 11           | 2005 |
| VERACRUZ MOCAMBO             | Golfo       | 10189        | 2                    | 10           | 2006 |
| CUAUTITLAN- CUAUTITLAN       | Metro Norte | 1173         | 2                    | 3            | 2101 |
| TOLUCA- NEVADO               | Metro Norte | 13426        | 2                    | 17           | 2102 |
| ACAPULCO- HIDALGO            | Metro Sur   | 1528         | 2                    | 4            | 2201 |
| CHILPANCINGO- CHILPANCINGO   | Metro Sur   | 3487         | 2                    | 11           | 2202 |
| CUERNAVACA- BORDA            | Metro Sur   | 593          | 2                    | 2            | 2203 |
| TUXTLA GUTIERREZ- TXTLA GTZ. | Sureste     | 8523         | 2                    | 16           | 2301 |
| TAPACHULA- TAKANA            | Sureste     | 3234         | 2                    | 3            | 2302 |
| OAXACA- BELISARIO            | Sureste     | 6796         | 2                    | 18           | 2303 |
| JUCHITAN- JUCHITAN           | Sureste     | 2829         | 2                    | 5            | 2304 |
| CANCUN- CASCADA              | Sureste     | 770          | 2                    | 3            | 2305 |
| VILLAHERMOSA- PASEO          | Sureste     | 8530         | 2                    | 7            | 2306 |
| MERIDA- PLAZA                | Sureste     | 4611         | 2                    | 11           | 2307 |
| <b>TOTAL</b>                 |             | <b>99095</b> | <b>36</b>            | <b>163</b>   |      |

Tabla 5.4 Relación de VLAN



INSTITUTO POLITÉCNICO NACIONAL  
ESIME CULHUACAN



| AREA   | RAC ID | RAC IP        | RAC MASK      | PCF IP        | PCFGW IP      | PCF MASK      | PCFGW MASK      | VLAN ID |
|--|--------|---------------|---------------|---------------|---------------|---------------|-----------------|---------|
| CANCUN-CASCADA   | 1      | 192.168.0.1   | 255.255.255.0 | 192.168.0.6   | 192.168.0.5   | 255.255.255.0 | 255.255.255.248 | 2305    |
| MERIDA-PLAZA   | 2      | 192.168.0.8   |               | 192.168.0.14  | 192.168.0.13  |               |                 | 2307    |
| VILLAHERMOSA-PASEO   | 3      | 192.168.0.16  |               | 192.168.0.22  | 192.168.0.21  |               |                 | 2306    |
| TUXTLA GUTIERREZ-TUXTLA GTZ  | 4      | 192.168.0.24  |               | 192.168.0.30  | 192.168.0.29  |               |                 | 2301    |
| TAPACHULA-TAKANA   | 5      | 192.168.0.32  |               | 192.168.0.38  | 192.168.0.37  |               |                 | 2302    |
| JUCHITAN-JUCHITAN  | 6      | 192.168.0.40  |               | 192.168.0.46  | 192.168.0.45  |               |                 | 2304    |
| OAXACA-BELISARIO   | 7      | 192.168.0.48  |               | 192.168.0.54  | 192.168.0.53  |               |                 | 2303    |
| COATZACOALCOS-PETROLERA  | 8      | 192.168.0.56  |               | 192.168.0.62  | 192.168.0.61  |               |                 | 2004    |
| VERACRUZ-MOCAMBO   | 9      | 192.168.0.64  |               | 192.168.0.70  | 192.168.0.69  |               |                 | 2006    |
| CORDOBA-CORDOBA  | 10     | 192.168.0.72  |               | 192.168.0.78  | 192.168.0.77  |               |                 | 2005    |
| POZA RICA-POZA RICA  | 11     | 192.168.0.80  |               | 192.168.0.86  | 192.168.0.85  |               |                 | 2002    |
| PACHUCA-REVOLUCION   | 12     | 192.168.0.88  |               | 192.168.0.94  | 192.168.0.93  |               |                 | 2001    |
| PUEBLA-FUERTES   | 13     | 192.168.0.96  |               | 192.168.0.102 | 192.168.0.101 |               |                 | 2003    |
| TOLUCA-NEVADO  | 14     | 192.168.0.104 |               | 192.168.0.110 | 192.168.0.109 |               |                 | 2102    |
| CUAUTITLAN-CUAUTITLAN  | 15     | 192.168.0.112 |               | 192.168.0.118 | 192.168.0.117 |               |                 | 2101    |
| ACAPULCO-HIDALGO   | 16     | 192.168.0.120 |               | 192.168.0.126 | 192.168.0.125 |               |                 | 2201    |
| CHILPANCINGO-CHILPANCINGO  | 17     | 192.168.0.128 |               | 192.168.0.134 | 192.168.0.133 |               |                 | 2202    |
| CUERNAVACA-BORDA   | 18     | 192.168.0.136 |               | 192.168.0.142 | 192.168.0.141 |               |                 | 2203    |
| PDSN SRU NET INTERFACE IP:192.168.10.10/255.255.255.0  |        |               |               |               |               |               |                 |         |
| PDSN RP PHYSICAL INTERFACE(Ethernet1/0/15 and Ethernet2/0/15) IP:192.168.0.254/255.255.255.0 |        |               |               |               |               |               |                 |         |
| PDSN PI PHYSICAL INTERFACE(Ethernet1/0/14 and Ethernet2/0/14) IP:192.168.3.1/255.255.255.0   |        |               |               |               |               |               |                 |         |
| PDSN RPIF LOGIC INTERFACE:192.168.1.1/255.255.255.255  |        |               |               |               |               |               |                 |         |
| PDSN RPIF LOGIC INTERFACE:192.168.1.2/255.255.255.255  |        |               |               |               |               |               |                 |         |

Tabla 5.5 Relación de estas VLAN con su respectivo direccionamiento IP

## 5.10 Configuración equipo PDSN

### 5.10.1 Cableado e instalación general del Hardware

La figura 5.3 muestra un procedimiento de instalación regular de hardware de PDSN incluyendo el subastidor y el AAA, en la instalación práctica:

- La instalación de la caja de la alarma debe ser finalizada antes que de los cables de la red, porque los cables de poder de la caja de la alarma se distribuyen normalmente junto con los cables de la red.
- Como la secuencia de la conexión y distribución de cables de señal, alambres de tierra, cables eléctricos es insignificante, se puede hacer la conexión y la distribución de una manera que se sienta cómoda.
- Por conveniencia de la conexión de cable externo, la instalación de otras guarniciones del gabinete debe ser el último del proceso de instalación.

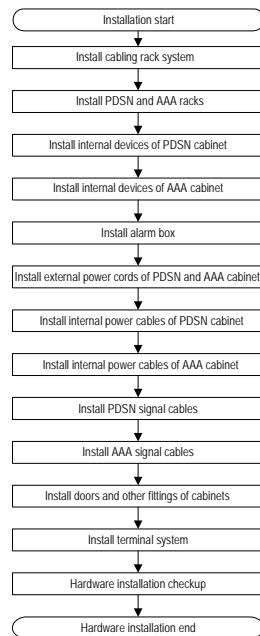


Figura 5.3  
Flujo de instalación de Hardware del PDSN9660

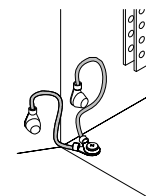
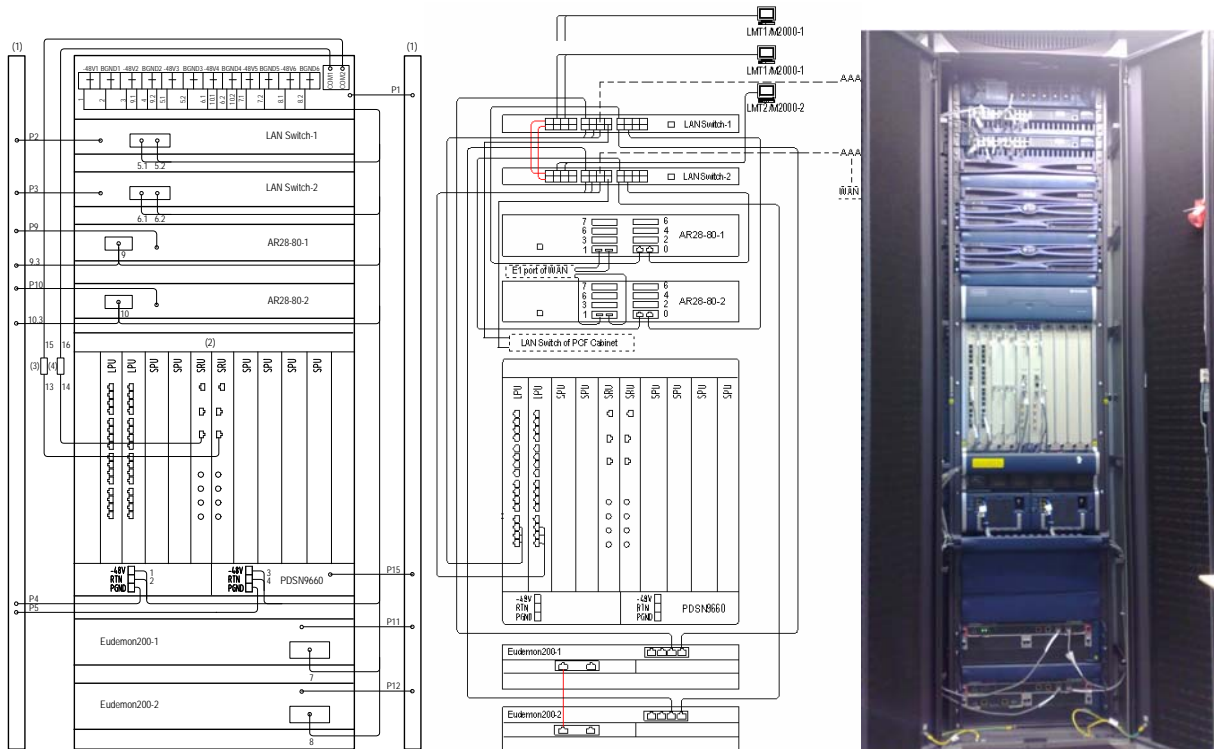


Figura 5.4  
Cables PGND en el cuerpo del gabinete

Sin embargo. Para fines de este trabajo solo indicaremos la instalación de Hardware de la parte del rack del PDSN solamente. En la figura 5.4 se muestra de manera más detallada como se debe de aterrizar el equipo cuando se este cableando toda la parte de poder. En la figura 5.5 se muestran de manera ya más resumida la conexión en alimentación y en cables de señalización con una pequeña imagen del equipo real ya finalizada esta instalación.



- (1) Barra de aterrizaje
- (2) Vista delantera del subrack de PDSN
- (3)/(4) Adaptador RS485-RS232

Conexion de los cables de señal

Cuadro verdadero de la instalación del rack de PDSN

Figura 5.5 Esquema eléctrico del gabinete PDSN9660. Cables al poner la tierra y la señalización

### 5.10.2 Configuración LanSWITCH

Una de las partes fundamentales que se tuvieron que configurar en el RAC, fue el LANSWITCH. EL LANSWITCH fue la interfaz que nos dio conectividad con el equipo OME (equipo que conecta a través de Fibra óptica a los RACs en los distintos sitios soportando también conexión de Fast Ethernet) ya que en el fue donde se configuraron las 18 VLAN anteriormente descritas en un solo puerto. Es decir, la conexión OME PDSN LANSWITCH era un solo cable UTP, al puerto a donde llegaba ese cable se le configuraron las 18 VLAN (Ethernet0/9). Tanto el equipo como la configuración se muestran a continuación:

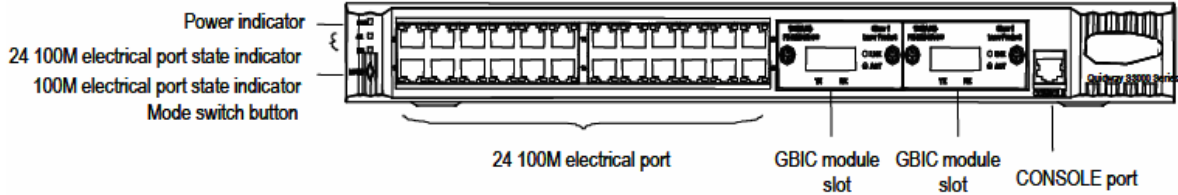


Figura 5.6 Estructura física del equipo



Figura 5.7 Imagen real del equipo

Configuración del equipo (hecha a través de un cable serial conectado a la consola del switch)

|  |   |
|--|---|
| <pre> &lt;Quidway&gt; &lt;Quidway&gt;dis vlan VLAN function is enabled. Now, the following VLAN exist(s): 1(default), 2-4, 2001-2006, 2101-2102, 2201- 2203, 2301-2307 &lt;Quidway&gt; &lt;Quidway&gt; &lt;Quidway&gt;dis vlan all VLAN ID: 1 VLAN Type: static ARP proxy disabled. Route Interface: not configured Description: VLAN 0001 Name: VLAN 0001 Tagged Ports: none Untagged Ports:     Ethernet0/1    Ethernet0/2 Ethernet0/3     Ethernet0/4    Ethernet0/5 Ethernet0/6  VLAN ID: 2 VLAN Type: static ARP proxy disabled. Route Interface: not configured Description: VLAN 0002 Name: VLAN 0002 Tagged Ports:     Ethernet0/1 Untagged Ports:     Ethernet0/7    Ethernet0/8         </pre> | <pre> VLAN ID: 2101 VLAN Type: static ARP proxy disabled. Route Interface: not configured Description: VLAN 2101 Name: VLAN 2101 Tagged Ports: Ethernet0/1    Ethernet0/9    Ethernet0/10 Untagged Ports: none  VLAN ID: 2102 VLAN Type: static ARP proxy disabled. Route Interface: not configured Description: VLAN 2102 Name: VLAN 2102 Tagged Ports:     Ethernet0/1    Ethernet0/9 Ethernet0/10 Untagged Ports: none  VLAN ID: 2201 VLAN Type: static ARP proxy disabled. Route Interface: not configured Description: VLAN 2201 Name: VLAN 2201 Tagged Ports:     Ethernet0/1    Ethernet0/9 Ethernet0/10 Untagged Ports: none         </pre> |
|--|---|





|  |  |
|--|--|
| <p>Ethernet0/11<br/>Ethernet0/12</p> <p>VLAN ID: 3<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 0003<br/>Name: VLAN 0003<br/>Tagged Ports:<br/>Ethernet0/1<br/>Untagged Ports:<br/>Ethernet0/13 Ethernet0/14<br/>Ethernet0/15<br/>Ethernet0/16 Ethernet0/17<br/>Ethernet0/18</p> <p>VLAN ID: 4<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 0004<br/>Name: VLAN 0004<br/>Tagged Ports:<br/>Ethernet0/1<br/>Untagged Ports:<br/>Ethernet0/19 Ethernet0/20<br/>Ethernet0/21<br/>Ethernet0/22 Ethernet0/23<br/>Ethernet0/24</p> <p>VLAN ID: 2001<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2001<br/>Name: VLAN 2001<br/>Tagged Ports:<br/>Ethernet0/1 Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> <p>VLAN ID: 2002<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2002<br/>Name: VLAN 2002<br/>Tagged Ports:<br/>Ethernet0/1 Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> | <p>VLAN ID: 2202<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2202<br/>Name: VLAN 2202<br/>Tagged Ports:<br/>Ethernet0/1 Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> <p>VLAN ID: 2203<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2203<br/>Name: VLAN 2203<br/>Tagged Ports:<br/>Ethernet0/1 Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> <p>VLAN ID: 2301<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2301<br/>Name: VLAN 2301<br/>Tagged Ports:<br/>Ethernet0/1 Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> <p>VLAN ID: 2302<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2302<br/>Name: VLAN 2302<br/>Tagged Ports:<br/>Ethernet0/1 Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> <p>VLAN ID: 2303<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2303<br/>Name: VLAN 2303<br/>Tagged Ports:<br/>Ethernet0/1 Ethernet0/9<br/>Ethernet0/10</p> |
|--|--|



|   |   |
|---|---|
| <p>VLAN ID: 2003<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2003<br/>Name: VLAN 2003<br/>Tagged Ports:<br/>    Ethernet0/1          Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> <p>VLAN ID: 2004<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2004<br/>Name: VLAN 2004<br/>Tagged Ports:<br/>    Ethernet0/1          Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> <p>VLAN ID: 2005<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2005<br/>Name: VLAN 2005<br/>Tagged Ports:<br/>    Ethernet0/1          Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> <p>VLAN ID: 2006<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2006<br/>Name: VLAN 2006<br/>Tagged Ports:<br/>    Ethernet0/1          Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> | <p>Untagged Ports: none</p> <p>VLAN ID: 2304<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2304<br/>Name: VLAN 2304<br/>Tagged Ports:<br/>    Ethernet0/1          Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> <p>VLAN ID: 2305<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2305<br/>Name: VLAN 2305<br/>Tagged Ports:<br/>    Ethernet0/1          Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> <p>VLAN ID: 2306<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2306<br/>Name: VLAN 2306<br/>Tagged Ports:<br/>    Ethernet0/1          Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> <p>VLAN ID: 2307<br/>VLAN Type: static<br/>ARP proxy disabled.<br/>Route Interface: not configured<br/>Description: VLAN 2307<br/>Name: VLAN 2307<br/>Tagged Ports:<br/>    Ethernet0/1          Ethernet0/9<br/>Ethernet0/10<br/>Untagged Ports: none</p> |
|---|---|

### 5.10.3 Configuración FIREWALL

Otra parte importante a configurar es el contrafuegos o mejor conocido como Firewall. Para este proyecto utilizamos la configuración que se detalla a continuación. En capítulos anteriores se explico cuales eran las funciones principales del Firewall. En nuestro caso el Firewall es el encargado de conectar el equipo a la red de Internet con una mayor seguridad, utilizando principalmente ACLs y rutas estáticas.

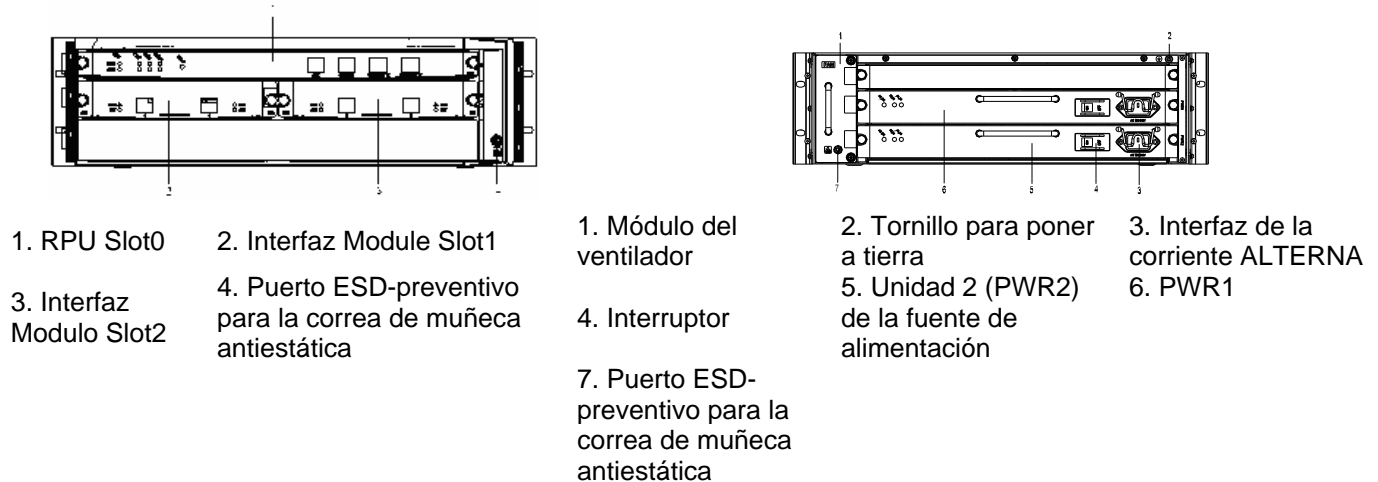


Figura 5.8 Panel delantero y trasero del Eudemon200



Figura 5.9 Imagen real del equipo

El siguiente es el script de la configuración del Firewall en cuestión. Se dieron de alta los ACL necesarios para dar acceso solamente del PDSN a Internet en los segmentos de red autorizados. El PDSN que esta del lado de la red CDMA se considera zona de confianza. La red de Internet (UNINET) se considera del área de desconfianza.

|   |   |
|---|---|
| <pre># sysname Eudemon # firewall packet-filter default permit interzone local trust direction inbound firewall packet-filter default permit interzone local trust direction outbound #</pre> | <pre># firewall zone local set priority 100 # firewall zone trust add interface Ethernet0/0/0 add interface Ethernet1/0/0 set priority 85</pre> |
|---|---|



|  |   |
|--|---|
| <pre> nat address-group 1 201.144.197.146 201.144.197.156 nat server global 201.144.197.157 inside 192.168.1.2 nat alg enable ftp nat alg enable dns nat alg enable icmp nat alg enable netbios undo nat alg enable h323 undo nat alg enable hwcc undo nat alg enable ils nat alg enable pptp nat alg enable qq nat alg enable msn undo nat alg enable user-define undo nat alg enable mgcp undo nat alg enable rtsp firewall permit sub-ip # firewall statistic system enable # interface Aux0 async mode flow link-protocol ppp # interface Ethernet0/0/0 ip address 192.168.3.2 255.255.255.0 # interface Ethernet0/0/1 ip address 201.144.197.145 255.255.255.240 # interface Ethernet1/0/0 ip address 200.44.44.42 255.255.255.0 # interface Ethernet1/0/1 # interface NULL0 # acl number 2001 rule 5 permit source 10.12.10.0 0.0.0.255 acl number 2003 rule 5 permit source 192.168.3.0 0.0.0.255 rule 10 permit source 10.0.0.0 0.255.255.255 rule 15 permit source 200.44.44.0 0.0.0.255 rule 20 permit source 192.168.0.0 0.0.255.255 acl number 2005 rule 5 permit source 192.168.3.3 0 acl number 2006 rule 5 permit source 192.168.3.2 0 acl number 2009 rule 5 permit source 192.168.3.0 0.0.0.255 acl number 2011 rule 5 permit source 201.144.0.0 0.0.255.255 </pre> | <pre> # firewall zone untrust add interface Ethernet0/0/1 set priority 5 # firewall zone dmz set priority 50 # firewall interzone local trust packet-filter 2006 inbound packet-filter 2006 outbound # firewall interzone local untrust packet-filter 2011 inbound packet-filter 2011 outbound # firewall interzone local dmz # firewall interzone trust untrust packet-filter 2003 inbound packet-filter 2003 outbound nat outbound 2003 address-group 1 # firewall interzone trust dmz # firewall interzone dmz untrust # aaa authentication-scheme default # authorization-scheme default # accounting-scheme default # domain default # ip route-static 0.0.0.0 0.0.0.0 201.144.197.158 ip route-static 10.0.0.0 255.0.0.0 192.168.3.1 ip route-static 192.168.0.0 255.255.255.0 192.168.3.1 ip route-static 192.168.1.2 255.255.255.255 192.168.3.1 # &lt;Eudemon&gt; &lt;Eudemon&gt; &lt;Eudemon&gt; &lt;Eudemon&gt; &lt;Eudemon&gt; </pre> |
|--|---|

### 5.10.4 Configuración subgabinete de tarjetas.

Luego de configurar los equipos auxiliares, se procede a configurar el subastidor que ya es propiamente el equipo PDSN. La configuración se hace a través de un cable especial DB9-RJ45 (cable azul) que se conecta del lado del PDSN a la consola ubicada en la tarjeta SRU (conector RJ45) y en la computadora al puerto serial. En caso de que la computadora no tenga cable serial se usa un adaptador de cable serial a USB (izq). La Figura 5.10 muestra como son físicamente estos cables



Figura 5.10 Cable para consola

La siguiente imagen muestra, la distribución de las tarjetas en el subastidor, las funciones de cada una de ellas ya se repasó en el capítulo 4:

|   |   |   |   |   |    |   |   |   |   |
|---|---|---|---|---|----|---|---|---|---|
| L | L | S | S | S | S  | S | S | S | S |
| P | P | P | P | R | R  | P | P | P | P |
| U | U | U | U | U | U  | U | U | U | U |
| 1 | 2 | 3 | 4 | 9 | 10 | 5 | 6 | 7 | 8 |



Figura 5.11 Tarjetas subastidor PDSN

De acuerdo a lo estudiado en el capítulo 4, usando los cables mencionados anteriormente, se procede a configurar el equipo. El siguiente es el script utilizado en este proyecto, en el se define todo el ruteamiento que va tanto a la red CDMA2000, a la red de UNINET y a RADIUS para la parte de autenticación. La configuración de parámetros en el PDSN consiste en 11 pasos:



- Configuración del sistema
- Configuración de las direcciones IP físicas
- Configuración de las direcciones IP lógicas
- Configuración del A11
- Configuración del AAA
- Configuración del servidor de autenticación
- Configuración del "pool" de direcciones IP
- Configuración PPP (servidor DNS)
- Configuración de los parámetros de tarificación
- Configuración de las rutas
- Salvar la configuración

```
+++ PDSN      2008-11-07 17:28:00
O&M #247
%%DSP MMLTXT:;%%
RETCODE = 0 Execution succeeded
```

```
● SET HOSTN: HOSTN = "NXGO";
ACT FTPSVR: ;
SET PRESPT: SPT = "/";
SET SUFSPT: SPT = "@";
SET LOCALUSER: USER = "XXXXXX",PT = SIMPLE,PWD = "*****";
SET FTPDIR: USER = "PDSN9660",DIR = "hd:";
SET LOCALUSER: USER = "XXXXX",PT = SIMPLE,PWD = "*****";
DEA SRUSWP: ;
SET PPP: HOST = "NXGO",TIMEOUT = 10;
SET MSIDAUTH: AUTHSW = OFF,IMSILEN = 5,PWD = "*****";
MOD RCK: LN = 0,ROW = 0,COL = 0;
● ADD INTF: INTFN = "Ethernet0/0/0";
SET NEGOAUTO: INTFN = "Ethernet0/0/0";
ACT INTF: INTFN = "Ethernet0/0/0";
ADD IP: INTFN = "Ethernet0/0/0", IPADDR = "10.166.65.10",MASK = "255.255.255.0";
ADD INTF: INTFN = "Ethernet1/0/0";
ADD INTF: INTFN = "Ethernet1/0/1";
ADD INTF: INTFN = "Ethernet1/0/2";
ADD INTF: INTFN = "Ethernet1/0/3";
ADD INTF: INTFN = "Ethernet1/0/4";
ADD INTF: INTFN = "Ethernet1/0/5";
ADD INTF: INTFN = "Ethernet1/0/6";
ADD INTF: INTFN = "Ethernet1/0/7";
ADD INTF: INTFN = "Ethernet1/0/8";
ADD INTF: INTFN = "Ethernet1/0/9";
ADD INTF: INTFN = "Ethernet1/0/10";
ADD INTF: INTFN = "Ethernet1/0/11";
ADD INTF: INTFN = "Ethernet1/0/12";
ADD INTF: INTFN = "Ethernet1/0/13";
ADD INTF: INTFN = "Ethernet1/0/14";
SET NEGOAUTO: INTFN = "Ethernet1/0/14";
ACT INTF: INTFN = "Ethernet1/0/14";
ADD IP: INTFN = "Ethernet1/0/14", IPADDR = "192.168.3.1",MASK = "255.255.255.0";
ADD INTF: INTFN = "Ethernet1/0/15";
```





```
RMV NEGOAUTO: INTFN = "Ethernet1/0/15";
SET DUPLEX: INTFN = "Ethernet1/0/15", DUPTYPE = FULL;
ACT INTF: INTFN = "Ethernet1/0/15";
ADD INTF: INTFN = "Ethernet1/0/15.1";
SET VLANTYPE: INTFN = "Ethernet1/0/15.1", VLANID = 2001;
ACT INTF: INTFN = "Ethernet1/0/15.1";
ADD IP: INTFN = "Ethernet1/0/15.1", IPADDR = "192.168.0.93",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.2";
SET VLANTYPE: INTFN = "Ethernet1/0/15.2", VLANID = 2002;
ACT INTF: INTFN = "Ethernet1/0/15.2";
ADD IP: INTFN = "Ethernet1/0/15.2", IPADDR = "192.168.0.85",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.3";
SET VLANTYPE: INTFN = "Ethernet1/0/15.3", VLANID = 2003;
ACT INTF: INTFN = "Ethernet1/0/15.3";
ADD IP: INTFN = "Ethernet1/0/15.3", IPADDR = "192.168.0.101",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.4";
SET VLANTYPE: INTFN = "Ethernet1/0/15.4", VLANID = 2004;
ACT INTF: INTFN = "Ethernet1/0/15.4";
ADD IP: INTFN = "Ethernet1/0/15.4", IPADDR = "192.168.0.61",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.5";
SET VLANTYPE: INTFN = "Ethernet1/0/15.5", VLANID = 2005;
ACT INTF: INTFN = "Ethernet1/0/15.5";
ADD IP: INTFN = "Ethernet1/0/15.5", IPADDR = "192.168.0.77",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.6";
SET VLANTYPE: INTFN = "Ethernet1/0/15.6", VLANID = 2006;
ACT INTF: INTFN = "Ethernet1/0/15.6";
ADD IP: INTFN = "Ethernet1/0/15.6", IPADDR = "192.168.0.69",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.7";
SET VLANTYPE: INTFN = "Ethernet1/0/15.7", VLANID = 2101;
ACT INTF: INTFN = "Ethernet1/0/15.7";
ADD IP: INTFN = "Ethernet1/0/15.7", IPADDR = "192.168.0.117",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.8";
SET VLANTYPE: INTFN = "Ethernet1/0/15.8", VLANID = 2102;
ACT INTF: INTFN = "Ethernet1/0/15.8";
ADD IP: INTFN = "Ethernet1/0/15.8", IPADDR = "192.168.0.109",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.9";
SET VLANTYPE: INTFN = "Ethernet1/0/15.9", VLANID = 2201;
ACT INTF: INTFN = "Ethernet1/0/15.9";
ADD IP: INTFN = "Ethernet1/0/15.9", IPADDR = "192.168.0.125",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.10";
SET VLANTYPE: INTFN = "Ethernet1/0/15.10", VLANID = 2202;
ACT INTF: INTFN = "Ethernet1/0/15.10";
ADD IP: INTFN = "Ethernet1/0/15.10", IPADDR = "192.168.0.133",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.11";
SET VLANTYPE: INTFN = "Ethernet1/0/15.11", VLANID = 2203;
ACT INTF: INTFN = "Ethernet1/0/15.11";
ADD IP: INTFN = "Ethernet1/0/15.11", IPADDR = "192.168.0.141",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.12";
SET VLANTYPE: INTFN = "Ethernet1/0/15.12", VLANID = 2301;
ACT INTF: INTFN = "Ethernet1/0/15.12";
ADD IP: INTFN = "Ethernet1/0/15.12", IPADDR = "192.168.0.29",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.13";
SET VLANTYPE: INTFN = "Ethernet1/0/15.13", VLANID = 2302;
```





```
ACT INTF: INTFN = "Ethernet1/0/15.13";
ADD IP: INTFN = "Ethernet1/0/15.13", IPADDR = "192.168.0.37",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.14";
SET VLANTYPE: INTFN = "Ethernet1/0/15.14", VLANID = 2303;
ACT INTF: INTFN = "Ethernet1/0/15.14";
ADD IP: INTFN = "Ethernet1/0/15.14", IPADDR = "192.168.0.53",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.15";
SET VLANTYPE: INTFN = "Ethernet1/0/15.15", VLANID = 2304;
ACT INTF: INTFN = "Ethernet1/0/15.15";
ADD IP: INTFN = "Ethernet1/0/15.15", IPADDR = "192.168.0.45",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.16";
SET VLANTYPE: INTFN = "Ethernet1/0/15.16", VLANID = 2305;
ACT INTF: INTFN = "Ethernet1/0/15.16";
ADD IP: INTFN = "Ethernet1/0/15.16", IPADDR = "192.168.0.5",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.17";
SET VLANTYPE: INTFN = "Ethernet1/0/15.17", VLANID = 2306;
ACT INTF: INTFN = "Ethernet1/0/15.17";
ADD IP: INTFN = "Ethernet1/0/15.17", IPADDR = "192.168.0.21",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet1/0/15.18";
SET VLANTYPE: INTFN = "Ethernet1/0/15.18", VLANID = 2307;
ACT INTF: INTFN = "Ethernet1/0/15.18";
ADD IP: INTFN = "Ethernet1/0/15.18", IPADDR = "192.168.0.13",MASK = "255.255.255.248";
ADD INTF: INTFN = "Ethernet2/0/0";
ADD INTF: INTFN = "Ethernet2/0/1";
ADD INTF: INTFN = "Ethernet2/0/2";
ADD INTF: INTFN = "Ethernet2/0/3";
ADD INTF: INTFN = "Ethernet2/0/4";
ADD INTF: INTFN = "Ethernet2/0/5";
ADD INTF: INTFN = "Ethernet2/0/8";
ADD INTF: INTFN = "Ethernet2/0/9";
ADD INTF: INTFN = "Ethernet2/0/10";
ADD INTF: INTFN = "Ethernet2/0/13";
ADD INTF: INTFN = "Ethernet2/0/14";
ADD INTF: INTFN = "Ethernet2/0/15";
ADD INTF: INTFN = "NULL0";
    • ADD INTF: INTFN = "Pif0";
ADD INTF: INTFN = "Piif3/0/0";
ADD IP: INTFN = "Piif3/0/0", IPADDR = "192.168.1.2",MASK = "255.255.255.255";
ADD INTF: INTFN = "Rpif3/0/0";
ADD IP: INTFN = "Rpif3/0/0", IPADDR = "192.168.4.1",MASK = "255.255.255.255";
    • SET SPI: PCFIP = "192.168.0.78",PDSNIP = "192.168.4.1",SPI = 256,SKEY =
      "1234567891234567";
SET SPI: PCFIP = "192.168.0.142",PDSNIP = "192.168.4.1",SPI = 256,SKEY =
"1234567891234567";
SET SPI: PCFIP = "192.168.0.134",PDSNIP = "192.168.4.1",SPI = 256,SKEY =
"1234567891234567";
SET SPI: PCFIP = "192.168.0.126",PDSNIP = "192.168.4.1",SPI = 256,SKEY =
"1234567891234567";
SET SPI: PCFIP = "192.168.0.118",PDSNIP = "192.168.4.1",SPI = 256,SKEY =
"1234567891234567";
SET SPI: PCFIP = "192.168.0.110",PDSNIP = "192.168.4.1",SPI = 256,SKEY =
"1234567891234567";
```



```
SET SPI: PCFIP = "192.168.0.102",PDSNIP = "192.168.4.1",SPI = 256,SKEY =
"1234567891234567";
SET SPI: PCFIP = "192.168.0.94",PDSNIP = "192.168.4.1",SPI = 256,SKEY = "1234567891234567";
SET SPI: PCFIP = "192.168.0.86",PDSNIP = "192.168.4.1",SPI = 256,SKEY = "1234567891234567";
SET SPI: PCFIP = "192.168.0.70",PDSNIP = "192.168.4.1",SPI = 256,SKEY = "1234567891234567";
SET SPI: PCFIP = "192.168.0.62",PDSNIP = "192.168.4.1",SPI = 256,SKEY = "1234567891234567";
SET SPI: PCFIP = "192.168.0.54",PDSNIP = "192.168.4.1",SPI = 256,SKEY = "1234567891234567";
SET SPI: PCFIP = "192.168.0.46",PDSNIP = "192.168.4.1",SPI = 256,SKEY = "1234567891234567";
SET SPI: PCFIP = "192.168.0.38",PDSNIP = "192.168.4.1",SPI = 256,SKEY = "1234567891234567";
SET SPI: PCFIP = "192.168.0.30",PDSNIP = "192.168.4.1",SPI = 256,SKEY = "1234567891234567";
SET SPI: PCFIP = "192.168.0.22",PDSNIP = "192.168.4.1",SPI = 256,SKEY = "1234567891234567";
SET SPI: PCFIP = "192.168.0.14",PDSNIP = "192.168.4.1",SPI = 256,SKEY = "1234567891234567";
SET SPI: PCFIP = "192.168.0.6",PDSNIP = "192.168.4.1",SPI = 256,SKEY = "1234567891234567";
    • SET CDN: NAME = "huawei.com";
SET DOMAIN: NAME = "mfkit";
SET DOMAIN: NAME = "foncos";
SET DOMAIN: NAME = "prodigy.net.mx";
SET DOMAIN: NAME = "multifon";
    • SET AUTH: DOMAIN = "mfkit",VPNSW = NO,MIP = "148.235.128.2";
SET AUTH: DOMAIN = "prodigy.net.mx",VPNSW = NO,MIP = "148.235.128.2";
SET AUTH: DOMAIN = "multifon",VPNSW = NO,MIP = "148.235.128.2";
SET AUTH: DOMAIN = "foncos",VPNSW = NO,MIP = "148.235.128.2";
SET AUTHSEC: DOMAIN = "mfkit",MSEC = "radius";
SET AUTHSEC: DOMAIN = "prodigy.net.mx",MSEC = "radius";
SET AUTHSEC: DOMAIN = "multifon",MSEC = "radius";
SET AUTHSEC: DOMAIN = "foncos",MSEC = "radius";
    • SET ACCT: MIP = "148.235.128.2";
SET ACCTSEC: MSEC = "radius";
    • SET POOL: DOMAIN = "multifon",PID = 0,SID = 0,IP = "10.1.20.1",LEN = 250;
SET POOL: DOMAIN = "prodigy.net.mx",PID = 0,SID = 0,IP = "10.1.10.1",LEN = 250;
SET POOL: DOMAIN = "foncos",PID = 0,SID = 0,IP = "10.1.0.1",LEN = 250;
SET POOL: DOMAIN = "huawei.com",PID = 0,SID = 0,IP = "10.0.0.0",LEN = 1024;
SET POOL: DOMAIN = "mfkit",PID = 0,SID = 0,IP = "10.1.30.1",LEN = 250;
    • SET DNS: DOMAIN = "multifon",SW = LOCAL,MDNSIP = "200.33.146.249",BDNSIP =
"200.33.146.241";
SET DNS: DOMAIN = "prodigy.net.mx",SW = LOCAL,MDNSIP = "200.33.146.249",BDNSIP =
"200.33.146.241";
SET DNS: DOMAIN = "huawei.com",SW = LOCAL,MDNSIP = "200.33.146.249",BDNSIP =
"200.33.146.241";
SET DNS: DOMAIN = "mfkit",SW = LOCAL,MDNSIP = "200.33.146.249",BDNSIP =
"200.33.146.241";
SET DNS: DOMAIN = "foncos",SW = LOCAL,MDNSIP = "200.33.146.249",BDNSIP =
"200.33.146.241";
    • ADD IPRT: IP = "0.0.0.0",MASK = "0.0.0.0",PREF = 60,OUTOP = GATEWAY,GATEWAYIP =
"192.168.3.2";
ADD IPRT: IP = "10.0.0.0",MASK = "255.255.0.0",PREF = 60,OUTOP = INTF,INTFTYPE =
"Pif",INTFNUM = "0";
ADD IPRT: IP = "10.1.0.0",MASK = "255.255.0.0",PREF = 60,OUTOP = INTF,INTFTYPE =
"Pif",INTFNUM = "0";
ADD IPRT: IP = "10.192.15.0",MASK = "255.255.255.0",PREF = 60,OUTOP =
GATEWAY,GATEWAYIP = "10.166.65.254";
```



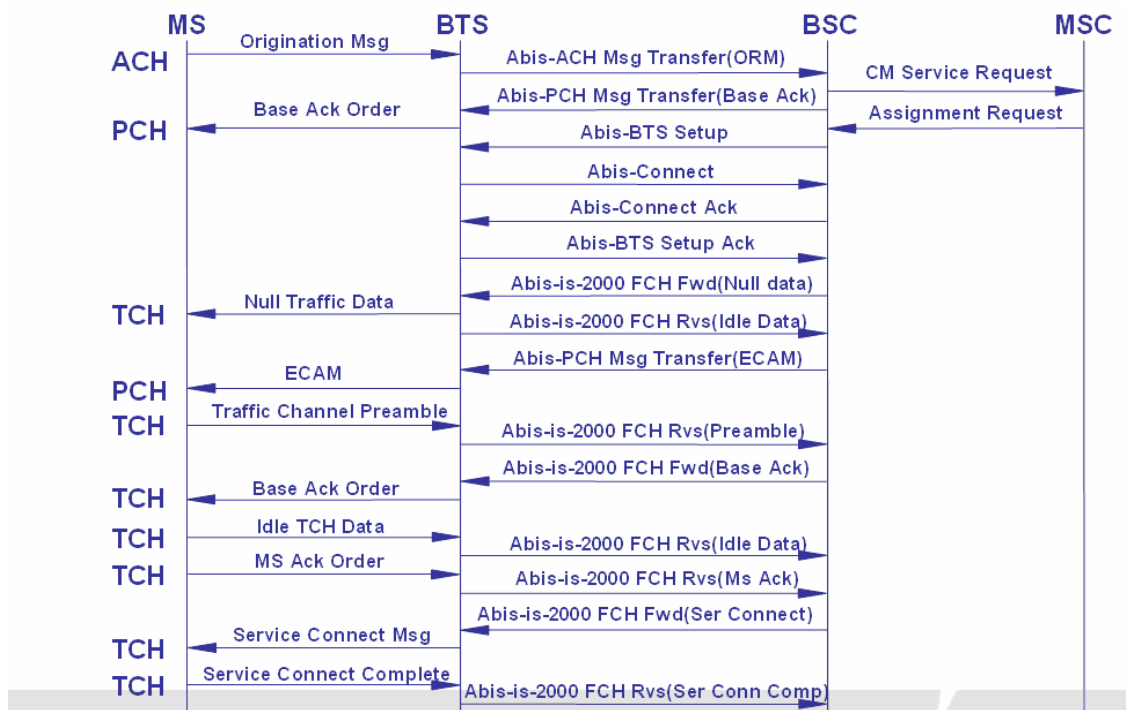
## 5.11 Puesta en funcionamiento del servicio de Internet en la Terminal FWT (Teléfono inalámbrico)

Después de haber configurado todo lo que se refiere al PDSN y suponiendo que tanto el RAC como la BTS se encuentran funcionando normalmente. Se procedió finalmente a hacer las pruebas finales de funcionamiento del servicio. Para ello fueron necesarias 4 cosas:

- Una Terminal, que en este caso es usada la FWT que se encuentra comercializando la empresa cliente para este proyecto de telefonía rural.
- Un cable DB9-USB que sirve para conectar la FWT a la computadora
- Controlador del cable, que nos ayudará a configurar la FWT como MODEM tipo "dial up".
- Computadora para poder navegar en Internet.

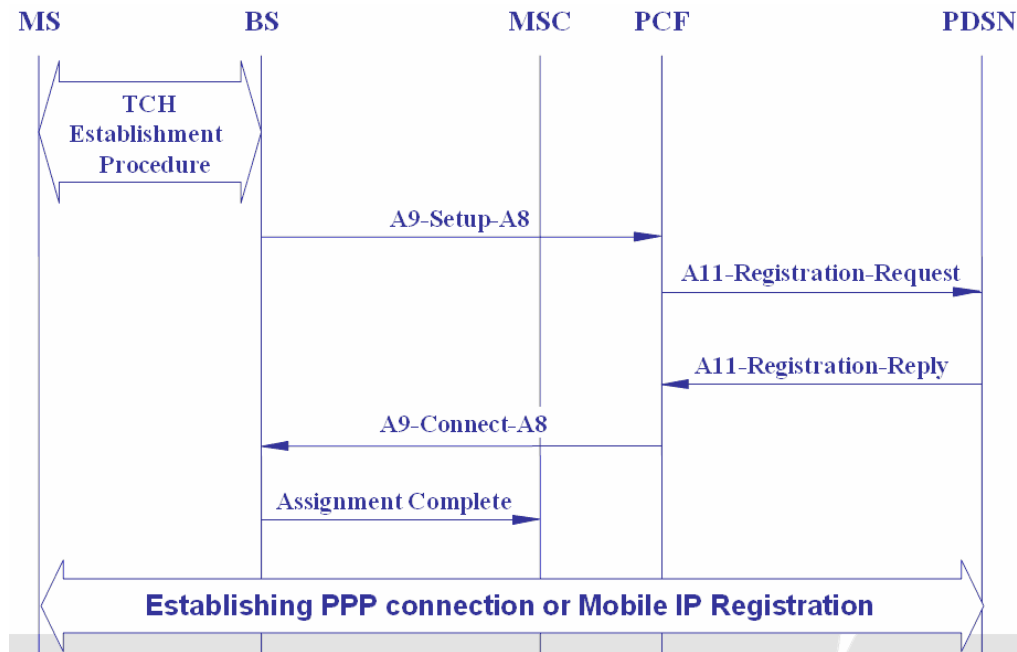
Como se vio en el capítulo 3 el servicio de Internet es posible gracias a la participación de varios equipos (FWT, BTS, RAC, PDSN), el flujo de señalización y mensajería del servicio se muestra a continuación:

- Primero el canal de tráfico (TCH) se establece

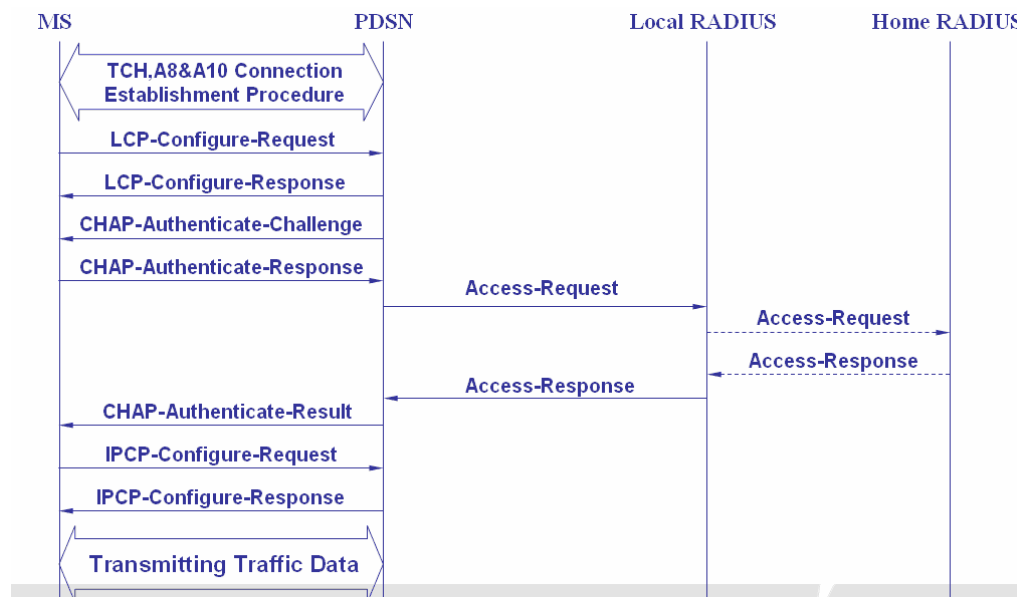




- Luego la conexión A8&A10 se establece



- Y finalmente el servicio es establecido a través de PPP (protocolo punto a punto)



Físicamente para llevar a cabo este proceso. Lo primero que hicimos para hacer estas pruebas finales fue dar del alta en el RAC los servicios de datos en la Terminal FWT correspondiente, la siguiente figura muestra como son este tipo de Terminales:



Figura 5.12 Terminales CDMA a 450 Mhz. tipo FWT



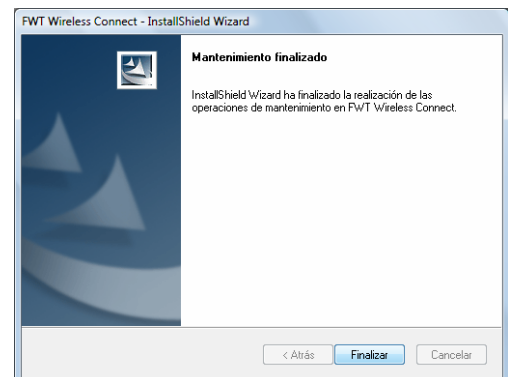
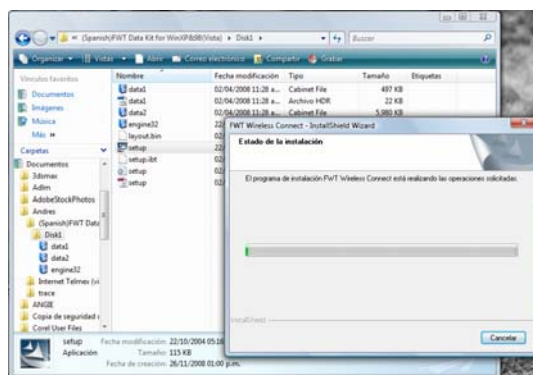
Figura 5.13 Terminal FWT conectada a la computadora con cable adaptador

Abajo y del lado izquierdo superior se pueden apreciar los teléfonos inalámbricos CDMA de 450 Mhz, del lado derecho superior se puede apreciar la llamada “caja negra” tiene la misma función solo que en lugar de tener la auricular integrada, solo tiene una entrada tipo RJ11 para conectar cualquier tipo de teléfono a gusto del usuario.

Ya que estén dados de alta los servicios de datos en el RAC, procedemos a conectar la FWT con nuestra computadora a través del cable que viene con el controlador DB9-USB, como lo muestra la figura 5.13 y se procede a configurar el respectivo controlador del cable para que la Terminal funja como MODEM de tipo dial up

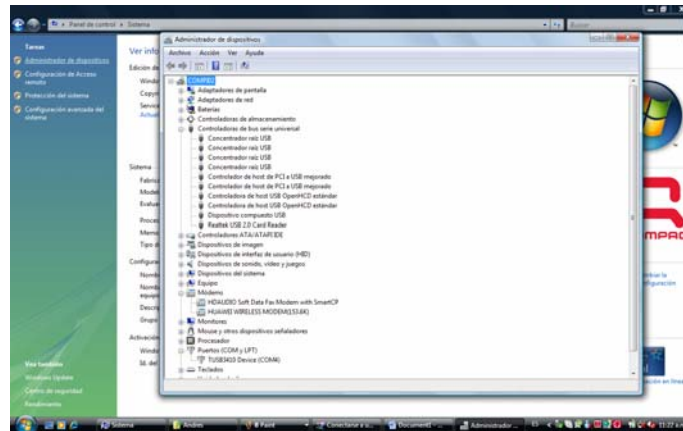
### Para la instalación del controlador se siguen los siguientes pasos:

1. Dentro del disco, se abre el archivo con nombre (Spanish)FWT Data Kit for WinXP&98(Vista) y se da doble click a setup.exe que viene ahí y se espera a que se termine esta operación (esto puede tardar varios minutos)



2. Después de varios minutos que Windows instale el controlador. Se verifica que el hardware se haya configurado correctamente en el administrador de dispositivos. tal como se ilustra en la figura siguiente:

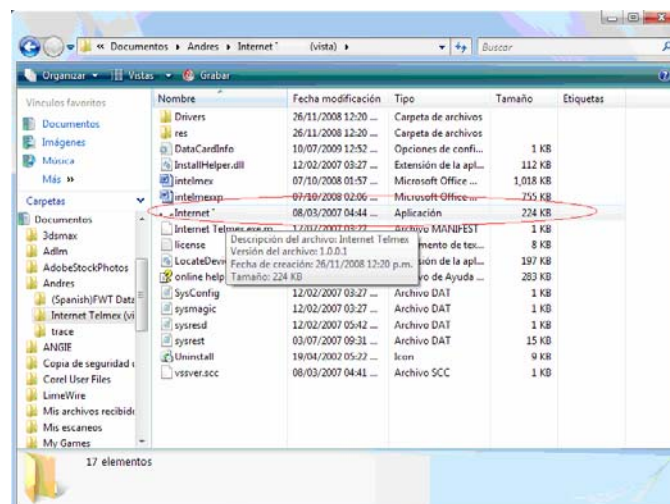
Inicio > Panel de control > sistema > Administrador de dispositivos.



- En controladores de bus serie universal NO DEBE DE HABER NINGUNO QUE DIGA DISPOSITIVO DESCONOCIDO.
- En módems debemos encontrar el WIRELESS MODEM
- En puertos (COM y LPT) debe estar el TUSB3410

En caso necesario. Se reinicia la maquina.

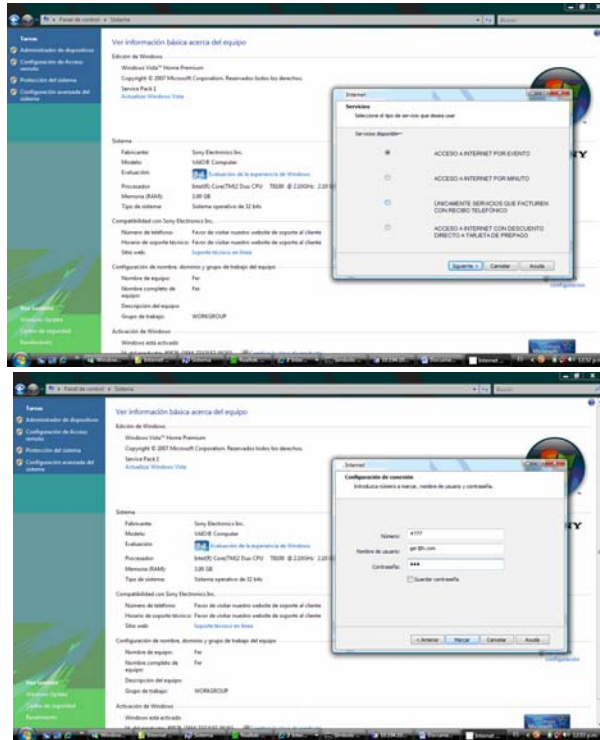
3. Ya instalado el controlador. Para conectarse a Internet, se utiliza el software llamado Wizard que viene con el nombre de Internet (vista). Aquí se da doble click al archivo que dice Internet que viene en el directorio Internet proporcionado:







En los siguientes cuadros de diálogos se escoge como se muestra:  
Pospago > (numero #777; usuario: Tlx@hw; contraseña Tlx) > marcar



4. Ya que se hayan terminado estos pasos, se abre el navegador iexplore.exe y se comienza a navegar en Internet:



Así al final logramos la meta inicial, que fue la de dar servicio de Internet a través de la Terminal inalámbrica FWT de tecnología CDMA y así cerramos el ciclo del proceso para dar dicho servicio: Computadora > FWT > BTS > RAC > **PDSN** > INTERNET.





## Acrónimos y Abreviaciones

|      |  |
|------|--|
| 3    |  |
| 3GPP | 3rd Generation Partnership Project   |
| A    |  |
| AAA  | Authentication, Authorization and Accounting<br>(Autenticación, Autorización y Tarificación) |
| ACL  | Access Control List<br>(Listado de Control de Acceso)  |
| ADM  | Add/Drop Multiplexer<br>(Multiplexor de Extracción-Inserción)                                |
| AMPS | American Mobile Phone Service<br>(Servicio de Telefonía Móvil Americana)                     |
| B    |  |
| BGP  | Border Gateway Protocol<br>(Protocolo de Entrada de la Frontera)                             |
| BSC  | Base Station Controller<br>(Controlador de la Estación Base)                                 |
| BSS  | Base Station System<br>(Sistema de la Estación Base)   |
| BTS  | Base Transceiver Station<br>(Estación de Transmisor-receptor Base)                           |
| C    |  |
| CDMA | Code Division Multiple Access<br>(Acceso Múltiple por División de Código)                    |
| CN   | Core Network<br>(Red Central)  |
| CPE  | Customer Premise Equipment<br>(Equipo de Premisa de Cliente)                                 |
| CS   | Circuit Switching<br>(Conmutación de Circuitos)  |
| D    |  |
| DNS  | Domain Name Server<br>(Servidor de Nombres de Dominio)                                       |
| E    |  |
| EM   | Estación Móvil   |
| EVDO | Evolution Data Only<br>(Evolución de Solo Datos)   |
| F    |  |
| FA   | Foreign Agent<br>(Agente Extranjero)   |
| FDD  | Frequency Division Duplex<br>(Duplexación por División de Frecuencia)                        |



|      |  |
|------|--|
| FDDI | Fiber Distributed Data Interface<br>(Interfaz de Datos Distribuida por Fibra)            |
| FDMA | Frequency Division Multiple Access<br>(Acceso Multiple por División de Frecuencias)      |
| FE   | Fast Ethernet<br>(Ethernet Rápido)   |
| FTP  | File Transfer Protocol<br>(Protocolo de Transferencia de Archivos)                       |
| FWT  | Fixed Wileless Telephone<br>(Teléfono Inalámbrico Fijo)                                  |
| G    |  |
| GRE  | Generic Routing Encapsulation<br>(Encapsulado de Ruteo Generico)                         |
| GSM  | Global System for Mobile Communication<br>(Sistema Global para Comunicaciones Móviles)   |
| GPRS | General Packet Radio Service<br>(Servicio de Radio de Paquetes Generales)                |
| H    |  |
| HA   | Home Agent<br>(Agente Domestico)   |
| HLR  | Home Location Register<br>(Registro de Localización Domestico)                           |
| HTTP | Hyper Text Transfer Protocol<br>(Protocolo de Transferencia de Hipertexto)               |
| I    |  |
| IEEE | Instituto de Ingenieros en Electricidad y Electrónica                                    |
| ISP  | Internet Service Provider<br>(Proveedor de Servicios de Internet)                        |
| IP   | Internet Protocol<br>(Protocolo de Internet)   |
| L    |  |
| LAN  | Local Area Network<br>(Red de Área Local)  |
| LPU  | PDSN Line interface Processing Unit<br>(Unidad Central del Interfaces de línea del PDSN) |
| M    |  |
| MAC  | Media Access Control<br>(Control de Acceso al Medio)                                     |
| MIP  | Mobile IP<br>(IP Móvil)  |
| MPLS | Multiprotocol Label Switching<br>(Conmutación Multi-Protocolo mediante Etiquetas)        |
| MS   | Mobile Station<br>(Estación Móvil)   |



|        |   |
|--------|---|
| N      |   |
| NGN    | Next Generation Network<br>(Red de Siguiente Generación)  |
| NP     | Network Processor<br>(Procesador de Red)  |
| NTP    | Network Time Protocol<br>(Protocolo de Tiempo de Red)   |
| O      |   |
| OSI    | Open System Interconnection<br>(Interconexión de Sistemas Abiertos)   |
| OT     | Orden de Trabajo  |
| P      |   |
| PCF    | Packet Control Function<br>(Función de Control del Paquete)   |
| PDN    | Packet Data Network<br>(Red de Paquetes de Datos)   |
| PDSN   | Packet Data Serving Node<br>(Nodo de Servicio de Paquetes de Datos)   |
| PDU    | Protocol Data Unit<br>(Unidad de Datos de Protocolo)  |
| PPP    | Point-to-Point Protocol<br>(Protocolo Punto a Punto)  |
| PPS    | Pre-Paid Service<br>(Servicio de Prepago)   |
| PS     | Packet Switching<br>(Conmutación de Paquetes)   |
| PSTN   | Public Switched Telephone Network<br>(Red Telefónica de Conmutación Pública)  |
| Q      |   |
| QoS    | Quality of Service<br>(Calidad de Servicio)   |
| R      |   |
| RADIUS | Remote Authentication Dial In User Service<br>(Servicio de Usuario de Marcado de Entrada para la Autenticación a Distancia) |
| RAN    | Radio Access Network<br>(Red de Acceso de Radio)  |
| RAC    | Radio Access Controller<br>(Controlador de Acceso de Radio)   |
| RAS    | Remote Access Server<br>(Servidor de Acceso Remoto)   |
| RCDT   | Red Corporativa de Datos Tlx (cliente)  |
| RFC    | Request For Comments<br>(Petición de Comentarios)   |



|      |  |
|------|--|
| S    |  |
| SCP  | Service Control Point<br>(Punto de Control de Servicios)                                       |
| SMTP | Simple Mail Transfer Protocol<br>(Protocolo Simple de Transferencia de Correo)                 |
| SPU  | PDSN Signaling Process Unit<br>(Unidad de Proceso de Señalización del PDSN)                    |
| SRU  | PDSN Switching and Routing Unit<br>(Unidad de Conmutación y Encaminamiento del PDSN)           |
| T    |  |
| TCP  | Transmission Control Protocol<br>(Protocolo de Control de Transmisión)                         |
| TDD  | Time Division Duplex<br>(Duplexación por División de Tiempo)                                   |
| TDMA | Time Division Multiple Access<br>(Acceso Múltiple por División de Tiempo)                      |
| TFTP | Trivial File Transfer Protocol<br>(Protocolo Trivial de Transferencia de Archivos)             |
| U    |  |
| UDP  | User Datagram Protocol<br>(Protocolo de Datagrama de Usuario)                                  |
| UMTS | Universal Mobile Telecommunication System<br>(Sistema de Telecomunicaciones Móviles Universal) |
| USR  | Universal Switching Router<br>(Ruteador de Conmutación Universal)                              |
| UTP  | Unshielded Twisted Pair<br>(Par Trenzado sin Apantallar)                                       |
| UDR  | User Data Record<br>(Expediente de Datos de Usuario)   |
| V    |  |
| VLR  | Visitor Location Register<br>(Registro de la Localización del Visitante)                       |
| VPN  | Virtual Private Network<br>(Red Privada Virtual)   |
| W    |  |
| WLL  | Wireless Local Loop<br>(Bucle Local Inalámbrico)   |
| WWW  | World Wide Web<br>Red Global Mundial   |



## Conclusiones

Una de las grandes ventajas que existen con las nuevas redes de tercera generación es la capacidad de dar conectividad y comunicación de infinidad de servicios no solo de voz, sino también de datos y video. Estos grandes avances tecnológicos dan cabida a una serie de ventajas que previamente en este trabajo ya se han expuesto.

El trabajo aquí presentado fue el caso particular de un proyecto de tecnología CDMA2000 a 450 Mhz. que esta actualmente llevándose a cabo en México por parte de una de las empresas de servicios de telecomunicaciones “carriers” más importantes de nuestro país con equipo de una de las proveedoras mas importantes a nivel mundial de origen chino. Se pretende que con este trabajo no solo exista una guía práctica para el que la consulte, si no que también sea una referencia actual para cualquier lector que quiera profundizar sus conocimientos en las redes inalámbricas de última generación.

Se cumple exitosamente con este documento la finalidad de explicar concisa y detalladamente el proceso técnico que se llevó a cabo para dar conexión a Internet en esta red comercial de telefonía fija rural inalámbrica, siendo el PDSN9660 el equipo mas importante de este proceso, para que poblaciones alejadas de las ciudades puedan tener la misma oportunidad de acceso a la red como en las grandes ciudades e intentar así disminuir un poco la brecha tecnológica que actualmente tenemos en México, entendiéndola como un importantísimo foco rojo que tenemos que combatir, refiérase al anexo 4, “Impacto Socioeconómico del proyecto (Brecha Tecnológica)”.

Particularmente en el tema aquí tratado, para poder implementar el equipo PDSN9660 en esta red, se involucraron todos los temas aquí abordados directa o indirectamente y se pusieron en práctica conocimientos básicos y avanzados de comunicación de datos, telefonía inalámbrica y medios físicos de comunicación. De igual forma se aprendió como se instala y comisiona un equipo de producción en campo.

No cabe duda que los conocimientos en redes y telecomunicaciones de la escuela fueron base para poder participar en este proyecto positivamente, se constato que lo aprendido en varias materias de la carrera se aplica al 100% en el campo laboral. Sin embargo, cabe aclarar, que este proyecto que ya es real de campo, fue un claro ejemplo de que no solo se conjunta todo lo visto en la escuela, si no que también a través de la experiencia es como uno aprende los pequeños detalles técnicos que hacen la gran diferencia entre que funcione y no funcione toda una red, siendo esto lo que realmente vale y nos hace desarrollarnos personal y profesionalmente.



## Bibliografía

1. Michael Daoud Yacoub, "Wíreles technology", CRC press
2. José M Huidobro, "Manual de Telecomunicaciones", Alfaomega
3. Minoru Ethou, "Next generation Mobile systems", Wiley
4. Ata Elia, Ph.D, "Network Communications Technology", Elahi
5. Jesús Garcia Tomas, Santiago Ferrando, Mario Piattini", Redes para Proceso Distribuido", Alaomega
6. David Roldan, "Comunicaciones Inalámbricas", Alfaomega
7. CCNA Cisco Vol.1
8. Documento del cliente Criterios de Ingeniería CDMA V.1 y V2.
9. Manual del equipo PDSN9660 del proveedor



## Anexos

| AREA             | CENTRAL      | SIGLAS | CELL EDIFICIO  | IDENTIFICACION DEL EQ. EN LA DIVISION O SOLDO | TIPO DE EQUIPO (MODELO) | FUNCION DEL EQUIPO | UBICACION DEL EQUIPO  |
|------------------|--------------|--------|----------------|---|-------------------------|--------------------|---|
| CUAUTLAN         | CUAUTLAN     | CUT    | CTUN/MC/UD00   | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | SUR/ET EN PROCESO   |
| TOLUCA           | NE/ADO       | NE/    | TOUC/OME       | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | En sabde tramite bu 03/10/1401, 03/10/1406 y 03/10/1411       |
| ACA PULCO        | HDA USO      | HD     | ACPL/GCH       | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | 7th 1034 por 15, 20 y 25                                      |
| CHILPANCIAGO     | CHILPANCIAGO | CHI    | CHPL/GCH       | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | 7th 1036 por 26, 31 y 36                                      |
| CHERILAVACA      | BORDA        | BO R   | CHM/XO/BO      | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | 7th 1044 por 6, 11 y 16                                       |
| PACHUCA          | PELOUCON     | PE/    | PCHEM/BO/3     | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | EL PACSERA UBICADO EN LA FILA 103 JUNTO AL GLT                |
| POZA RICA        | POZA RICA    | POZ    | PEPO/PR/0051   | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | EL PACSERA UBICADO EN LA FILA 107 JUNTO AL BASTIDOR EXISTENTE |
| PUEBLA           | FUERTES      | FUR    | PUBL/BB/PL/02  | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | EL PACSERA UBICADO EN LA FILA 101                             |
| COATEACOLAOS     | PETROLERA    | PTR    | CTCS/PR/PT/051 | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | EL PACSERA UBICADO EN LA FILA 105 JUNTO AL GLT                |
| COFOBOA          | COFOBOA      | COB    | CFBOV/BO/0000  | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | EL PACSERA UBICADO EN LA FILA 104 JUNTO AL GLT                |
| VER              | MICA MBO     | MOA    | VPRCZ/PR/CO/00 | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | EL PACSERA UBICADO EN LA FILA 2018 POSICIONES 49, 54, 59      |
| TUXTLA GUTIERREZ | TUXTLA GTE.  | TGU    | TNG/XTG/TS     | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | Sabde tramite bu En tramite 01/10/0846 y 01/10/0851           |
| TUXTLA GUTIERREZ | TALANA       | TAL    | TNG/XTG/TA     | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | En sabde tramite bu 03/10/0859 y 03/10/0864                   |
| OAXACA           | BLERARIO     | BL     | OAX/CO/ABE     | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | En sabde tramite bu 01/10-105 -Lank: A Postbne e 01, 06, 11   |
| OAXACA           | JUCHITAN     | JUC    | JCH/NO/SAU     | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | En sabde tramite bu 01/10-105 -Lank: A Postbne e 01, 06, 11   |
| OAXACA           | COSCOA       | AYD    | CMS/CO/CO/0051 | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | 007101A, 20, 007101A, 15 Y 007101A, 10.                       |
| VILLAHERMOSA     | PASIBO       | PE     | VH/PR/PR       | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | 0272020A, 01 y 0272020A, 06.                                  |
| MERIDA           | PLAZA        | PLA    | MEPR/UP/L      | ESTACION CONTROLADO RA COMA                   | Pac 6610                | Controlador de BTS | 0272020A, 24, 0272020A, 29 y 0272020A, 34                     |

| TIPO DE SALA | PISO | PROVEEDOR | ESTADO | MUNICIPIO                 | LOCALIDAD        | DOMICILIO                                   |                                   |
|--------------|------|-----------|--------|---------------------------|------------------|---|-----------------------------------|
| TRANSMISION  | 1er. | HUAWB     | MEX    | CUAUTLAN DE RO MERO RUBIO | MEXICO           | AV 30 DE NOVIEMBRE NR 206                   | CENTRO                            |
| TRANSMISION  | 3er. | HUAWB     | MEX    | TOLUCA                    | MEXICO           | FELICE BERRIOSA VAL #504                    | VALLE VERDE                       |
| TRANSMISION  | 1er. | HUAWB     | GRO    | ACA PULCO                 | GUERRERO         | HDA USO #28                                 | CENTRO                            |
| TRANSMISION  | 2do  | HUAWB     | GRO    | CHILPANCIAGO              | CHILPANCIAGO     | B. DOMINGUES ESQ. 5 DE MAYO                 | CENTRO                            |
| TRANSMISION  | P.B. | HUAWB     | MOR    | GUERRAVACA                | MOBLOS           | HDA USO OTE. # 307, GUERRAVACA, MOR.        | CENTRO                            |
| TRANSMISION  | 1er  | HUAWB     | VER    | PACHUCA DESOTO            | PACHUCA DESOTO   | C. 12 DE OCTUBRE No. 12                     | PERIFERIAS                        |
| TRANSMISION  | 1er  | HUAWB     | VER    | POZA RICA                 | POZA RICA        | CALLE CUA No 108                            | 27 DE SEPTIEMBRE                  |
| TRANSMISION  |      | HUAWB     | VER    | PUEBLA                    | PUEBLA           | C-26 NOFTE No. 1013                         | HUMULOT                           |
| TRANSMISION  |      | HUAWB     | VER    | COATEACOLAOS              | COATEACOLAOS     | HDA USO No. 1526                            | BENITO JUAREZ NORTE               |
| TRANSMISION  | P6   | HUAWB     | VER    | VERACRUZ                  | VERACRUZ         | AV. PETA No. 15                             | FRACC. HILDO                      |
| TRANSMISION  | 1    | HUAWB     | GCH    | TUXTLA GUTIERREZ          | TUXTLA GUTIERREZ | 2A AVENIDA SUP ORIENTE No.387               | CENTRO                            |
| TRANSMISION  | 3    | HUAWB     | GCH    | TAPACHULA                 | TAPACHULA        | 2A AVENIDA SUP No 7                         | CENTRO                            |
| TRANSMISION  | 1    | HUAWB     | OAX    | OAXACA                    | OAXACA           | B. EL SA RDO DOMINGUEZ SIN ESQ. MAHUBA, PUC | PERIFERIA                         |
| TRANSMISION  | 1    | HUAWB     | OAX    | JUCHITAN                  | JUCHITAN         | AV. OAXACA SIN                              | CENTRO                            |
| TRANSMISION  | 1    | HUAWB     | GRO    | BENITO JUAPEZ             | CANJUN           | AV. PUERTO JUAPEZ, NC 500 LOTES 1-8         | REGION 102                        |
| TRANSMISION  | 1er  | HUAWB     | TAB    | CENTRO                    | VILLAHERMOSA     | PDLONGACON 27 DE FEBRERO # 2848             | FRACC. GALA MANSOOL TABASCOO 2000 |
| TRANSMISION  | 2er  | HUAWB     | YUC    | MERIDA                    | MERIDA           | CALLE 59 # 532 POR 61                       | CENTRO                            |

Anexo 1. Ubicación de los 18 RACs del proveedor





INSTITUTO POLITÉCNICO NACIONAL  
ESIME CULHUACAN



| AREA             | CENTRAL     | SIGLAS      | CLLIEDIFICIO | TIPO DE EQUIPO (MODELO)      | FUNCION DEL EQUIPO | ANILLOTMS A UTILIZAR | SALA        | PISO |
|------------------|-------------|-------------|--------------|------------------------------|--------------------|----------------------|-------------|------|
| CUAUTITLAN       | CUT         | CTLXMXCUDCO | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | POR DEFINIR        | PTAZ                 | POR DEFINIR |      |
| TOLUCA           | NEV         | TOLOXME     | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | MEXICO-TOLUCA ST   | PTAZ                 | 2           |      |
| ACAPULCO         | HIDALGO     | ACPLXGH     | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | BUSACAPULCO-CUES3  | PTAZ                 | POR DEFINIR |      |
| CHILPANCIAGO     | CHI         | CHLPXGH     | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | BUSACAPULCO-CUES3  | PTAZ                 | POR DEFINIR |      |
| CUERNAVACA       | BORDA       | CRNVXBO     | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | CENTRAL S6         | PTAZ                 | 30.         |      |
| PACHUCA          | REVOLUCION  | REV         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | SUR19              | PTAZ                 | 1           |      |
| POZARICA         | POZARICA    | PZCRPPODS1  | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | SUR15              | PTAZ                 | 3           |      |
| PUEBLA           | FUERTES     | FUR         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | SUR59              | PTI                  | P.B.        |      |
| COATEACALCOS     | PETROLERA   | PTR         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | SUR59              | PTI                  | P.B.        |      |
| COPACUA          | COPACUA     | COB         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | SUR15              | PTAZ                 | 5           |      |
| VER              | MOCAMBO     | MOA         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | SUR59              | PTAZ                 | 1           |      |
| TUXTLA GUTIERREZ | TUXTLA GUT. | TGU         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | SUR59              | PTAZ                 | 5           |      |
| OAXACA           | TAKANA      | TAK         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | SUR59              | PTAZ                 | 1           |      |
| OAXACA           | BELISARIO   | BEL         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | COATZA-OAXACA ST   | PTAZ                 | 1           |      |
| OAXACA           | JUCHITAN    | JUC         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | SUR59              | PTAZ                 | 2           |      |
| CANCON           | CASCADA     | AKD         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | V.HSA-CANCON SI    | PTAZ                 | 1           |      |
| VILLAHERMOSA     | PASEO       | PSE         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | SUR59              | PTAZ                 | 2           |      |
| MERIDA           | PLAZA       | PLA         | 0ME6500      | TERMINAL MULTISERVICIO (ADM) | COATZA-MERIDA S8   | PTAZ                 | 6           |      |

| FLA | LADO | BASTIDOR | PROVEEDOR | ESTADO                     | MUNICIPIO        | LOCALIDAD                               | DOMICILIO                       |
|-----|------|----------|-----------|----------------------------|------------------|---|---------------------------------|
| 104 | 6    | 48       | MEX       | CUAUTITLAN DE ROMERO RUBIO | MEXICO           | AV. 20 DE NOVIEMBRE #206                | CENTRO                          |
| 104 | 6    | 48       | MEX       | TOLUCA                     | MEXICO           | FELIPE BERRIOGUALTESO                   | VALLEVERDE                      |
| 104 | 6    | 48       | MEX       | ACAPULCO                   | GUERRERO         | HIDALGO #28                             | CENTRO                          |
| 104 | 6    | 48       | MEX       | CHILPANCIAGO               | CHILPANCIAGO     | B. DOMINGUES EDO. 5 DE MAYO             | CENTRO                          |
| 101 | 6    | 23       | MOR       | CUERNAVACA                 | MOR ELIOS        | HIDALGO OTE. # 307, CUERNAVACA, MOR.    | CENTRO                          |
| 104 | 6    | 21       | HGO       | PACHUCA DE SOTO            | PACHUCA DE SOTO  | C. 12 DE OCTUBRE No. 12                 | PERDIDAS                        |
| 103 | 6    | 10       | PUE       | POZARICA                   | POZARICA         | CALLE URUA No. 108                      | 27 DE SEPTIEMBRE                |
| 101 | 6    | 40       | VER       | PUEBLA                     | PUEBLA           | C. 26 NO. RTE. No. 1013                 | HUBOLOT                         |
| 101 | 6    | 19       | VER       | COATEACALCOS               | COATEACALCOS     | HIDALGO No. 1535                        | BENITO JUAREZ NO RTE            |
| 104 | 6    | 21       | VER       | VERACRUZ                   | VERACRUZ         | AV. PIETA No. 45                        | FRACC. HIRCO                    |
| 103 | 6    | 39       | CHH       | TUXTLA GUTIERREZ           | TUXTLA GUTIERREZ | 2A AVENIDA SUR ORIENTE No. 387          | CENTRO                          |
| 103 | 6    | 06       | CHH       | TAPACHULA                  | TAPACHULA        | BELISARIO DOMINGUES SIN EDO. MANUEL RUE | CENTRO                          |
| 104 | 6    | 26       | OAX       | OAXACA                     | OAXACA           | AV. OAXACA SIN                          | PERIFERIA                       |
| 101 | 6    | 01       | OAX       | JUCHITAN                   | JUCHITAN         | AV. PUERTO JUAREZ ME. 300 LOTE 3+8      | CENTRO                          |
| 102 | 6    | 45       | YAB       | BENITO JUAREZ              | BENITO JUAREZ    | PROLOGADIN 27 DE FEBRERO #2848          | RESION 102                      |
| 105 | 6    | 31       | YUC       | CENTRO                     | VILLAHERMOSA     | CALLE 59 #532 P.O.R. 64                 | FRACC GALAXIAS COLTA 8-520 2000 |
| 102 | 6    | 31       | YUC       | MERIDA                     | MERIDA           | CALLE 59 #532 P.O.R. 64                 | CENTRO                          |

Anexo 2. Ubicación de las Terminales de Transporte Multi Servicio FE (ADM) en la red de larga distancia





## Anexo 4

# Impacto Socioeconómico del proyecto (Brecha Tecnológica)

Como lo hemos visto, la tesis aquí presentada tiene como objetivo dar una referencia puramente técnica del acceso a Internet en una red de telefonía rural CDMA2000. Sin embargo, me pareció también importante dar una breve reflexión con base en estadísticas, del impacto que tiene este proyecto en nuestro país desde el punto de vista socioeconómico, ya que en mi opinión es de suma importancia desarrollarnos en el ámbito laboral como ingenieros sin perder de vista algo básico en nuestra educación, las necesidades que existen en nuestro país en todos los ámbitos y nuestra constante participación, aunque sea mínima, para combatir esas necesidades con el uso de nuestros conocimientos.

Y es así precisamente cuando entramos a definir el concepto de Brecha Tecnológica, entendiéndola como “una expresión que hace referencia a la diferencia socioeconómica entre aquellas comunidades que tienen accesibilidad a Internet y aquellas que no, aunque tales desigualdades también se pueden referir a todas las nuevas tecnologías de la información y la comunicación (TIC), como el computador personal, la telefonía móvil, la banda ancha y otros dispositivos.”<sup>1</sup>

Esta definición nos permite relacionar el impacto de este proyecto de ingeniería realizado en México en varios aspectos de la vida social, política y por supuesto económica del país. Pero antes de hondar en el impacto de cada uno de estos aspectos y justificar la razón de la importancia que tiene el cerrar esta brecha tecnológica en México, me parece importante resaltar dos cosas; la primera es la importancia que tiene este tema a nivel mundial y la segunda, el lugar que estadísticamente ocupa nuestro país en acceso a Internet.

La importancia que tiene este tema es tal que apenas el pasado 5 de septiembre de 2009, se llevó a cabo en Monterrey N.L. una serie de simposios para denotar este problema. En esta serie de congresos internacionales, llamados World Summit Award y Alianza Global para las Tecnologías de la Información de las Naciones Unidas, se dio origen al llamado “Consenso de Monterrey”. El copresidente de la Cumbre Mundial de la información, Ramón Alberto Garza, detalló que este instrumento contiene conceptos “importantes” de lo que deben hacer las autoridades para cerrar la brecha informática.

<sup>1</sup> Definición conceptual. [http://es.wikipedia.org/wiki/Brecha\\_digital](http://es.wikipedia.org/wiki/Brecha_digital)



“El consenso de Monterrey pretende que se enfoquen los esfuerzos a cerrar la brecha digital en el mundo y en México [...] debemos de lograr que cada vez más gente esté conectada a la sociedad de la información, a las redes, al Internet, entonces, se propone con esta declaración que Naciones Unidas lleve la propuesta a nivel iniciativa, para buscar que así como se hace con la educación, los gobiernos del mundo contribuyan fuertemente para que la gente de escasos recursos tenga acceso a la sociedad de la información.”<sup>2</sup>

Ahora bien, ¿cuál es realmente el lugar que ocupa México en cuestión de acceso a las tecnologías de información? Hay muchos datos que nos dan distintas cifras pero podemos desmembrar estos datos, y sacar los 2 únicos aspectos que nos interesan relacionados con este proyecto.

- ¿Cuántos mexicanos tienen acceso a Internet?

Para el segundo semestre del 2001, México contaba en promedio con cinco computadoras por cada cien habitantes, y el Internet era usado sólo por 1.7 millones de los 97 millones de habitantes en nuestro país.<sup>3</sup> Para 2009, el número es mayor, sin embargo el tema de la Brecha Tecnológica no deja de ser importante, sobre todo para México, ya que únicamente 2 de cada 10 ciudadanos tienen acceso a las tecnologías de la información en el país.<sup>4</sup>

- ¿Cuántos mexicanos tienen acceso a Internet de Banda Ancha?

Recientemente “The Economist” publicó un gráfico sobre el porcentaje de personas en cada país de la OCDE (Organización para la Cooperación y Desarrollo Económico) que están suscritas a Internet de banda ancha. El país que encabeza la lista es Dinamarca, con aproximadamente 37 suscriptores a banda ancha por cada 100 habitantes. En Holanda, Suiza, Noruega y Corea del Sur hay más de 30 suscriptores por cada 100 habitantes. En último lugar está México, con apenas 7 suscriptores por cada 100 habitantes. (España, que no aparece en la gráfica de abajo, tiene 20.8 suscriptores por cada 100 habitantes). No obstante, existe una explicación por la baja penetración en México (el único país latinoamericano que pertenece a la OCDE) del Internet de banda ancha, es el alto precio de una suscripción. Los precios abajo están ajustados por paridad de compra, y muestran que sólo en Eslovaquia cuesta más el acceso a Internet de banda ancha, que en México.<sup>5</sup>

<sup>2</sup> El Universal, *ONU exige reducir la brecha tecnológica*, <http://www.eluniversal.com.mx/estados/72991.html>, Sábado 05 de septiembre de 2009

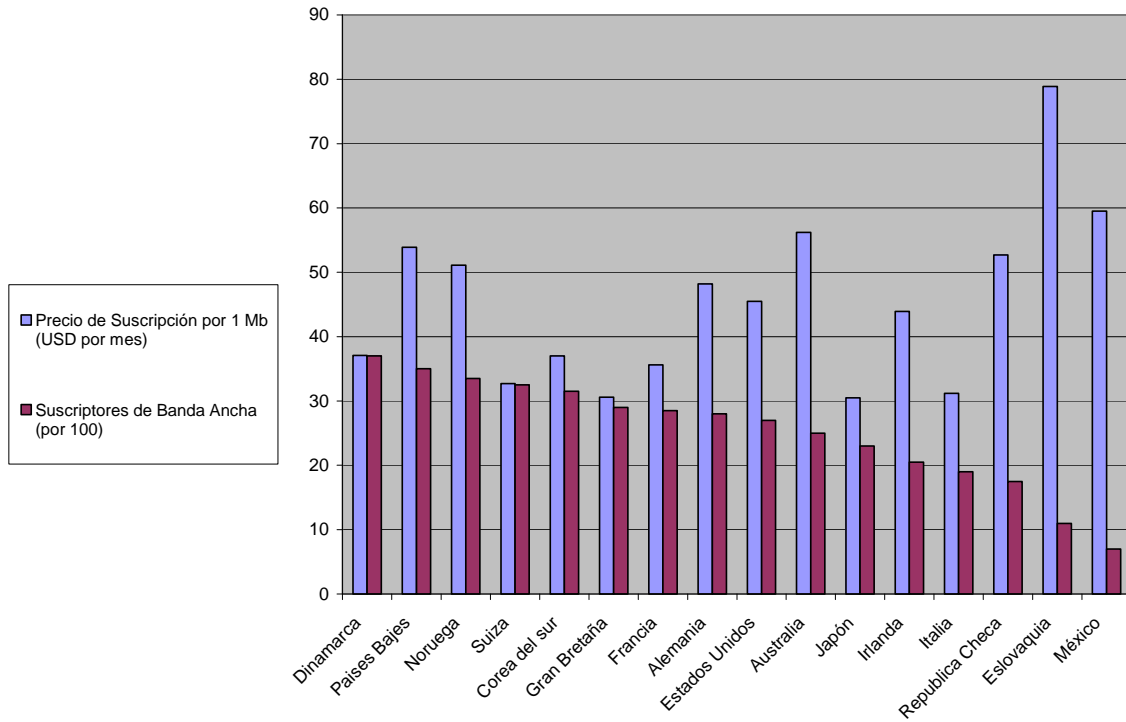
<sup>3</sup> Ing. Jorge Mendoza, *Proyecto E-Mexico*, <http://www.informaticamilenium.com.mx/paginas/mn/articulo43.htm>, Agosto 15 del 2001

<sup>4</sup> El Universal, *ONU exige reducir la brecha tecnológica*, <http://www.eluniversal.com.mx/estados/72991.html>, Sábado 05 de septiembre de 2009

<sup>5</sup> Victor, *Acceso a Internet de Banda Ancha, limitante para el e-learning*, <http://taec.com.mx/blog/2009/05/acceso-a-internet-de-banda-ancha-limitante-para-el-e-learning/>, Mayo 25, 2009



Suscriptores banda ancha OCDE - tomado de The Economist



Se hace la distinción de estos dos aspectos ya que la Banda Ancha permite tener más recursos que simplemente un acceso a Internet básico (o dial-up). Las ventajas en los aspectos sociales, económicos y políticos que a continuación analizaremos en su mayoría contemplan enlaces de Banda Ancha.

Tal es el caso de *e-learning*<sup>6</sup> ya que sin duda el acceso de Banda Ancha afecta enormemente este potencial, pues limita la calidad de los cursos multimedia, las aulas virtuales y en general la calidad de la experiencia del usuario (estudiante). Es también evidente que los siete millones y medio de usuarios con acceso a Internet de banda ancha en México en sus hogares están concentrados en los estratos socio-económicos más altos. Esta “brecha digital” entre quienes tienen acceso a ésta tecnología y quienes no tienen acceso se refleja en mejores oportunidades de educación y capacitación, que a su vez amplían la brecha socio-económica.

Dicho lo anterior, podemos ahora relacionar el proyecto “Red 3G CDMA450 para acceso a Internet” de telefonía rural con el impacto de la Brecha Tecnológica en los tres aspectos ya mencionados de la siguiente manera:

<sup>6</sup> Se le atribuye el concepto de e-learning al sistema de educación electrónica o a distancia en el que se integra el uso de las tecnologías de la información y otros elementos pedagógicos para la formación, capacitación y enseñanza de los usuarios o estudiantes en línea.





## **1) Aspecto Social**

En este aspecto podemos encontrar 2 vertientes.

- El proyecto como parte de un proyecto más grande llamado e-México
- El proyecto como instrumento de desarrollo para la educación en áreas marginadas y rurales

En el primer punto se desarrolla el proyecto CDMA450 para telefonía fija rural como parte de un proyecto mucho más ambicioso del gobierno federal llamado e-México.

### ▪ E- México<sup>7</sup>

Nace a principios del siglo XXI con varios objetivos, sin duda, en los momentos de mayor incertidumbre acerca de los efectos de la globalización y el Internet, el Gobierno de México hace público un proyecto de integración de tecnologías de comunicación a la infraestructura pública y privada en nuestro país. A continuación, citó los diez puntos más sobresalientes entorno a esta iniciativa:

1. El propósito es integrar la tecnología e ingeniería de todas las redes existentes, tanto públicas como privadas, seleccionar contenidos adecuados que permitan mejorar los servicios en cada comunidad, nivel territorial o auditorio, que incluya la interacción de sistemas en los que se despliegue información clara en sus contenidos y de fácil consulta, así como contemplar aspectos legales y jurídicos que permitan el uso universal de ciertos servicios que garanticen la privacidad y protección legal en el caso de ciertos trámites gubernamentales, entre otros aspectos.

2. Para que México pueda realmente superar los enormes contrastes que existen en el desarrollo, es necesario unir cada vez más a los mexicanos y dar igualdad de acceso y oportunidades a cada uno de los que en este país vivimos. El proyecto e-MÉXICO permitirá enlazarnos entre sí y con el resto del mundo.

3. El Gobierno Federal y las empresas privadas han invertido miles de millones de dólares en infraestructura, redes individuales que conectan al mínimo de puntos indispensables y consecuentemente tienen una capacidad que no está debidamente utilizada, tanto en las redes privadas como en las diferentes dependencias gubernamentales.

4. En México, la mayoría de la población no tiene teléfono ni acceso a una computadora y mucho menos Internet. No obstante, con e-MÉXICO se planea llevar el teléfono y otras tecnologías de información a cerca de 2,500 municipios y a unas

<sup>7</sup> Ing. Jorge Mendoza, *Proyecto E-Mexico*, <http://www.informaticamilenium.com.mx/paginas/mn/articulo43.htm>, Agosto 15 del 2001



14 mil localidades del país en los próximos cinco años, lo cual representaría un aumento de entre el 30 y 40 por ciento de dichos servicios. El propósito es que las comunidades más apartadas puedan contar con un entronque mínimo de dos megabits que les facilite el acceso a cuatro puertos: uno para gobierno, otro para salud, otro para educación y otro para comercio.

5. Esta conectividad se dará en condiciones exactamente iguales a las que tendría una población o habitante de cualquier parte del mundo. Entramos a una globalización impresionante, de la noche a la mañana, y las poblaciones marginadas podrán hacer uso paulatino de esta tecnología, en beneficio propio y de su comunidad.

6. La Secretaría de Comunicaciones y Transportes ya modificó las especificaciones para la construcción de carreteras, con el fin de que éstas tengan ductos para cables de fibra óptica y otros sistemas.

7. El e-Business se ha extendido globalmente como el intercambio de bienes y servicios, y este manejo electrónico ha abierto una enorme cantidad de posibilidades. En el momento en que exista esa mega red, seguramente existirán más posibilidades de negocios para las empresas.

8. El proyecto e-MÉXICO se propone revisar los aspectos legales y jurídicos relativos a la Internet para fortalecer la seguridad y privacidad de los usuarios.

9. Para el desarrollo del plan, el Gobierno Federal ha consultado a importantes firmas como IBM, Hewlett Packard, Microsoft, Teléfonos de México, Ericsson, Nortel Networks, Cisco Systems, Nextel Communications y Pricewaterhouse Coopers. Integran un primer grupo de trabajo del sistema e-MÉXICO representantes de las empresas Axtel, Alestra, Unefon, Pegaso, Iusacell, Telcel, Avantel, Bestel y Telmex, así como funcionarios de la Secretaría de Gobernación y del Sector Comunicaciones y Transportes.

10. México cuenta en promedio con cinco computadoras por cada cien habitantes, y el Internet es usado sólo por 1.7 millones de los 97 millones de habitantes en nuestro país. A la fecha de publicación de este artículo existen 72,742 dominios registrados en México (.mx), de los cuales un 92% son comerciales (.com.mx), 1,5% son de dependencias gubernamentales (.gob.mx), 1% de proveedores de Internet (.net.mx), 1.5% sector educación (.edu.mx) y un 4% a diversas organizaciones (.org.mx).

Por otro lado, la segunda vertiente de este proyecto de tecnología inalámbrica de tercera generación contempla la reducción significativa de costos de conectividad a Internet, en nuestro caso, a través de EVDO, permitiendo que las escuelas ubicadas zonas marginadas puedan tener acceso a la Banda Ancha y por lo tanto a este tipo de tecnologías de la información.





## **2) Aspecto Económico**

Otro aspecto importante, relacionado al anterior, donde el proyecto tiene impacto, es el económico. Como lo declaró Rafael Rangel, el Rector del Tecnológico de Monterrey para el periódico la voz de Michoacán “Para enfrentar fenómenos como la migración y el desempleo se requiere del impulso en el uso de nuevas tecnológicas a fin de que la mayoría pueda acceder a la educación en todos los sectores”<sup>8</sup>. La cuestión de que esta brecha tecnológica, cada vez sea más amplia tiene que ver básicamente con el tema económico y el retraso que esto implica en el mercado.

Indudablemente, el proyecto de Internet por telefonía rural que presento en esta tesis intenta contrarrestar el problema de la rentabilidad casi nula que encuentra otro tipo de tecnologías para este mercado de consumo. “Pensemos que en estas regiones sólo el 3% de los habitantes tiene banda ancha en los hogares y sólo un 15% computadoras personales. Esto debido a que por un lado se tiene, la incapacidad económica que tiene el usuario de poder adquirir las nuevas tecnologías, pero por otro el lado la falta de una cultura y una educación que encamine el consumo de la tecnología hacia una valoración, que sea vista como una solución a muchos problemas y no sólo como una tendencia del momento.”<sup>9</sup>

El hecho de querer interconectar el mayor número de puntos y regiones en nuestro país, como lo propone e-México, tiene como objetivo tratar de complementar las estrategias de desarrollo económico con el uso de las tecnologías de información. Tal como afirma Judith Mariscal, analista del Centro de Investigación y Docencia Económicas (CIDE). “La implementación de la banda ancha a todos los niveles fomentará las transacciones comerciales, impulsará a la banca electrónica y permitirá a la población tener un mayor nivel de desarrollo, mientras que las empresas y el país podrán ser más competitivos a nivel internacional”<sup>10</sup>.

El crecimiento de las TIC's (tecnología de la información y comunicación) tiene un crecimiento 4 veces mayor que la economía mexicana, al permitirse el incremento en la penetración de la banda ancha se contribuye al crecimiento del país, se convierte en una herramienta para aumentar la competitividad y para combatir la exclusión del mercado a través de capacitación laboral.”<sup>11</sup>

<sup>8</sup> La Voz de Michoacán, *Brecha Tecnológica Propicia Migración*,  
[http://migrantes.michoacan.gob.mx/index.php?option=com\\_content&task=view&id=346&Itemid=278](http://migrantes.michoacan.gob.mx/index.php?option=com_content&task=view&id=346&Itemid=278), 13 de noviembre de 2008

<sup>9</sup> Master Magazine, *La Brecha Tecnológica y América Latina*,  
<http://www.mastermagazine.info/articulo/12252.php>, Octubre de 2007

<sup>10</sup> CNNExpansion.com, *La Banda Ancha impulsa el Desarrollo*,  
<http://www.cnnexpansion.com/tecnologia/2009/09/03/la-banda-ancha-impulsa-al-desarrollo>, 04 de septiembre de 2009

<sup>11</sup> ibidem



### **3) Aspecto Político**

En este último aspecto podríamos hablar de lo que se refiere al acceso a la información pública y la posibilidad de participación ciudadana en el ámbito político del país a través del uso de la red.

En el primer aspecto encontramos que, como ya se mencionó, hoy en día no es suficiente el acceso a las tecnologías de la información y por ende el acceso a la información que puedan proporcionar nuestros gobernantes acerca de las decisiones que toman y que afectan a nuestra comunidad y/o entorno también es escaso.

Georgina Olson, lo dice en su artículo titulado *Sólo 20% escudriña datos del gobierno* publicado en el Excelsior en diciembre del 2008: "Alonso Lujambio Irazábal, titular del Instituto Federal de Acceso a la Información (IFAI) aseguró que, En México hay una brecha tecnológica importante porque sólo 20% de la población tiene acceso a Internet, y por lo tanto, al sistema de solicitudes de información a la administración pública federal"<sup>12</sup>

De igual forma encontramos en la actualidad la existencia de *blogs*<sup>13</sup> con tendencias políticas por toda la red, cuyos principales objetivos son precisamente levantar la voz para expresar lo que no consideramos adecuado y de esta forma crear círculos de personas más participativas en cuestiones políticas.

Finalmente, cabe decir que a pesar de que un proyecto de esta magnitud tiene un costo aproximado de \$10 a \$15 mdd (contemplando el costo del equipo, la instalación, el recurso humano, etc.) y normalmente se busca la recuperación de la inversión a partir de los 5 años de servicio, en mi opinión en este caso, Teléfonos de México, más que buscar la rentabilidad del mismo al mediano plazo, busca cumplir con los requerimientos del gobierno Federal como parte del proyecto E-México para cubrir estas zonas donde su infraestructura cableada no llega. Por lo que este proyecto es parte de las políticas públicas llevadas a cabo por el gobierno del país.

Así concluyo que el impacto del proyecto aquí presentado tiene implicaciones socioeconómicas de peso cuyo breve análisis intentó darse en estas últimas cuartillas. De ahí que nunca debemos de perder de vista que en todo nuestro desarrollo profesional debemos de aplicar tanto la ingeniería y como la técnica al servicio de la patria.

---

<sup>12</sup> Georgina Olson, *Solo 20% escudriña datos del gobierno*  
<http://www.periodistasenlinea.org/modules.php?op=modload&name=News&file=article&sid=10664>, El Excelsior, 3 de diciembre de 2008

<sup>13</sup> Un **blog**, o en español también una bitácora, es un sitio web periódicamente actualizado que recopila cronológicamente textos o artículos de uno o varios autores, apareciendo primero el más reciente, donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente.