# UNIVERSIDAD NACIONAL DE INGENIERÍA

## FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA


# IMPLEMENTACIÓN DEL SERVICIO DE TRANSMISIÓN DE DATOS A TRAVÉS DEL SISTEMA DE TELEFONÍA MOVIL CELULAR EN EMPRESAS CORPORATIVAS"

## INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

## INGENIERO ELECTRÓNICO


## PRESENTADO POR:
## HUGO ALFREDO CHUPA CHACÓN


PROMOCIÓN
1997-I
**LIMA-PERÚ**
**2003**

A Dios por la fuerza espiritual.

A mis padres Nicanor y Viviana por su apoyo moral.

A mi hermana Laura por su constante estímulo y apoyo incondicional.

A mi querido hijo Rigel y esposa Marivel razones del éxito.

# IMPLEMENTACIÓN DEL SERVICIO DE TRANSMISIÓN DE DATOS A TRAVÉS DEL SISTEMA DE TELEFONÍA MÓVIL CELULAR EN EMPRESAS CORPORATIVAS

# SUMARIO

El presente Informe de suficiencia da a conocer los mecanismos de transmisión de datos a través de la red de telefonía celular que se están empleando en la actualidad, mostrando una gran variedad de posibilidades a desarrollar en los sistemas de información, ya que es posible acceder a la información que uno necesita desde cualquier lugar, a cualquier hora o en cualquier momento, siempre garantizando los niveles de seguridad que esta información amerita tener, es decir no es necesario encontrarse en las oficinas de nuestras empresas para tener la información que necesitamos

Las empresas en general pueden emplear el medio inalámbrico celular para poder conectarse a través de los teléfonos celulares, PC portátiles o Dispositivos de asistencia personal a la red interna de sus empresas, y así poder acceder o dejar información en tiempo real.

# ÍNDICE

**CAPÍTULO IV**



**CAPÍTULO V**

# PRÓLOGO

Las nuevas tecnologías y el crecimiento de Internet desde 1995 como medio de comunicación ha sido sencillamente espectacular. Internet evolucionó hasta convertirse en el canal de negocios potencialmente más poderoso que jamás haya existido, en este sentido los sistemas de Telefonía Celular abocan sus esfuerzos en brindar soluciones de datos sobres su infraestructura llegando a trasmitir datos a velocidades no pensadas, actualmente sé esta transmitiendo datos, videos y multimedia sobre infraestructura Celular en el Japón, conocido como 3G (Tercera Generación), nuestro país no ha llegado aún a alcanzar dichas velocidades de transmisión de datos pero se encuentra en una etapa intermedia, 2.5G permite a los operadores celulares poder alcanzar velocidad nada despreciables para soluciones móviles. En tal sentido y gracias a la experiencia laboral obtenida en mis 6 años trabajando en diferentes empresas, primero en Electrodata S.A. como especialista en redes LAN/WAN y luego en Telefonica Móviles como especialista en Sistemas de Seguridad de Redes de Datos y Consultor en Soluciones Inalámbricas, me permito presentar este informe de Suficiencia, donde se detalla los fundamentos teóricos y describe los tipos de soluciones a las cuales esta orientada este tipo de tecnología, tales como fuerza de ventas de las empresas, empresas de transporte, empresas de vigilancia, usuarios que viajan constantemente etc.

La evolución de la Telefonía Celular e Internet ha sido verdaderamente notable, inclusive comparándola con otros saltos tecnológicos y de provisión de información.

El impacto de la implantación de este sistema en las organizaciones previsoras ha sido nada menos que espectacular, teniendo como modelo básico de estrategia competitiva, basada en los principios de bajos costos, grandes volúmenes y amplios servicios que se pueden lograr.

El desarrollo de este nuevo modelo de servicios es muy amplio, infraestructura, tecnología, servicios y mercados son un todo que en conjunto resultan siendo el arma potencial de competitividad.

El presente trabajo de investigación se limita a la formulación y sustentación del proyecto. La ingeniería del proyecto estará soportada sobre una tecnología de punta existente en el país, ésta tecnología es conocida como PACKET DATA, ideal para el nuevo modelo. Finalmente los conocimientos de formulación y evaluación de proyectos nos darán la fortaleza necesaria y la relevancia para la toma de decisiones a futuro sobre la implementación de sistemas similares.

# CAPÍTULO I
# INTRODUCCIÓN

## 1.1 Generalidades

Todos somos conscientes que los nuevos avances tecnológicos aplicados en los sistemas de Información y telecomunicaciones, constituyen uno de los acontecimientos más importantes del presente siglo como por ejemplo el desarrollo de la red de redes llamado Internet. En los años 70s y 80s, las redes consideradas como importantes y grandes eran las redes privadas de negocios como las de los bancos, cadenas de supermercados, empresas de tecnología como la red mundial de IBM, y la gran mayoría usaba protocolos propietarios principalmente como el SNA de IBM, y la arquitectura de redes Burroughs (Arquitectura de red Burroughs, BNA) de Unisys entre otros.

Así mismo las tecnologías inalámbricas están teniendo mucho auge y desarrollo en estos últimos años, una de las que ha tenido un gran desarrollo ha sido la telefonía celular, desde sus inicios a finales de los 70s ha revolucionado enormemente las actividades que realizamos diariamente. Los teléfonos celulares se han convertido en una herramienta primordial para la gente común y de negocios, las hace sentir más segura y las hace más productivas. A pesar que la telefonía celular fue concebida para la voz únicamente, debido a las limitaciones tecnológicas de esa época, la tecnología celular de hoy en día es capaz de brindar otro tipo de servicios tales como

datos, audio y video con algunas limitaciones, pero la telefonía inalámbrica del mañana hará posible aplicaciones que requieran un mayor consumo de ancho banda.

Así también en los 90s la telefonía celular comenzó al crecimiento tecnológico en la telefonía celular tiene como se integra a la transmisión de datos es así como hoy en día nos encontramos experimentando la Tercera generación de la telefonía celular en el mundo

## 1.2 Antecedentes

### 1.2.1 Breve historia de la Telefonía Celular

Martín Cooper fue el pionero en esta tecnología, a él se le considera como "el padre de la telefonía celular" al introducir el primer radioteléfono en 1973 en los Estados Unidos mientras trabajaba para Motorola; pero no fue hasta 1979 en que aparece el primer sistema comercial en Tokio Japón por la compañía NTT (Nippon Telegraph & Telephone Corp.)

En 1981 en los países Nórdicos se introduce un sistema celular similar a AMPS (Sistema Avanzado de Teléfonos Móviles). Por otro lado, en los Estados Unidos gracias a que la entidad reguladora de ese país adopta reglas para la creación de un servicio comercial de telefonía celular, en octubre de 1983 se pone en operación el primer sistema comercial en la ciudad de Chicago. A partir de entonces en varios países se diseminó la telefonía celular como una alternativa a la telefonía convencional alámbrica. La tecnología inalámbrica tuvo gran aceptación, por lo que a los pocos años de implantarse se empezó a saturar el servicio, por lo que hubo la imperiosa necesidad de desarrollar e implementar otras formas de acceso múltiple al canal y transformar los sistemas analógicos a digitales para darle cabida a más

usuarios. Para separar una etapa de la otra, a la telefonía celular se ha categorizado por generaciones. A continuación se describen cada una de ellas.

1.2.2 Las generaciones de la Telefonía Inalámbrica

La primer generación 1G

La 1G de la telefonía móvil hizo su aparición en 1979, se caracterizó por ser analógica y estrictamente para voz. La calidad de los enlaces de voz era muy baja, baja velocidad [2400 bauds], la transferencia entre celdas era muy imprecisa, tenían baja capacidad [basadas en FDMA (Acceso Múltiple por División de Frecuencia) y la seguridad no existía. La tecnología predominante de esta generación es AMPS (Sistema Avanzado de Teléfono Móvil).

La segunda generación 2G

La 2G arribó hasta 1990 y a diferencia de la primera se caracterizó por ser digital. El sistema 2G utiliza protocolos de codificación más sofisticados y son los sistemas de telefonía celular usados en la actualidad. Las tecnologías predominantes son: GSM (Comunicación Móvil para Sistema Global); IS-136 (conocido también como TIA/EIA-136 o ANSI-136) y CDMA (Acceso Múltiple por División de Códigos).

Los protocolos empleados en los sistemas 2G soportan velocidades de información mas altas para voz pero limitados en comunicaciones de datos. Se pueden ofrecer servicios auxiliares tales como datos, fax y SMS (Servicio de Mensajería Corta). La mayoría de los protocolos de 2G ofrecen diferentes niveles de encriptación. En los Estados Unidos y otros países se le conoce a 2G como PCS (Servicio de Comunicación Personal).

La generación 2.5G:

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

La generación 2.5G ofrece características extendidas para ofrecer capacidades adicionales que los sistemas 2G tales como GPRS (Sistema de Radio General Paquetes), HSCSD (Datos Conmutados por Circuitos de Alta Velocidad), EDGE (Velocidad de Datos Mejorados para Evolución Global), IS-136B, IS-95B, entre otros. Mientras que Japón fue directo de 2G a 3G también en el 2002

La tercer generación 3G

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

Los sistemas 3G alcanzaran velocidades de hasta 384 Kbps, permitiendo una movilidad total a usuarios viajando a 120 kilómetros por hora en ambientes exteriores y alcanzará una velocidad máxima de 2 Mbps permitiendo una movilidad limitada a usuarios caminando a menos de 10 kilómetros por hora en ambientes estacionarios de corto alcance o en interiores. Entre las tecnologías contendientes de la tercera generación se encuentran UMTS (Servicio Telefónico Móvil Universal), cdma2000, IMT-2000, ARIB[3GPP], UWC-136, entre otras.

El impulso de los estándares de la 3G está siendo apoyando por la ITU (Unión Internacional de Telecomunicaciones) y a este esfuerzo se le conoce como IMT-2000 (Teléfono Móvil Internacional).

La cuarta generación 4G

La cuarta generación es un proyecto a largo plazo que será 50 veces más rápida en velocidad que la tercer generación. Se planean hacer pruebas de esta tecnología hasta el 2005 y se espera que se empiecen a comercializar la mayoría de los servicios hasta el 2010.

1.2.3 Estatus actual de la Telefonía Móvil

Existen hoy en día tres tecnologías de telefonía celular predominantes en el mundo: IS-136, IS-95 y GSM.

IS-136 (Estándar Ínterin 136) fue la primer tecnología digital de telefonía celular (D-AMPS, versión la versión digital de AMPS) desarrollada en Estados Unidos, IS-136 esta basada en TDMA (Acceso Múltiple por División de Tiempo), una técnica de acceso múltiple la cual divide los canales de radio en tres ranuras de tiempo, cada usuario recibe en una ranura diferente. Este método permite a tres usuarios en cada canal de radio comunicarse sin interferirse uno con el otro. D-AMPS (IS-54) es utilizado principalmente en Norteamérica, Latinoamérica, Australia, partes de Rusia y Asia.

Por otro lado, CDMA, tecnología desarrollada por Qualcomm, utiliza la tecnología de espectro disperso en la cual muchos usuarios comparten simultáneamente el mismo canal pero cada uno con diferente código. Lo anterior permite una mayor capacidad en usuarios por celda. A CDMA de segunda generación se le conoce como cdmaOne. Hasta diciembre del 2000 existen más de 27 millones de usuarios en más de 35 países alrededor del mundo utilizando cdmaOne.

GSM es tecnología celular desarrollada en Europa considerada como la tecnología celular más madura, con mas de 200 millones de usuarios en mas de 100 países

alrededor del mundo. GSM es un servicio de voz y datos basado en conmutación de circuitos de alta velocidad la cual combina hasta 4 ranuras de tiempo en cada canal de radio

# CAPÍTULO II
# MARCO GENERAL

## 2.1 Propósito del proyecto

El propósito principal de este documento es formular evaluar y analizar el proyecto de "Implementación de una red de transmisión de datos a través del Sistema de Telefonía Celular para empresas Corporativas" para la toma de decisiones.

La ingeniería del proyecto estará soportada sobre una Red de Telefonía Celular CDMA y redes de datos LAN y WAN TCP/IP, el cual permitirá formular nuevos modelos de comunicación para usuarios que por su naturaleza de trabajo se encuentran fuera de las oficinas de la empresa, o para aquellas necesidades de comunicación entre nodos remotos donde los enlaces de tierra no pueden ser posibles por el alto costo que implica o la limitación del área de su cobertura

## 2.2 Justificación

Nuestro desafío por consiguiente, es dotar a las pequeñas , medianas y grandes empresas del país, los medios, herramientas e instrumentos basados en nuevas tecnologías mediante el acceso inalámbrico celular a la información almacenadas en sus empresas y evitar se siga perdiendo tiempo para el desplazamiento hacia la oficina, coordinar con personal de la oficina para obtener información o para que realicen su gestión. La trasmisión de datos en línea es sin duda una herramienta de alta productividad hoy en día y permite al usuario tres grandes ventajas:

- Ahorro en tiempo

- Eficiencia del personal
- Mejoras de procesos

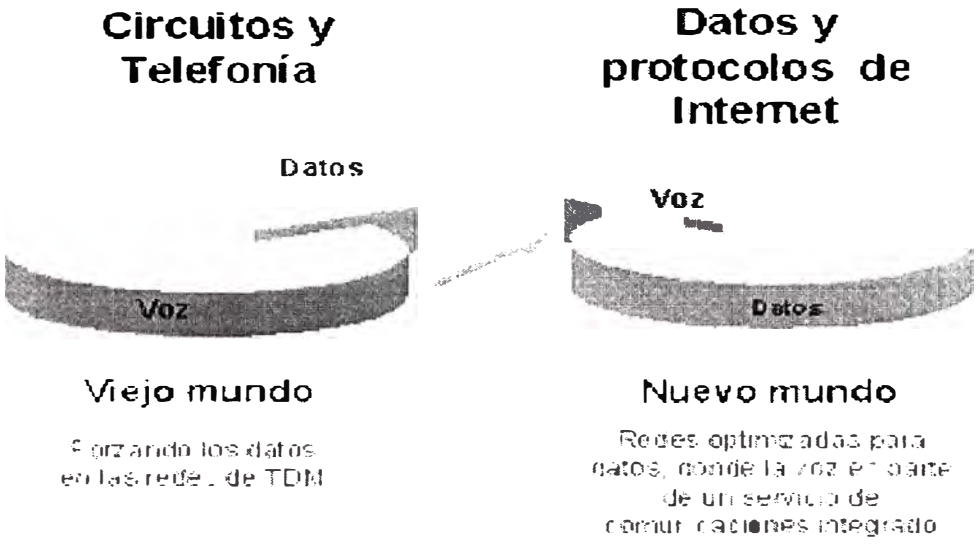



Figura 2.1. Migración de la comunicación de VOZ a DATOS

En la figura 2.1 se representa como en el pasado la concentración de información era referida a voz, actualmente este escenario esta cambiando hacia un nuevo proceso de manejo y fluidez de información de datos y protocolos de Internet.

Uno de los beneficios más importantes es la adaptación de los flujos de tráfico a los recursos físicos de la red. Con esto se puede equilibrar la forma óptima de utilizar los recursos, de manera que no haya algunos que estén sobre utilizados, con cuellos de botella, o subutilizados.

## 2.3 Mercado de servicios

Los servicios objetivos para este nuevo modelo "Implementación del servicio de transmisión de datos a través del Sistema de Telefonía Móvil Celular para empresas

están orientadas a la pequeña empresa, mediana empresa y corporaciones los cuales aun se encuentran en pleno proceso de desarrollo hacia la nueva cultura llamada Internet.

El mercado objetivo para el proyecto, esta dirigido a todas las empresas que deseen ahorro de tiempo, eficiencia del personal y mejora de procesos

## 2.4 Estudio del Mercado

A continuación se presentan las operadoras con los servicios de transmisión de datos que se ofrecen en el mercado de comunicaciones inalámbricas del país.

**Nextel:** Dentro de los servicios de transmisión de datos se puede enumerar los siguientes servicios:

Servicios WAP: Sobre las cuales están desarrollando aplicaciones a una velocidad de 9600 Kbps. Ejemplo Toma de pedidos de Filtros Lys publicado en PC World.

Transmisión de datos móviles: Conexión de terminales a PDAs, laptops, etc. La velocidad que ellos indican alcanzar es 19200 bps.

Su sistema WAP trabaja en WML 4.1 y sus terminales permiten manejar Java. Esto les da una ventaja sobre nuestra plataforma WAP. Nuestra ventaja en velocidad no es vista por el cliente como determinante, sobre todo si hablamos de soluciones WAP. Nextel es el operador que ofrece una opción equivalente a cada uno de nuestros servicios en data.

**TIM:** están ofreciendo el servicio Tim Data: uso del telefono TIM conectado a PC, laptop, PDA, etc. Ellos indican que pueden manejar 9,6 kbps o 14,4 kbps. vía circuitos en ambos casos.

**BellSouth:**

No hay ninguna mención por parte de los clientes con respecto a soluciones de transmisión de Datos de esta operadora, ellos están enfocando sus esfuerzos en la transmisión de mensajería.

**Telefónica:**

En la actualidad Operador Celular brinda servicios de transmisión de datos en WAP y transmisión de circuitos a una velocidad de 14400 bps, este nuevo servicio permitirá posicionarnos a la vanguardia en transmisión de datos, ofreciendo conexiones a velocidades que pueden alcanzar 64 Kbps, tarificación por transmisión y recepción de datos, el tiempo de conexión no importa.

# CAPÍTULO III
# OBJETO Y ALCANCE DEL ESTUDIO

## 3.1 Objetivos

Los objetivos principales considerados en el proyecto Implementación del Servicio de Transmisión de datos a través del sistema de Telefonía Móvil Celular para empresas Corporativas son:

- Asegurar resultados eficaces en la toma de decisiones para la implementación de sistemas de transmisión de datos empleando la infraestructura de la Red Celular CDMA garantizando la privacidad e integridad de los sistemas de comunicaciones y los datos.
- Implementar una red con acceso remoto sobre tecnología de Telefonía Celular CDMA.
- Contribuir al conocimiento y desarrollo de la cultura informática en salvaguarda de los sistemas y datos activos importante para las empresas en general.
- Examinar los nuevos medios de comunicación, sistemas y tecnologías para la optimización de los procesos, generar un verdadero cambio de actitud y aptitud en la Alta Dirección y en el nivel Gerencial de las entidades financieras hacia el resguardo de personas y bienes.

## 3.2 Alcance del proyecto

El desarrollo del proyecto alcanza a Directores, Gerentes de sistemas y telecomunicaciones, administradores de redes, áreas de soporte técnico y desarrollo, consultores, profesionales técnicos y profesionales en redes y telecomunicaciones que contribuyen en la toma de decisiones para la implementación de nuevas tecnologías dentro de la empresa en la que laboran.

### 3.3 Ingeniería del Proyecto

El desarrollo de la ingeniería del proyecto consistirá en diseñar un Sistema de Comunicación para satisfacer las siguientes necesidades de una EMPRESA

- Brindar conexión para 80 usuarios móviles con una cobertura a nivel nacional a una velocidad superior a 14 kbps:
- Permitir que los empleados de la empresa puedan realizar consultas a un servidor de aplicaciones para obtener información sobre el stock de productos, lista de precios, ofertas y promociones de productos, línea de crédito del cliente, histórico de pedidos realizados por clientes etc., para los vendedores
- Conexión al servidor de correo corporativo para enviar y recibir correos para los vendedores y Gerentes
- Operación y mantenimiento de los enrrutadores y plataformas Unix para los usuarios del área técnica
- Consultas rápidas vía WAP para los vendedores
- Control y reporte diario de vigilantes de seguridad

# CAPÍTULO IV
# TECNOLOGÍA DE SOPORTE

## 4.1 Red de Datos TCP/IP

### 4.1.1 Arquitectura del modelo TCP/IP

a. Definición

Se llama TCP/IP (TCP: Protocolo de Control Transmisión, e IP: Protocolo Internet), es un protocolo de transporte de comunicaciones; esto es, un conjunto de reglas, convenciones y comandos para que las computadoras y los programas, no personas, puedan comunicarse desde cualquier parte del mundo, a casi la velocidad de la luz. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware, proporcionando una abstracción total del medio. Se compone de dos protocolos interrelacionados:

El protocolo TCP: Funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.

El protocolo IP: Funciona en el nivel de red del modelo OSI, que nos permite encaminar los datos hacia otros equipos.

b. Características de TCP/IP

Las características del protocolo son:

- Los programas de aplicación no tienen conocimiento del hardware que se utilizara para realizar la comunicación.

o La comunicación no esta orientada a la conexión de dos equipos, eso quiere decir que cada paquete de datos es independiente, y puede viajar por caminos diferentes entre dos equipos.

o La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre que tipo de red trabajan.

o El uso de la red no impone ninguna topología en especial.

c. Niveles del modelo TCP/IP

El modelo TCP/IP está basado en la de conmutación de paquetes (packet switched), y tiene cuatro niveles: el nivel de aplicación, el nivel de transporte, el nivel de Internet y el nivel de red. Es importante observar que algunas de los niveles del modelo TCP/IP poseen el mismo nombre que los niveles del modelo OSI, aunque no se corresponden exactamente unas con otras, por lo que no deben confundirse. Ver Fig.4.1.

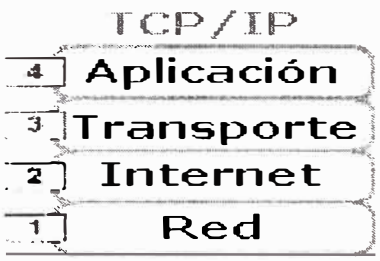



Fig. 4.1 Niveles del modelo TCP/IP

Nivel de aplicación: En este nivel maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una solo nivel y da por sentado que estos datos están correctamente empaquetados para la siguiente capa. Se incluyen

protocolos destinados a proporcionar servicios tales como correo electrónico (smtp), transferencia de ficheros (ftp), conexión remota (telnet) y otros como http.

Nivel de transporte: Permite que niveles pares emisor y receptor puedan conversar. El nivel de transporte se refiere a la calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Utiliza los servicios del nivel de red para proveer un servicio eficiente y confiable a los procesos del nivel de aplicación. En este nivel se produce la segmentación de los datos producidos en el nivel de Aplicación en unidades de menor tamaño, denominadas paquetes o datagramas (un datagrama es un conjunto de datos que se envía como un mensaje independiente), El nivel de transporte no se preocupa de la ruta que van a seguir los datos para llegar a su destino final. simplemente considera que la comunicación entre ambos extremos está ya establecida y la utiliza.

Nivel de Internet o de red: El propósito del nivel de Internet es enviar paquetes origen desde cualquier red y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí. En este nivel se produce la determinación de la mejor ruta y la conmutación de paquetes. Durante su transmisión los paquetes pueden ser divididos en fragmentos, que se montan de nuevo en el destino. Para poder enrrutar los datagramas de la capa de Transporte, éstos de encapsulan en unidades independientes, en las que se incorporan diferentes datos necesarios para el envío, como dirección de origen del datagrama, dirección de destino, longitud del mismo.

Nivel de acceso a la red: Uno de los principales elementos que maneja este nivel es el de las direcciones físicas, números únicos de 6 bytes asignados a cada tarjeta de red, y que son el medio principal de localización de un host (cualquier computadora

conectado a Internet, capaz de compartir información con otra computadora) dentro de una red. Cada tarjeta tiene un número identificador, cuyos 3 primeros bytes son asignados por el fabricante de la misma, mientras que los otros 3 se asignan de forma especial. Cuando un host debe enviar un paquete a otro de su red busca a éste mediante su número de tarjeta de red (dirección física).

d. Comparación de modelos OSI y TCP/IP

Si comparamos el modelo TCP/IP y OSI. Ver Fig.4.2, observaremos que ambos presentan las siguientes Analogías y diferencias:

Analogía: Se dividen en niveles, tienen niveles de aplicación (aunque incluyen servicios muy distintos), La tecnología es de conmutación de paquetes (no de conmutación de circuitos).

Diferencias: OSI distingue de forma clara los servicios (lo que un nivel hace), las interfaces (como se pueden acceder a los servicios) y los protocolos (implementación de los servicios). TCP/IP no lo hace así, no dejando de forma clara esta separación. OSI fue definido antes de implementar los protocolos, por lo que algunas funcionalidades necesarias fallan o no existen. En cambio, TCP/IP se creó después que los protocolos, por lo que se amolda a ellos perfectamente. TCP/IP combina las funciones del nivel de presentación y de sesión en el nivel de aplicación. TCP/IP combina el nivel de enlace de datos y el físico del modelo OSI en una solo nivel.

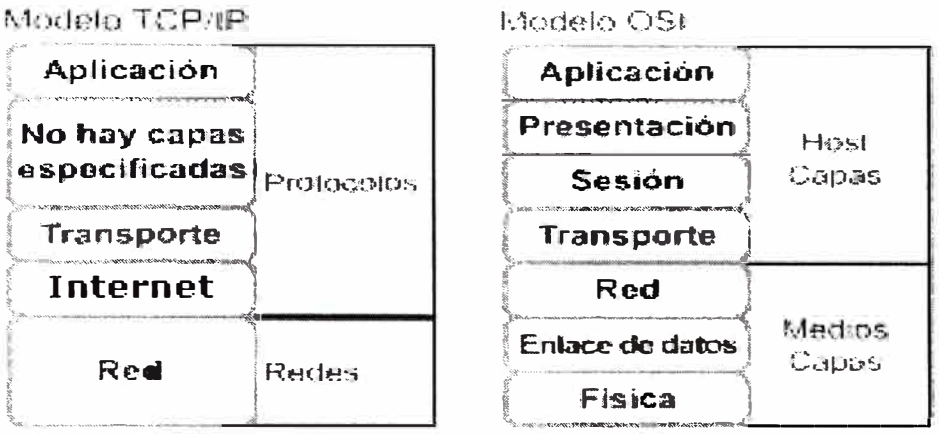



Fig.4.2 Comparación de Modelos TCP/IP - OSI

4.1.2 Encapsulamiento

Si el emisor desea enviar datos al receptor, en primer término los datos que se deben enviar se deben colocar en paquetes que se puedan administrar y rastrear a través de un proceso denominado encapsulamiento. Los tres niveles superiores (aplicación, presentación y sesión) preparan los datos para su transmisión definiendo un formato común para la transmisión. Una vez pasados a formato común, el encapsulamiento, rodea los datos con la información de protocolo necesaria antes de que se una al transito de la red. Los tres niveles inferiores (red, enlace de datos, física) del modelo OSI son los niveles principales de transporte de los datos a través de una red interna o de Internet. A medida que los datos se desplazan a través de los niveles del modelo OSI, reciben encabezados(agregar la información correspondiente a la dirección), información final y otros tipos de información. Una vez que se envían los datos desde el origen, viajan a través del nivel de aplicación directo hacia los otro niveles. El empaquetamiento y el flujo de los datos que se intercambian experimentan cambios a medida que las redes ofrecen sus servicios a los usuarios finales. Como muestra la figura 4.2, las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos:

a. Definir los datos (nivel de Presentación): Cuando un usuario (emisor) envía un mensaje de correo electrónico, sus caracteres alfanuméricos se convierten en datos que pueden recorrer el conjunto de redes interconectadas.
b. Empaquetar los datos para ser transportados de extremo a extremo (nivel de Transporte): Se dividen los datos en unidades de un tamaño que se pueda administrar, llamados segmentos, y se les asignan números de secuencia para asegurarse que los computadores receptores vuelvan a unir los datos en el orden correcto. Luego los empaqueta para ser transportados por el conjunto de redes interconectadas. Al utilizar segmentos, la función de transporte asegura que el emisor y receptor del sistema de correo electrónico se puedan comunicar de forma confiable.

c. Agregar la dirección de red al encabezado (nivel de Red): El siguiente proceso se produce en el nivel de red, que encapsula el segmento creando un paquete o datagrama, agregándole una dirección de red destino y origen, por lo general IP. Con esto, los datos se colocan en un paquete que contiene el encabezado de red con las direcciones lógicas de origen y destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.
d. Agregar la dirección local al encabezado de enlace de datos (nivel Enlace de datos): En el nivel de enlace de datos continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama la dirección local (control de acceso al medio de la tarjeta de red, única para cada tarjeta) origen y destino. Luego, el nivel de enlace de datos transmite los bits binarios de la trama a través

de los medios del nivel físico. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de la red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.

e. Transmitir el tren de bits creado. (nivel Físico): Por último, el tren de bits originado se transmite a la red a través de los medios físicos (cableado, fibra óptica, etc.), Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el conjunto de redes interconectadas.

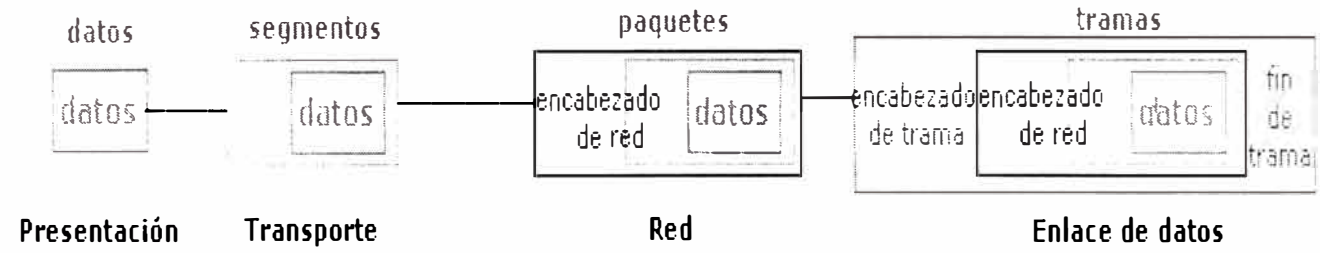



Fig.4.2 Encapsulamiento de datos

4.1.3 Servicios de seguridad

Para hacer frente a las amenazas a la seguridad de los datos se definen los servicios para proteger los sistemas de proceso de datos y de transferencia de información de las entidades financieras y bancarias. Estos servicios hacen uso de varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

a. Autenticación: Requiere de una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Por ejemplo la autenticidad se consigue

mediante el uso de los certificados y firmas digitales en las transacciones electrónicas.

b. Confidencialidad: Requiere que la información sea accesible únicamente por las entidades autorizadas. Por ejemplo la confidencialidad se consigue en las transacciones electrónicas con el uso de la criptografía. Se distinguen dos tipos de confidencialidad:

b.1 Confidencialidad de datos: El cual está relacionada con el almacenamiento de los datos.

b.2 Confidencialidad del flujo de tráfico: Se encuentra relacionada con el proceso de transmisión de datos. Se dan tres casos diferentes de confidencialidad de flujo: confidencialidad de un servicio orientado a la conexión, confidencialidad de un servicio no orientado a la conexión y servicio de confidencialidad de campo selectivo.

c. Integridad de datos: Asegura que los datos que enviamos lleguen íntegros, sin modificaciones, a su destino final. Por ejemplo la integridad de datos se consigue combinando criptografía, funciones hash y firmas digitales.

d. No repudio: Debemos estar seguros de que una vez enviado un mensaje con datos importantes o sensibles el destinatario de los mismos no pueda negar el haberlos recibido. Por ejemplo en una compra on-line debe garantizarse que una vez finalizada la misma ninguna de las partes (emisor y receptor) que intervienen pueda negar haber participado en ella. El no repudio se consigue mediante los certificados y la firma digital.

4.1.4 Políticas de seguridad

a. Definición

Una política de seguridad es un conjunto de normas, procedimientos y prácticas que regulan como las entidades financieras manejan, protegen y distribuyen los datos.

b. Características de la Políticas de Seguridad

- Debe ser simple y entendible.
- Debe estar siempre disponible.
- Debe ser practicable y desarrollable.
- Se debe hacer cumplir.
- Debe ser estructurada.
- Se establece como una guía.
- Debe ser cambiante con la evolución tecnológica.
- Una política debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas como una unidad corporativa.

c. Elaboración de la Política de seguridad

Para la elaboración de la política de seguridad en las entidades financieras, el primer procedimiento es hacer una relación de los aspectos sensibles dentro de la organización, tanto físicos (equipos computo, comunicaciones, etc.), Como no materiales (aplicaciones, software, bases de datos, etc.), una vez realizada esta lista de puntos sensibles a proteger, se pondera cada uno de ellos con un peso específico, y se calcula la posibilidad de que sea vulnerado, ya sea por ataques intencionados o por causas meramente accidentales. Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También es importante definir los usuarios con accesos a los recursos de acuerdo a las funciones a

realizar. Las tres preguntas fundamentales que debemos responder para desarrollar cualquier política de seguridad son:

¿Qué queremos proteger?

¿Contra quién?

¿Cómo?

Respondiendo a estas preguntas tenemos: Se deberían proteger todos los elementos de la red interna, incluyendo hardware, software, datos, etc., de cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir. Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros. La respuesta a la tercera pregunta requiere unas soluciones más dinámicas y cambiantes en lo que se refiere a la vigencia de dicha política de seguridad, podemos aplicar el modelo de que: Todo lo que no se prohíbe expresamente está permitido, todo lo que no se permite expresamente está prohibido y realizando un análisis de riesgo clasificando por el nivel de serevidad en la cual involucra hacer decisiones costo-beneficio.

No existe un único mecanismo capaz de proveer todos los servicios de seguridad, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

a. Intercambio de autenticación: Corrobora que un usuario, ya sea emisor o receptor de la información, es la deseado, por ejemplo, el usuario UNI1 envía un número

aleatorio cifrado con la llave pública del usuario UNI2, UNI2 lo descifra con su llave privada y se lo reenvía a UNI1, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.

b. Cifrado: El cifrado de datos se puede hacerse utilizando sistemas criptográficos simétricos o asimétricos y se puede aplicar desde el emisor al receptor o individualmente a cada enlace del sistema de comunicaciones. Soporta el servicio de confidencialidad de datos al tiempo que actúa como complemento de otros mecanismos de seguridad.

c. Integridad de datos: Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

d. Firma digital: Este mecanismo implica el cifrado, por medio de la llave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos. Este mensaje se procesa en el receptor, para verificar su integridad, esta relacionado con el servicio de no repudio.

e. Control de acceso: La función es de asegurar si el emisor está autorizado a usar los recursos del sistema o a la red comunicación requeridos. Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al

tiempo que puede informar del incidente, con el propósito de generar un registro y/o alarma.

f. Unicidad: Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

g. Tráfico de relleno: Consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.

## 4.2 Telefonía Celular

### 4.2.1 Elementos Básicos de la Telefonía Celular

El término celular se debe a que la cobertura radioeléctrica de una zona geográfica completa se realiza cubriendo pequeñas regiones llamadas células. En cada una de estas células existe una Estación Radio Base (BTS) que controla el tráfico de los teléfonos móviles que se desplazan en la zona correspondientes . A su vez estas estaciones están enlazadas con el centro de conmutación de Servicios Móviles (Mobile Switched Center, MSC) y este a su vez esta conectado a la Red de Telefonía Publica Fija (Public Switched Telecommunications Networks, PSTN). El Centro de Conmutación de Servicios Móviles a su vez se divide en un conmutador telefónico (PABX ) y en el Subsistema de Telefonía Móvil (MTS)

Dependiendo del tipo de antena de transmisión empleada en la estación base, se puede cubrir una o más áreas de la estación base. Estas áreas reciben el nombre de células .

Existen dos tipos de células las omnidireccionales y sectoriales:

Células Omnidireccionales : Esta se produce cuando una estación base esta equipada con una antena omnidireccional transmitiendo igualmente en todas las direcciones y se forma un área de forma circular, con la estación base en el centro de la célula. Para representar una célula usualmente se utiliza un hexágono en forma teórica, pero en la realizar el área de la cobertura es circular.

Célula Sectorial : Para formar este tipo de célula la estación base esta equipada con tres antenas direccionales, cada una cubriendo una célula sectorial de 120 grados. En cada una de las estaciones base, algunas unidades de canal están conectadas a una antena cubriendo una célula sectorial, otras unidades de canal están conectadas a la segunda antena cubriendo una segunda célula y el resto a una antena para tener una tercera célula. Por tanto la estación base controla a tres células sectoriales.

La estación base está conectada a un Centro de Conmutación de Servicios Móviles por medio de circuitos de enlace punto a punto. La estación base maneja la radiocomunicación con los teléfonos celulares o estaciones móviles y supervisa la calidad de la radio transmisión durante la llamada de voz o datos.

Una de las principales características de los sistemas celulares es el reuso de frecuencias, que consiste en comunicar al teléfono celular con la estación base por medio de un canal telefónico con frecuencia disponible en ese momento. El teléfono celular no tiene una frecuencia fija de enlace. Esta técnica permite hacer un eficiente uso del espectro electromagnético disponible, así como atender a mas usuarios en un número determinado de canales de radio. Este reuso de frecuencias es posible utilizando canales de la misma frecuencia en varias celdas que no son adyacentes, evitando así alguna interferencia.

Todos los teléfonos celulares pueden utilizar un canal de la estación base la cual detectará su desplazamiento en el área asignándole una nueva frecuencia si cruza la frontera de la célula en que se encontraba y pasa a otra célula diferente, este cambio es imperceptible para el usuario debido a que su teléfono continua funcionando normalmente.

4.2.2 Arquitectura Básica del Sistema CDMA

¿Por qué CDMA?

Los sistemas celulares analógicos tales como TACS, AMPS, NAMP etc., alcanzaron rápidamente su punto de saturación. Aunque en teoría los sistemas analógicos pueden expandirse sin límites introduciendo micro celdas y computadores más potente, el costo de esta expansión es excesiva. Un nuevo sistema es requerido el cual proveerá mas capacidad que estos sistemas analógicos . El CDMA provee hasta 9 veces la capacidad de los sistemas AMPS (según cálculos de Motorola que tienden a ser conservadores)

El CDMA provee el nivel mas alto de seguridad de cualquier sistema analógico o digital actualmente en el mercado. Codificando la señal a ser transmitida con secuencias digitales que son extremadamente difíciles (si no imposible) de reproducir, se consigue un sistema a prueba de fraude. Esto es muy atractivo para los operadores de sistemas celulares, ya que el fraude es muy común en la tecnología celular analógica.

El CDMA actualmente es el único sistema que provee make-before-break (cerrar antes de abrir) handoffs. Esto significa que la señal no es interrumpida mientras el móvil empieza a funcionar con otra estación base. La calidad de la voz es mejorada en CDMA.

La arquitectura básica de un Sistema CDMA (ver figura 4.3)

PSTN – Red Telefónica Pública de Conmutación, provee la vía hasta y desde los subscriptores (abonados) terrestres.

MSC – Centro Móvil de Conmutación, que hace la interfase entre el sistema CDMA y la PSTN. El MSC encamina las llamadas hacia y desde la PSTN al CBSC y mantienen archivos de subscriptores y facturas. El MSC es necesario para proveer el servicio celular.

AROUITECTURA BASICA CDMA

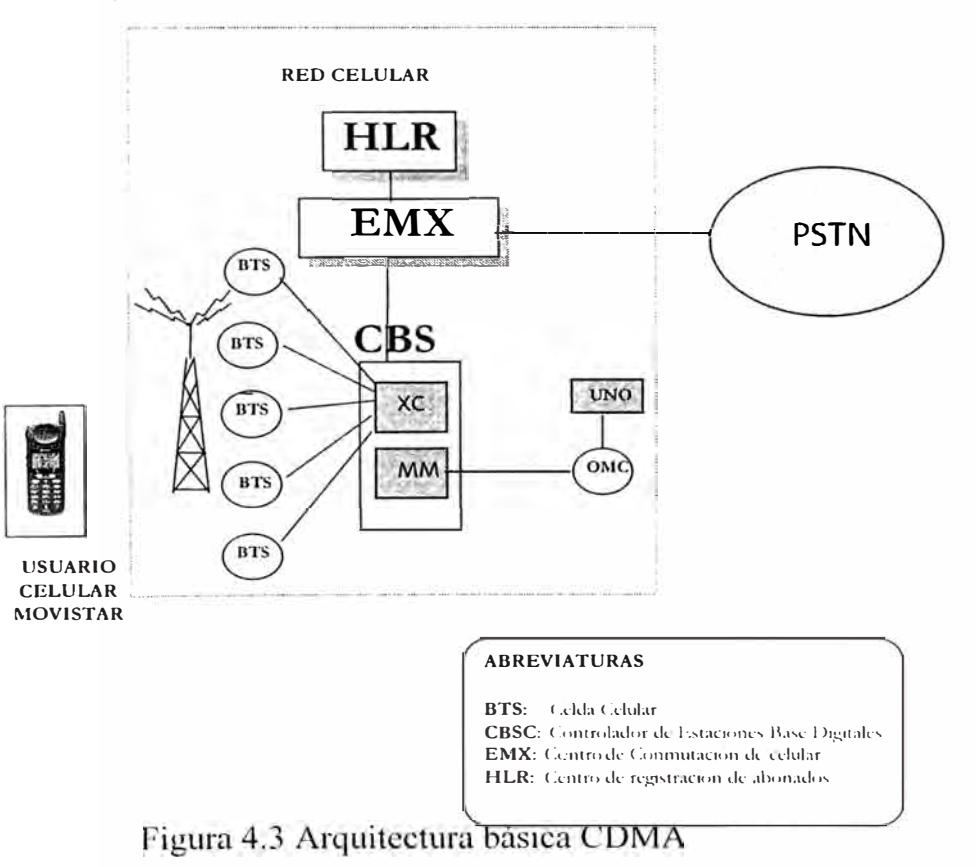



Figura 4.3 Arquitectura básica CDMA

CBSC – Controlador Centralizado de la Estación Base, el CBSC es la combinación del MM con el XC y otros dispositivos para establecer rutas.

MM – Dispositivo Administrador de las Unidades Móviles, consiste de un computar TAMDEM, que es responsable de la administración de las características de canales de radio especializados, administrar asignación de canales, ciertos tipos de handoffs y es el agente administrador de todos los dispositivos que requieren control operacional en el CBSC (BTS, XC)

BTS – Estación Base Transreceptora, esta entidad provee la interfase de la onda de RF entre ésta y las estaciones móviles (MS)

OMC-R – Centro de Operación y Mantenimiento Centralizado de Radio, esta es un computador TANDEM responsable de los datos estadísticos de uno o más CBSC

UNO – Centro de Operación de Red, es un servidor "SUN SPARCStation 20" que provee una interfase gráfica del usuario para proveer el estado del equipo de la red CDMA

4.2.3 Transmisión de datos en la red de Telefonía Celular CDMA

Para la realización de trasmisión de Datos en la infraestructura celular CDMA es necesario adicionar elementos de red que sirvan de pasarela entre la red Celular CDMA y la red de datos TCPIP. En tal sentido la transmisión de datos puede ser por circuitos o paquetes

Transmisión de Datos por Circuitos

Trasmisión de Datos por Paquetes

4.2.4 Transmisión de Datos por Circuitos : Para transmitir datos por circuitos es necesario añadir a la red celular un equipo que sirva de pasarela entre la red Celular y la red de datos TCP/IP (ver figura 4.4). El equipo que sirve de pasarela para poder transmitir datos a través de una comunicación por circuitos es el IWF.

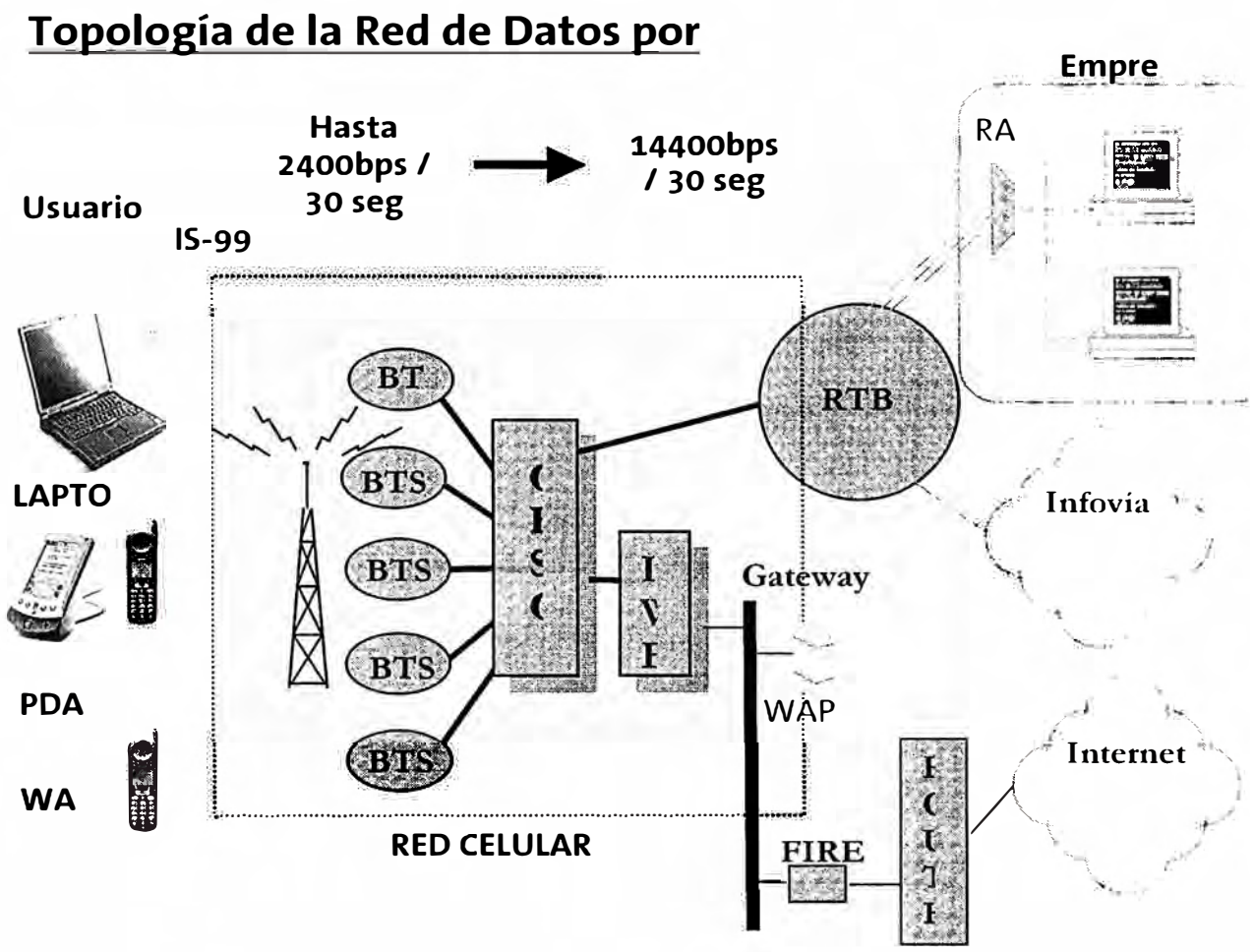



Figura 4.4 Topología de la red – Transmisión de datos por Circuitos

IWF

El equipo para interconectar redes, IWF o TOTAL CONTROL CDMA DATA SYSTEM (Equipo de Control para el Sistema de Datos CDMA), eesta sección proporciona una apreciación global del Total Control CDMA (IWF) para el Sistema de transmisión de Datos CDMA con el CBSC.

El Total Control CDMA permite al CBSC de Motorola procesar llamadas de datos y fax a velocidades de 14400 y 9600 bps de acuerdo con la Norma El sistema de datos

CDMA es conocido como Internetwork Function (IWF), Motorola prefiere el termino Internetworking Unit (IWU)

Un equipo Total Control CDMA configurado completamente pueden atender hasta 40 llamadas en forma simultanea La transmisión de datos CDMA en un sistema de comunicaciones inalámbrico digital, permite el uso eficaz del ancho de banda analógico o incluso otros sistemas inalámbricos digitales y la seguridad es inherente al sistema. El dispositivo móvil, típicamente una computadora portátil, ejecuta el software de comunicación que espera tratar con un modem anaiógico, no con un teléfono de CDMA.

El teléfono CDMA tiene un puerto de datos conectado directamente al puerto serial de la PC y la llamada que el usuario móvil esta realizando tiene como destino por lo general un módem analógico o una máquina fax que se conecta a la Red Publica de Telefonía Fija (PSTN). Los módems se comunican usando los tonos analógicos, los tonos analógicos se encuentran en el mismo rango de frecuencia de la voz humana, pero los tonos usan todo de la capacidad de la portadora de datos proporcionada por "el voiceband." El CDMA utiliza conceptos de codificación digital de voz, usando un proceso llamado "vocoding".El proceso de "vocoding" toma como entrada muestras digitales de una forma de onda de voz analógica, y como salida una cadena de códigos digitales. La conversación de una forma de onda de voz analógica muestreada digitalmente a una forma comprimida es llamada "encoding", mientras que lo inverso es llamado "decoding" El objetivo es minimizar la cantidad de data transmitida, mientras se mantiene una calidad de voz aceptable a un costo de equipamiento adecuado.

El CDMA emplea vocoder de capacidad variable convirtiendo las señales de voz muestreadas a :8K o 13k proporcionando luego velocidades de transmisión de datos 9600 o14400 bps respectivamente.

Debido a la fluctuación en el entorno de Radio Frecuencia de CDMA estas velocidades solo pueden ser alcanzadas a través de la utilización equipos especialmente fabricados para este propósito.

características del IWU

- Transferencia de datos Asíncronos: Una de las características es proveer un camino dedicado entre el dispositivo móvil y el dispositivo de tierra u otro móvil durante toda la llamada. El camino es una conexión doble asíncrona que proporciona una conectividad punto a punto Los datos son llevados digitalmente desde y sobre la interfase aire. Cuando localiza el IWU se convierte en una señal digital PCM antes de ser trasmitida por la PSTN. Las originaciones y terminaciones de llamadas móviles son soportados.
- Las opciones de servicio 4 y 12 de las normas IS-99 y IS-707 son soportadas por el IWU para llamadas asíncronas de datos de velocidades de 9.6 kbps y 14.4kbps.
- V.42bis Compresión : Se puede usar la compresión V.42bis sobre el enlace de aire para un uso más eficiente de la frecuencia de la radio (RF). Empleando esta característica se puede incrementar el rendimiento en 1.5 veces (esta característica no incluye la transmisión de faxes). Si habilitó esta característica, la negociación de la compresión V.42bis se efectúa entre el teléfono y el IWU después de que el orden de ATD se recibe del Móvil
- Clase 2.0 Fax : Esta característica transfiere datos asíncronos, proporciona un el camino permanente entre el dispositivo móvil y el dispositivo de tierra mientras

dura la llamada . La transferencia de datos de fax se basa en la Clase de ITU-T 2.0 de fax estándar. Pueden enviarse los facsímiles del dispositivo móvil, un PC que ejecuta una Clase 2.0 adaptado a una aplicación del facsímil conectada a teléfono CDMA, a un dispositivo de tierra.

El IWU soporta las opciones de Servicio 5 y 13 de las normas IS-99 para los faxes class 2.0 a velocidades de 9.6 y 14.4 Kbps.

- Fax Analógico : : Esta característica transfiere datos asíncronos, proporciona el camino permanente entre el dispositivo móvil y el dispositivo de tierra mientras dura la llamada . La transferencia de datos de fax se basa en T.30 y T.4 de fax estándar
- Conexión Rápida de Red de Pila Simple (Single Stack Quick Net Connect, SS QNC):Esta característica permite una conexión directa a Internet / Intranet sin acceder a la PSTN. El IWU enrruta los datos desde la red inalámbrica CDMA hacia Internet o Intranet empleando el protocolo PPTP (Protocolo Punto a Punto Perfeccionado) originado en la Laptop Esto evita el uso de los recursos de red de la PSTN
  - ✓ Laptop conectado al teléfono.
  - ✓ Asimismo esta conexión permite establecer la conexión de los terminales celulares con el programa de navegación (browser) en los teléfonos. Al abonado de la red celular CDMA le permite acceder a contenidos de datos en la red TCP/IP de Internet o Intranet vía el programa instalado en el teléfono (micro browser)
  - ✓ Usa conmutación de circuitos con salida IP desde el IWF, quiere decir que el uso de los recursos de una llamada de este tipo (llamada de datos) utiliza los mismos

recursos de la red celular con la diferencia que por esta llamada se cursa DATOS, por tanto la facturación de estos tipos de llamadas estas sujetas al tiempo que duren las mismas.

- ✓ Este tipo de llamada es atendido bajo la opción de servicio de datos asíncronos, hace eficiente el uso de la pila de protocolo CDMA
- ✓ Las llamadas son establecidas completamente en 2-3 transacciones
- ✓ Por tanto este tipo de llamada permiten al Celular con micro browser la navegación por Internet ó intranet, conexión WAP (Protocolo de Aplicaciones Inalámbrica).
- ✓ teléfono celular con micro browser

4.2.5 Transmisión de datos por paquetes

La transmisión de datos por paquetes (Packet Data) introduce una característica particular a la red Celular CDMA, red que ha sido configurada para transmitir trafico de voz. Los subsistemas MSS, BSS y HLR están instalados en la infraestructura de la red Celular y soportan tráfico de voz. El Inter-Working Unit (IWU) para transmisión de datos por paquetes deberá permitir la conectividad entre l red de datos y la red Celular.

El propósito de este documento es para:

Describir la operación del HSPD ( Datos por Paquetes a Alta Velocidad) en el sistema

Descripción del impacto del HSPD entre las interfaces con los subsistemas

IS-41 sobre el enlace entre el HLR y el MSS

IS-634 sobre el enlace A+ entre el MSS y BSS

IS-658 sobre la interfase L entre el BSS i el IWU

IS-95 y IS-707 sobre la interfase aire y el móvil (terminal celular)

a. Arquitectura del Sistema

La red IP de paquetes provee de varios niveles de servicio y asegura la comunicación entre los nodos de la red de datos (ver figura 4.5). El extremo final móvil (teléfono celular)con High Speed Packet Data permite obtener una dirección IP al terminal celular y hacerla parte de una red IP de tierra. El nivel superior del protocolo IP permite manejar conexiones al nivel de aplicación

El IWU por paquetes provee conexiones hacia red de paquetes Internet .aunque la red IP podría contener diferentes equipos de red dentro del dominio de la red Celular la configuración de estos equipos permitirá tener una interfase estándar para todas las conexiones entre la red Celular y la red de datos permitiendo conexiones PPP y WAP en el terminal Celular. La interfase entre el IWU por paquetes y el BSS es la interfase "L" (IS-658). Una base de datos dentro del IWU provee el IMSI/MIN para la dirección IP mapeada permite al terminal móvil tener una operación continua sobre el canal de radio empleado, el estándar empleado provee una dirección IP para el acceso a Internet.

El BSS provee la movilidad y administra al móvil durante el soft handoff y conexión para el terminal celular vía la interfase aire IS95B CDMA y el estándar IS-707. El protocolo de enlace de radio provee el nivel 2 para la corrección y detección de errores del servicio. El BSS debería también soportar el IS-658 I-interfase con el IWU. Con este servicio se genera una nueva mensajeria (IS-634) que requiere un enlace de conexión con el MSS para soportar la administración de las llamadas.

El MSS no realiza un papel activo logrando la conectividad a una red de IP. Proporciona una entrada para la llamada, la asignación de recursos, y conectividad permanente a los elementos de la red celulares. Perfil del subscriptor dentro del VLR o el HLR es apoyado dentro del MSS. La modificación de algunas mensajerías del IS-41 permitirá al IWU notificar a un móvil de paquetes entrantes cuando este puede ó no estar bajo el servicio del IWU.

En general una unidad que soporta el servicio de paquetes logrará una conexión PPP a través de una comunicación entre el BSS y el IWU.

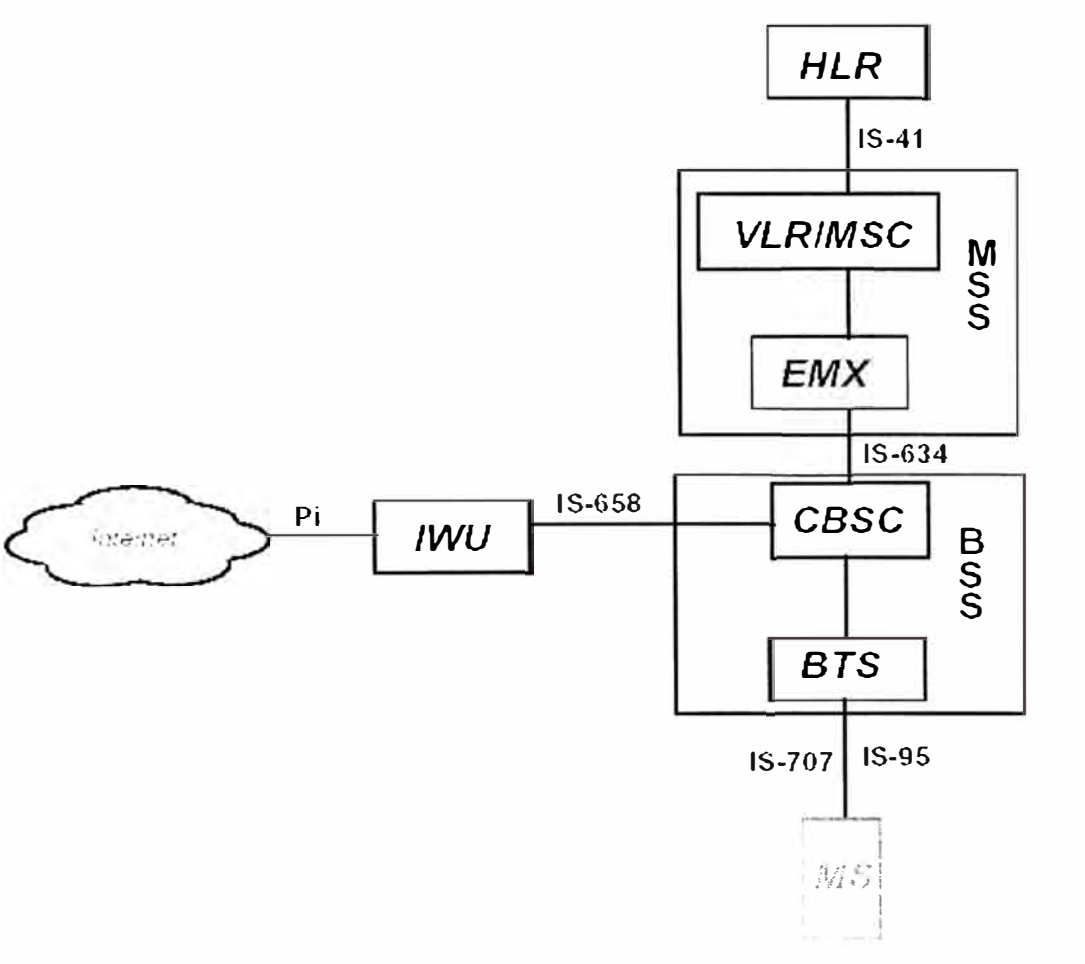



Figura 4.5 Arquitectura del Sistema

b. Descripción y características del sistema

Descripción del Servicio de Paquetes, el servicio del paquete permite al equipo de la estación móvil acceder una red de IP (internet o intranet). La llamada de voz es tratada de forma diferente a una llamada de datos, en esta última llamada se enrruta el tráfico a una red de tierra

El servicio de paquetes soporta una conexión a Internet o Intranet a través de un dirección IP, y soporta también conexión WAP

Cuando se asigna una dirección IP de una rango de direcciones IP y el móvil registra una sesión, la dirección IP usada durante esta sesión de paquetes deberá mantenerse.

El servicio WAP permite al móvil usar una dirección IP permanente única, asignada y administrada por la red del operador, esta dirección IP será asignada al dispositivo mientras dure la sesión WAP.

Aprovisionamiento del Servicio de paquetes, la baja o alta velocidad del servicio deberá aprovisionarse sobre la base de cada subscriptor. Si el subscriptor requiere el servicio de paquetes y este no esta aprovisionado o no soportado entonces la llamada deberá ser liberada. Si el aprovisionamiento es llevado a cabo, entonces el id del móvil (IMSI/MIN) es asociado a una lista de opciones de servicios para el subscriptor. Esta lista de servicios es llamada CDMAServiceOptionList (Lista de Opción de Servicio CDMA). Hay múltiples servicios para el servicio de paquetes.

Interfase Aire, la interfase aire esta basada en el estándar CDMA IS-95 y IS-707, la transmisión de datos a baja o alta velocidad están soportados por estos estándares del servicio de paquetes. El formato de tráfico no esta soportado por estos estándares

Canales de enlace directo (hacia el móvil), el sistema podrá concatenar 6 RS-1 o 5 RS-2 canales de trafico de datos (según el estándar IS-95B) sobre el enlace directo logrando alcanzar una velocidad máxima de 64 Kbps sobre este enlace.

La nota: La velocidad real alcanzada en la comunicación dependerá de los recursos disponibles en la red celular, interfase aire, canales disponibles de la red celular etc.

El número máximo de canales de tráfico de datos en el Forward será provisionable (variable). Esto permite al operador limitar la cantidad de canales empleados para transmisión de datos para una llamada de este tipo (servicio de paquetes). La razón principal de esta facilidad es proporcionar los medios para controlar la cantidad de interferencia que puede generar este tipo llamadas de paquete sobre las llamadas de voz que producirían una degradación en la calidad de la misma

Enlace Reverso, (desde el móvil a la estación base), el sistema soportará un máximo de un RS-1 (9.6kbps) o un RS-2 (14.4kbps) de canal de tráfico inverso.

La nota: El rendimiento real de esta comunicación dependerá de varios factores tales como los recursos disponibles, la señal de radio, utilización del buffers, etc..

Estados de la conexión en Paquetes, son dos los estados principales de una sesión en paquetes: abierta y Cerrada. Cuando la sesión del paquete está abierta, los sub estados permitidos son activos (active) o inactivos (Dormant). Se tiene una sesión activa cuando la interfaz de L ha sido establecido para el móvil, al móvil se le asigna uno o más canales de tráfico para la transmisión de paquetes. El modo Dormant

ocurre cuando el enlace se encuentra en modo de descanso, la sesión esta activa pero la interfase L no esta establecida o activa.

Mantenimiento de una sesión abierta, para que se genere una transmisión de paquetes esta sesión antes debe de registrarse en la red IP. Como el móvil se desplaza a través de la red Celular este terminal deberá ser atendido por diferente equipos y mantener la configuración que obtuvo en la registración.

Sesión de Paquetes Abierta (Registración Inicial), En una llamada para el servicio de paquetes se establece dos registraciones, una registración en la red Celular y la otra registración en la red de Datos, entonces un subscriptor abre una sesión de paquete mediante una previa registración a la red de Datos. Esta comunicación es análoga a la registración a la red Celular. La registración de la sesión en la red de paquete asigna una dirección IP al móvil así mismo esta dirección IP es anunciada al IWU. Para realizar la registración, el móvil debe originar una llamada de paquete.

Antes de la registración del servicio de paquetes debe haberse realizado la registración del servicio en la red Celular de voz con el MSS. En el proceso de la registración de la llamada el HLR enviará el perfil del subscriptor y asociará el CDMAServiceOptionList que ha sido aprovisionado como opciones del servicio de paquetes. El MSS guardará el perfil que se usará para validar la llamada del subscriptor (originaciones y terminaciones)

Cuando la sesión se abre, la infraestructura temporizará dicha sesión para los estados de inactividad, tiempo que puede ser configurado por el operador, cuando el sistema registra actividad en la comunicación este timer es reiniciado y llevado a cero pero si la temporización llega a su tiempo de expiración la sesión de paquetes se cerrará y si

se deseará transmitir información será necesario iniciar una nueva sesión de paquetes.

Mantenimiento de Sesión de paquete (Re-registración), como los móviles se desplazan constantemente a través de la red Celular son varios los equipos que atienden dicha comunicación, el móvil debe mantener siempre la dirección IP e informar de este dato cada vez que migre a otra zona. El móvil realizará un re-registración de paquete cuando descubre una nueva transmisión de SID/NID hacia el sistema que lo esta sirviendo. El móvil tiene la habilidad de recordar las múltiples zonas a las cuales se ha registrado y sólo se re-registrará si la zona del paquete no es ninguna de las zonas que guarda en memoria. El móvil realiza la misma función que realizó en la primera registración. La red no necesita enviarle una nueva dirección IP debido a que esta conexión tiene una sesión activa y debe usar la dirección de IP ya asignada. Para la conexión WAP, no hay ninguna diferencia entre la registración inicial y re-registración.

Ingreso al modo Dormant (inactivo), la sesión de paquete del subscriptor entra en el Modo Dormant cuando se produce uno de los siguientes eventos:

- Cuando el canal(es) de tráfico RF es liberado,
- Cuando la interfase L es liberado, o
- La conexión del SCCP se libera.

Cuando este modo se activa la sesión empieza a cronometrar el tiempo que permanece en inactividad, este tiempo es configurable por el operador en las unidades de segundos (el rango de tiempo permitido es de 0-255 seg –4 min. 15

seg.). Es recomendable que este tiempo no sea menor a los 20 seg. Para valores menores a los 20 seg la asignación de canales de tráfico el sistema es ineficiente. Este tiempo corresponde al tiempo para soltar y el reasignar un canal de tráfico.

BSS recibe la orden de liberación bajo el IS-95 desde el móvil, el móvil puede enviar la orden de liberación IS-95 el orden del descargo debido a estas razones:

• El BSS debido a la inactividad en la transmisión de paquetes llega al tiempo de expiración de la sesión

• Una llamada de paquetes es liberada debido al hard handoff

BSS tiempo de expiración de inactividad de paquetes, el BSS soporta un tiempo de inactividad de transmisión de paquetes el cual es configurable en el rango de 0-255 seg.. Este temporizador deberá ser reiniciado si el BSS envía o recibe tráfico RPL sobre la interfase IS-95/RPL. Si este temporizador expira entonces el BSS deberá ingresar al modo Dormant. El BSS inicia la liberación de la interfase L. El BSS enviara el mensaje de control de opción de servicio al móvil indicándole que esta a la espera de su reconexión Luego el BSS liberará los canales de tráfico IS-95, asimismo el BSS comenzará a liberar la interfase IS-634 con el MSS.

Liberación de llamadas de paquetes debido a Hard Handoff, ccuando el BSS determina que se requiere un hard handoff, el BSS comenzará la entrada en el Modo Dormant, actuando de forma idéntica a la descripción anterior.

Salida del modo Dormant (inactivo), la sesión de paquete de un subscriptor terminará el Modo Dormant (modo inactivo) y entrará en el Modo Activo cuando uno de estos eventos ocurra:

• Móvil origina una llamada de paquete

• IWU recibe un paquete para el móvil

Al terminar el Modo Inactivo (dormant), un canal de tráfico RF intentará ser asignado y la interfase L establecerá su conexión.

Móvil origina una llamada de paquetes, esta invocación puede ser el resultado de cualquier número de actividades por el móvil. Algunos de éstos podrían incluir la conexión de paquete el equipo, una petición del subscriptor, alguna petición de software de la aplicación, etc.,

De la perspectiva de la infraestructura, esto aparece como una llamada de paquetes originada en el móvil.

Sobre esta orden de originación IS-95, el BSS realiza un requerimiento de servicio CM al MSS a través de la interfase IS-634, el MSS valida la originación del móvil y en paralelo, el BSS intenta asignarle canales de tráfico. El BSS debería también intentar iniciar el RPL. El BSS recibe una asignación a la petición IS-634 desde el MSS, luego el móvil es validado en el BSS y este intenta establecer la conexión con la interfase L. Después de que la interfaz de L se establece entre el BSS e IWU, el móvil y el IWU levantarán cualquier capa protocolo adicional (PPP, TCP/IP, UDP). Si el IWU avisara que no tiene una sesión abierta actualmente, el móvil puede necesitar registrarse en la red de IP de datos.

c. Servicios de Datos CDMA

Formato de Opción de servicio

En CDMA los servicios de datos son identificados por las Opciones de Servicio (Service Option). Una Opción de Servicio está compuesta de tres campos, el Indicador Propietario, la Revisión de Opción de Servicio, y el Servicio Base (ver tabla 4.1)

Tabla4.1 Opciones de Servicio

| Indicador Propietario | Revisión de la Opción de Servicio | Servicio Base, número de opción |
|---|---|---|
| 1 bit | 3 bits | 12 bits |

Servicio de Alta Velocidad de Datos por Paquetes

Los Servicios Option número 22 al 29 provee el servicio portador compatible con muchas redes de paquetes. Las opciones de servicio del 22 al 25 soportan el protocolo Internet (IP) y Connectionless Red Protocolo (CLNP) las redes. Las opciones de servicio del 26 al 29 soportan Datos por Paquetes Celular Digital (CDPD).

d. Servicio de transmisión por Paquetes (Packet Data)

d.1 Red de Paquetes

La Topología de la Red consiste de los elementos de red celular (ANSI 41) y de la red de paquetes. El IWU Packet actúa como el puente entre estas dos redes (ver figura 4.6).

Los elementos de la red celular incluyen lo siguiente:

- HLR (Home Local Register): Responsable de proveer el aprovisionamiento para el uso de la red celular y el servicio de paquetes de datos. Incluye el listado de opciones de servicio en el perfil del usuario.
- Central Celular (EMX): Controla la salida de la llamada, validación, estadísticas y las características de interacción de voz. La Central Celular no realiza alguna conexión de circuitos para las llamadas por paquetes.
- Controlador de Estaciones Base Digitales y Estaciones Base (CBSC y BS): Provee la interfase inalámbrica para el terminal y la interfase con el IWU. Controla la mayor parte de las funciones de proceso de llamada para el Packet Data.
- Packet IWU: Actúa como un gateway y transfiere el tráfico de datos por paquetes entre el sistema celular y la red de datos por paquetes.

Los elementos de la red de datos por paquete incluyen lo siguiente:

- RADIUS (Remote Accces Dial-In User Server): Equipo ubicado en la red del Operador Celular encargado de realiza la autenticación y la asignación de números IP, en el caso de sus usuarios locales (servicio de Internet por paquetes), deriva los pedidos de autenticación a otros servidores según su dominio para el caso de los usuarios de Intranet por paquetes. También mantiene una asociación entre el usuario y la dirección del IP asignado, tanto así que la misma dirección IP es reasignada durante el re-registro.
- Enrrutador: Equipo en donde se establecerán las rutas para el tráfico IP de los usuarios móviles ya sea a Internet o a las empresas a donde deseen conectar.
- Gateway WAP: Equipo que permitirá brindar el servicio de e-mocion por paquetes a los usuarios móviles.

- Red IP: Es el medio de interconexión entre la red de paquetes de OPERADOR CELULAR y las redes LAN de las empresas.
- Servidor Radius en la empresa: Equipo que permitirá la autenticación así como la asignación de los números IP a los usuarios móviles que deseen acceder a la Intranet.

SERVICIO PACKET DATA – IS95 B

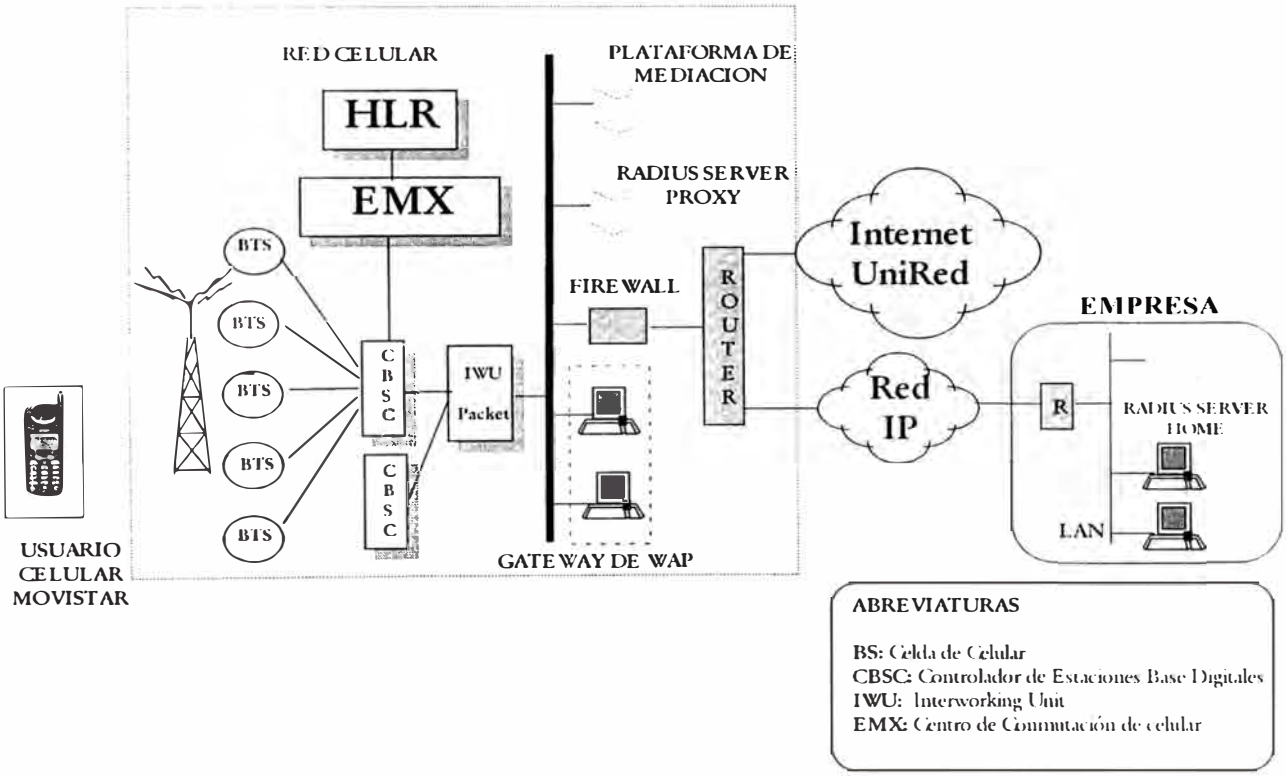



Figura 4.6 Red de Paquetes

d.2 Servicios la red de datos por paquetes

**E-mocion en paquetes y E-mocion Empresarial en paquetes**

El usuario móvil digital ahora podrá conectarse a los servicios de WAP mediante la red de paquetes de Operador Celular (ver figura 4.7), las principales diferencias que experimentarán son:

- No se tarifica por tiempo, sólo por volumen de data transferida durante la sesión.
- Bajo precio por trafico de datos.
- Se puede alcanzar velocidades de hasta 64 Kbps, según el terminal.

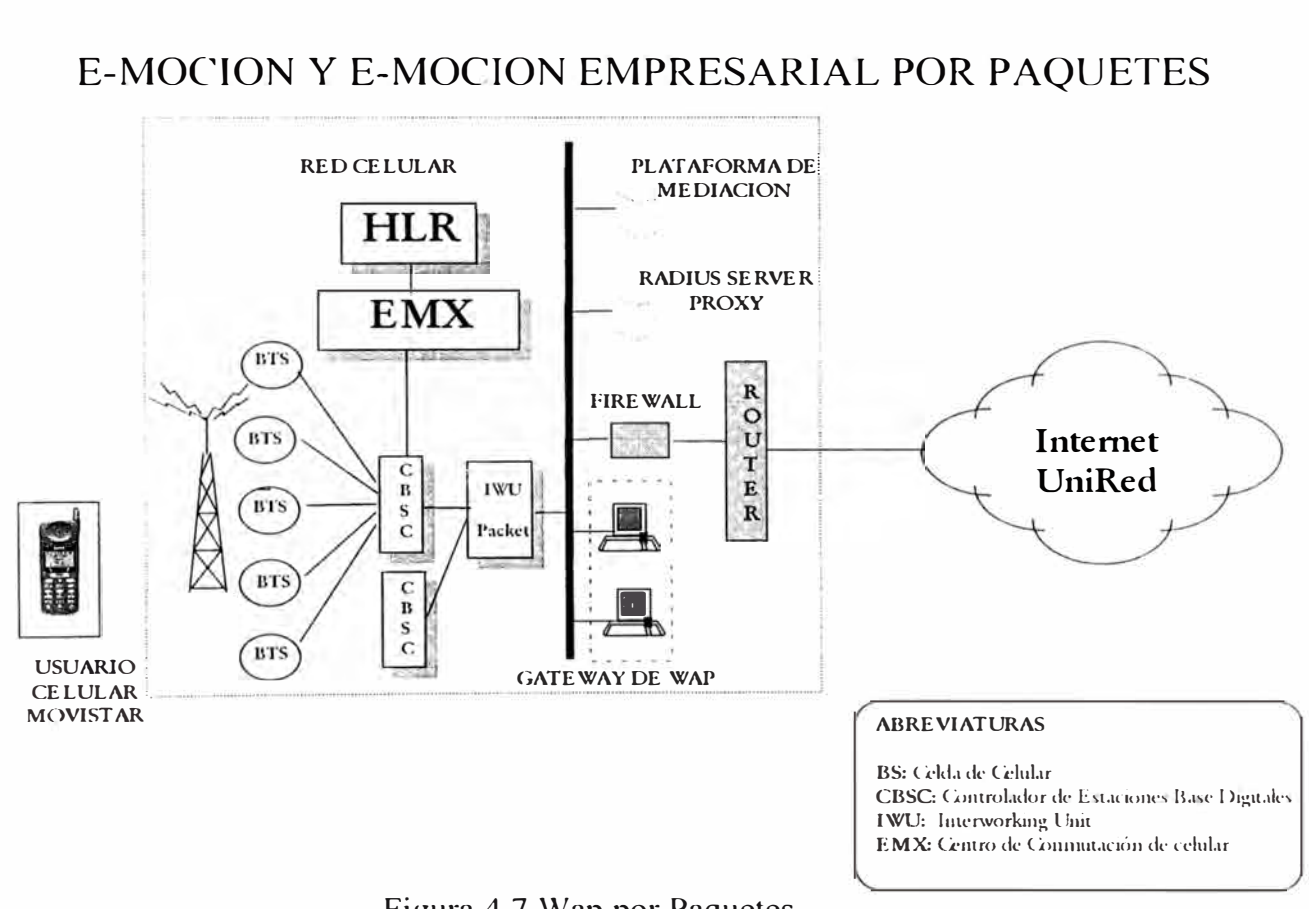



Figura 4.7 Wap por Paquetes

Intranet en paquetes

Permitirá al usuario Celular digital comunicarse mediante el terminal celular y una computadora o PDA, directamente con su empresa vía un enlace de la Red IP hacia la Red de Operador Celular (ver figura 4.8). A diferencia de servicio Circuitos y/o

Paquetes en el cual se disca un número telefónico del RAS de la empresa. El usuario tendrá las siguientes ventajas:

- Establecimiento de conexión casi inmediata (5 seg. aprox.).
- Velocidades hasta de 64 Kbps Rx/ 14,4 Kbps Tx desde el terminal.
- Estado de Dormant, sin perder la sesión.
- Tarificación por información transferida.
- Autenticación realizada por Operador Celular y por la Empresa.

La dirección de IP es asignada durante el registro de la sesión y es asignada por el servidor Radius Home de la empresa desde un pool de direcciones anteriormente brindada por operador Celular a la empresa.

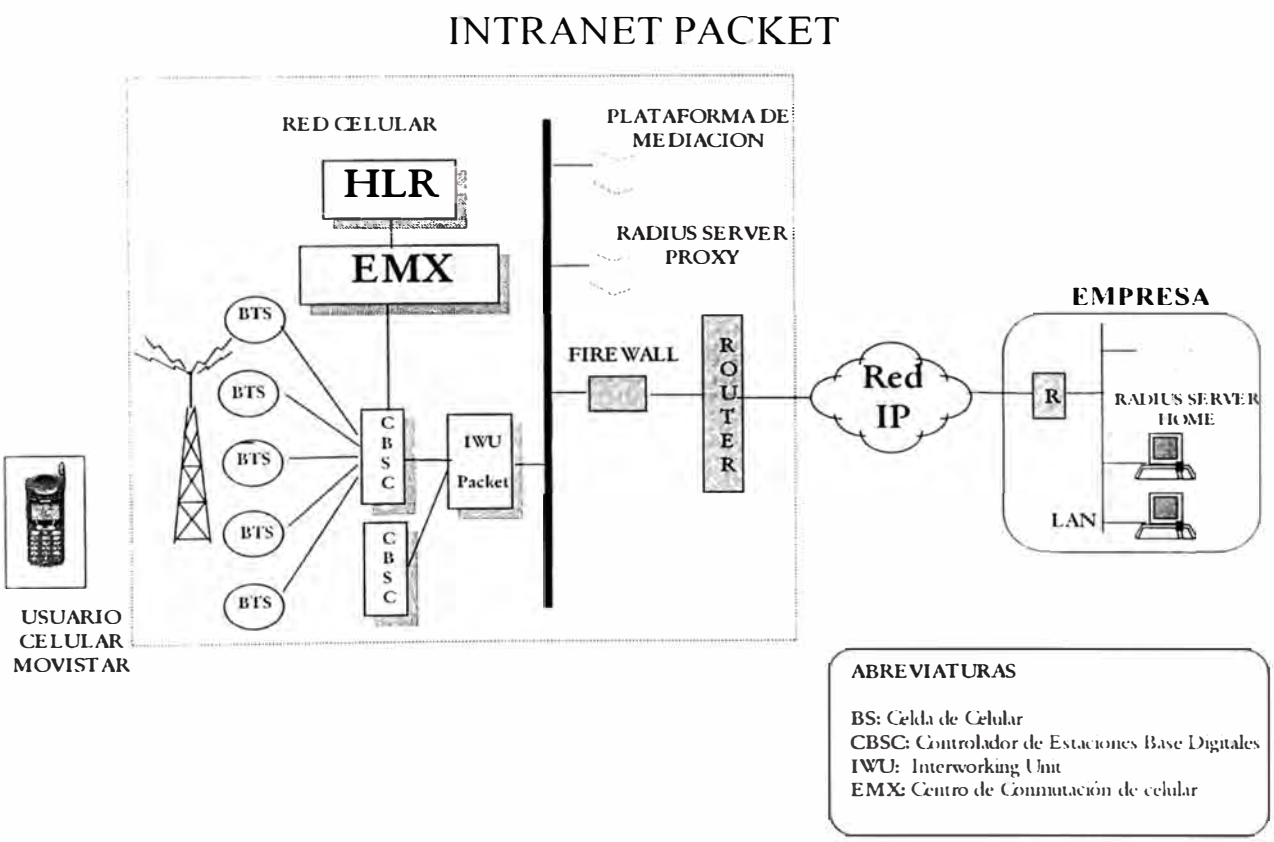



Figura 4.8 Intranet por Paquetes

***Internet en paquetes***

Permitirá al usuario Celular digital comunicarse mediante el terminal celular y una computadora o PDA, directamente a Internet (ver figura 4.9). El usuario tendrá las siguientes ventajas:

- Establecimiento de conexión casi inmediata (5 seg. aprox.).
- Velocidades hasta de 64 Kbps Rx/ 14,4 Kbps Tx.
- Estado de Dormant, sin perder la sesión.
- Tarificación por información transferida.
- Cuenta de acceso al servicio Internet incluido en la tarificación.
- Servicio de Autenticación por Operador Celular.

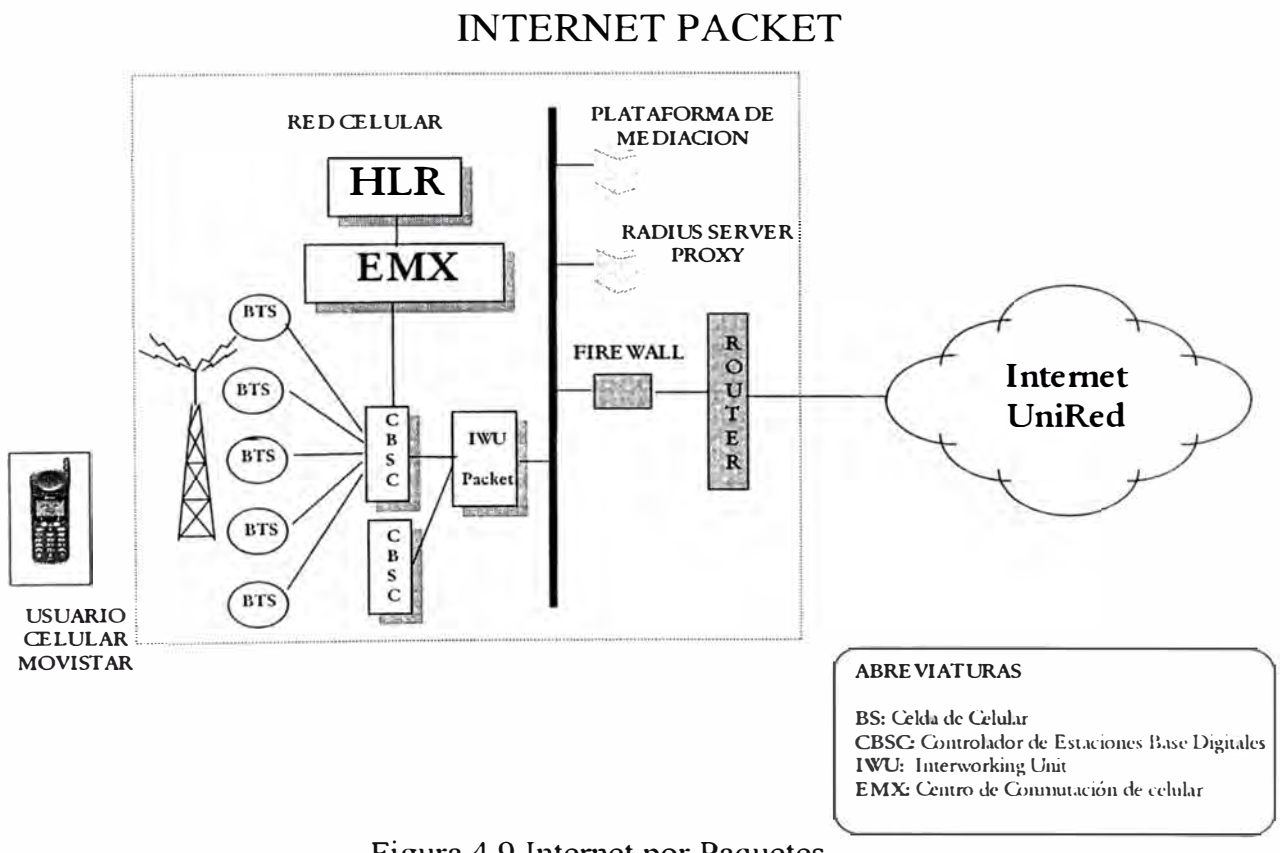



Figura 4.9 Internet por Paquetes

La dirección de IP es asignada durante el registro de la sesión y es asignada por el servidor Radius Home de OPERADOR CELULAR. Operador Celular brindará a los usuarios el servicio de acceso a Internet.

d.2 Sistema de Tarificación y Aprovisionamiento

La tarificación se realizará en base a la suma de los paquetes transmitidos desde y hacia los terminales móviles. El área comercial deberá crear tarifas dependientes a volumen de tráfico que curse el móvil, además se sugiere una tarifa mensual fija por interconexión a la red de paquetes de Operador Celular.

Las funcionalidades de la Tarificación y Aprovisionamiento del servicio IS 95B se realizará a través de una Plataforma de Mediación, la cual se comunicará usando el protocolo TCP/IP tanto al servidor Radius como al Sistema Comercial.

Entre las funcionalidades que presentará la plataforma de Mediación se tiene:

Tarificación:

- La plataforma es capaz de extraer la información que el PROXY RADIUS Server de la plataforma IS-95B Packet Data almacena para cada usuario que realiza una sesión.
- Una vez recolectados los datos, son procesados y se genera un XDR (eXtensible Detail Record) que contiene toda la información de la sesión TX de datos que un usuario ha realizado.
- Cuenta con una interfaz de comunicación con el Sistema de Facturación para el envió de los XDRs generados por la plataforma.

Aprovisionamiento:

- La plataforma permitirá el aprovisionamiento transaccional de usuarios, es decir, que por medio de OAS (Servicio de Ordenes Automáticas) desde el sistema comercial se podrán de dar de alta, baja y modificación del perfil a los usuarios en el servidor RADIUS.

El servidor Radius también permite un aprovisionamiento manual a través de una interfaz WEB. Esto podrá ser utilizado para la creación de dominios de usuarios corporativos.

4.2.6 Protocolo de Aplicaciones Inalámbricas (WAP)

WAP, Protocolo de Aplicaciones Inalámbricas, es un protocolo que apunta a proveer contenido internet y avanzar en el servicio de la telefonía para teléfonos digitales móviles, pagers y otro terminales inalámbricos que dispone de una capacidad de proceso (CPU y memoria) limitada, un display reducido, sin capacidades multimedia ni de representación gráfica, teclado básico y con estrictos requerimientos de consumo de batería. . Esta familia de protocolos trabaja a través de diferentes entornos de redes inalámbricas y muestras páginas web en terminales con baja resolución y bajo ancho de banda. Los teléfonos WAP son "smart phones" (teléfonos ligeros), que les permiten a sus usuarios responder e-mail, acceder a base datos de computadores y concede al teléfono interactuar con contenidos de Internet y e-mail.

Wap puede utilizar distintas opciones de transporte:

- ✓ Mensajes cortos (SMS)
- ✓ Datos en modo circuito (CDMA / GSM / TDMA)
- ✓ Datos en modo paquete (Packet / CDPD)

- ✓ Wap nace en respuesta al crecimiento a nivel mundial que experimentan los mercados de telefonía móvil e Internet
- ✓ Comenzó con soluciones propietarias de distintos fabricantes que fueron convergiendo a través de distintos acuerdos
- ✓ En Enero 98 nace el Wap Forum como asociación para la estandarización de protocolos y cuyos socios fundadores son Unwired Planet, Ericsson, Motorola y Nokia. Posteriormente se han unidos los demás fabricantes de terminales, equipos de red y tarjetas así como operadores de telefonía móvil

WAP especifica el Entorno de Aplicación Inalámbrica(WAE) y los protocolos inalámbricos. El WAE descansa sobre el WSP (Protocolo de Sesión Inalámbrica) y WTP (Protocolo de Transacción Inalámbrica)

La estructura básica de la arquitectura WAP puede explicarse usando el siguiente modelo. El orden de los niveles independientes, los cuales son jerárquicos, este sistema tiene como ventaja que es muy flexible y puede ser escalable de arriba hacia abajo porque los diferentes niveles o pilas las cuales están dividas en 5 niveles diferentes:

- Capa de Aplicación. Wireless Application Enviroment (WAE)
- Capa de Sesión. Wireless Session Layer (WSP)
- Capa de Seguridad. Wireless Transport Layer Security (WTLS)
- Capa de Transacción. Wireless Transaction Protocol (WTP)
- Capa de Transporte. Wireless Datagram Protocol (WDP)

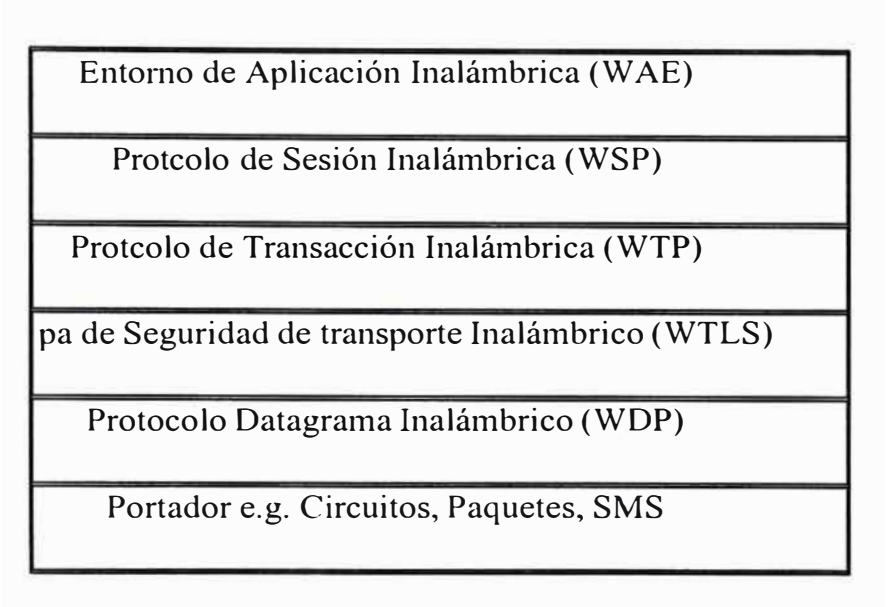



Figura 4.10 PROTOCOLO WAP

Cada capa esta encima de la otra, esta estructura hace posible que los fabricantes de software desarrollen aplicaciones y servicios.

La pila WAP entidad de protocolos las cuales cubre la transferencia de datos inalámbricos. El diagrama anteriormente citado muestra el orden de los protocolos. El nivel mas bajo se encarga de la transferencia y seguridad a través WTLS, todas las pilas debajo descritas son llamadas pilas de red (network stack). Debido a esta organización de pilas cualquier cambio hecho en la capa de red (network stacks) no debería afectar las capas superiores.

Capa de Aplicación (WAE y WTA)

El entorno para aplicaciones inalámbricas WAE (Entorno de Aplicación Inalámbrica) y aplicaciones para teléfonos inalámbricos WTA (Aplicación de teléfonos

inalámbricos) están en el nivel mas alto de esta jerarquía. Estas dos son las principales interfaces para el dispositivo del cliente, el cual proporciona y controla la descripción del lenguaje, y los scripts lenguaje de cualquier aplicación y especifica de los teléfonos. WAE y WTA tienen algunas simple funciones sobre el dispositivo cliente.

Capa de Sesión (Protocolo de Sesión Inalámbrica, WSP)

El Wireless Session Protocol (WSP) tiene todas las especificaciones para una sesión. Una sesión consta principalmente de 3 fases: Inicio de la sesión, transferencia de la información y fin de la sesión. Adicionalmente una sesión puede ser interrumpida e iniciada nuevamente desde el punto donde fue interrumpido.

Wireless Session Protocol. WSP provee el mas alto nivel de aplicación dc WAP, consiste de servicios de sesiones. El primero es el servicio de modo de conexión este trabaja sobre el nivel superior de capa de transacción WTP, y el segundo es un servicio sin conexión (connectionless) que opera sobre un datagrama de transporte seguro o no

El Wireless Session Protocol actualmente ofrece servicio http 1.1, ofrece la funcionalidad de data pus, capacidad de negociación, suspender / reanudar sesiones. El protocolo en la familia WSP están optimizado para ancho de banda bajo

Capa de Seguridad (Seguridad de la Capa de Transporte Inalámbrico, WTLS.)

EL WTLS es una capa opcional o una pila la cual consiste en llevar características propias del dispositivo (terminal). Una segura transmisión es crucial para ciertas

aplicaciones como comercio electrónico o WAP-banking y es un estándar en estos días. Además WTLS revisa el contenido de los datos de forma integral, autenticación de usuario y puertas de seguridad.

WTLS :Es un protocolo basado sobre el protocolo TLS. Esto es usado con el protocolo de transporte WAP y esta siendo optimizado por el usuario sobre un angosto canal de comunicación de ancho de banda. El protocolo WTLS esta encima de la capa del protocolo de transporte. Esta capa de protocolo de seguridad requiere determinar si es usado o no. Este provee un seguro interfase de servicio de transporte adicionalmente provee una interfase de administración de conexión segura. WTLS apunta a proveer privacidad, integridad de los datos y autenticación entre la comunicación de dos aplicaciones. En medio de estas características los datagramas son soportados, optimizando su negociación (handshaking) y renovación dinámica de las llaves de autenticación. Esto es optimizado con **latencia larga** para pequeño ancho de banda portador de las redes.

La estructura del protocolo WTLS. El registro de protocolo toma mensajes para ser transmitidos, opcionalmente comprime los datos, encripta y transmite el resultado. Los datos recibidos son desencriptados, verificados y descomprimidos y luego enviados a el nivel superior de la capa del cliente. En el estándar WTLS se describen 4 registros: El cipher spec protocol, el protocolo de handshake, el protocolo de alertas y el protocolo de aplicación de datos. En el protocolo WTLS si se recibe un registro de este tipo que no es entendido entonces esta información es ignorada. Varios registros pueden ser concatenados dentro de un transporte SDU. Por ejemplo varios mensajes handshake pueden ser transmitidos dentro de un transporte SDU.

Esto es particularmente practico con paquetes orientados transporte como mensajes cortos GSM.

EL protocolo de handshake esta constituido de 3 sub protocolos. Todos los mensajes son encapsulados en una estructuras texto plano (plaintext).

Capa de Transacción (Protocolo de Transacción Inalámbrica, WTP)

El WTP, provee los servicios necesarios para interactuar con el browser de la aplicación. Durante la sesión del Browser, el cliente solicita información del servidor y este responde con información. Esto es referido como una transacción. WTP se ejecuta sobre el servicio de datagrama y servicios de seguridad posibles.

La especificación para el nivel de transferencia está en el WTP. De forma similar al Protocolo de Datagrama de Usuario (UDP) y el WTP se ejecuta sobre la cabecera del datagrama. Tanto el protocolo UDP y el WTP son parte la aplicación estándar de TCP/IP que permite se simplifique el protocolo para terminales móviles. WTP concatena el protocolo de datos y la respuesta a los retardos reduce los numero de transmisiones. El protocolo intenta optimizar la interacción con el usuario y ordena que la información pueda ser recibida cuando se necesite.

Ventajas del protocolo WTP:

- Provee confiabilidad sobre los datagramas.
- Provee eficiencia sobre los servicios orientados a conexión.
- Esto es destinado para servicios orientados a transacciones.

Capa de Transporte (Protocolo Dagrama Inalámbrico, WDP)

El WDP representa la tranfrerencia o capa de transmisión y es también la interfase con la capa de red para todos los niveles o capas arriba mencionada. Con la ayuda de WDP el nivel de transmisión puede ser entendido por el nivel de red de los diferentes operadores. Esto significa que el WAP es completamente independiente de cualquier operador de red. La transmisión de SMS, USSD, CSD, CDMA, IS-136 paquetes de datos y GPRS son soportada.

### 4.2.7 Comunicación WAP

Plataforma UP.Link

Elementos requeridos para una comunicación WAP (ver figura 4.11)

I. UP.Browser :Micro navegador del terminal

II. UP.Link :Gateway Wap

III. UP.DSK :Software para el desarrollo de aplicativos

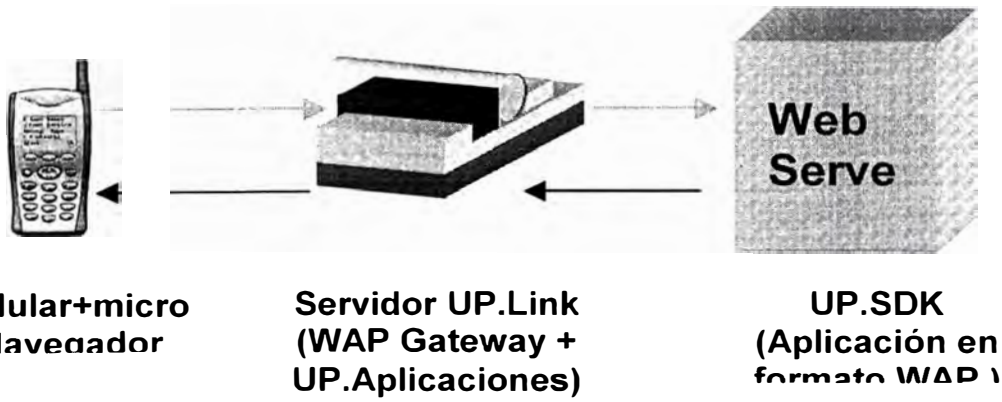



Figura 4.11 Elementos en la comunicación WAP

Browser del Terminal (micro navegador del celular)

Las características del software del teléfono celular que permite interactuar con Internet y las Intranet son las siguientes:

- Voz y datos en un simple dispositivo celular.
- Cumple totalmente con WAP 1.1
- Optimiza la producción de dispositivos pequeños en masa, a bajo costo, requiere por lo menos 160KB ROM, 10KB RAM
- Soporta encriptación a 40-bit o 128-bit
- Soporta las características de valor añadido que vienen con el UP.Link

  -Aplicaciones de Entorno Local (LAE)

  –WML+

  –Notificaciones

Gateway WAP (UP.Link)

La plataforma del gateway wap (equipo que sirve de pasarela entre la red celular y la red de datos) provee el armazón para la distribución de aplicaciones sobre redes de datos inalámbricas para teléfonos celulares y dispositivos Digitales de Asistencia Personal (PDA)

Componentes de la plataforma UP.Link

Esta plataforma tiene tres componentes básicos:

- El teléfono celular, que permite a los usuarios o subscriptores acceder a aplicaciones Web empleando un micronavegador especial
- El servidor UP.Link, que facilita la comunicación entre el teléfono celular y el servidor Web.
- Aplicaciones, que trabajan con el servidor UP.Link y el teléfono celular para proveer información y servicio a los subscriptores.

Teléfonos Celulares. Emplean un micro navegador equipado en teléfono convencionalmente conocido como web browser. El subscriptor requiere de unas llaves para que pueda navegar a las peticiones de los URLs. Los navegadores estándar emplean el formato para mostrar la información en las pantallas de los computadores, los micronavegadores hacen uso de un lenguaje diseñados para estos teléfonos. Los teléfonos celulares tienen una pagina hogar que les provee un menú de opciones básicas, los teléfonos celulares equipados con micro navegadores Phone.com son llamados UP.phones

Servidor UP.Link : Los terminales celulares emplean la capacidad de datos de la red convencional Celular para enviar los requerimientos de los usuarios al UP.Link . El servidor UP.Link convierte luego este requerimiento en formato http (Hypertext Transport Protocol) y lo reenvía hacia Internet. Cuando el servicio destino responde, el Servidor UP.Link pasa esta información al teléfono celular. Si el servicio emplea un formato que el teléfono celular no puede leer, como HTML, el servidor UP.Link traduce la respuesta a un lenguaje entendible por el teléfono celular. El servidor UP.link es el corazón de la plataforma UP.Link porque el servidor UP.Link puede traducir HTML a un formato que los usuarios del UP.Phone pueden entender y así lograr el acceso a cualquier lugar de Internet . La comunicación puede ser también por "Pushing" (comunicación del servidor UP.Link al teléfono celular) llamadas notificación WAP. El servidor UP.Link almacena la base de datos de todos los subscriptores que tienen este servicio

Aplicaciones : Las aplicaciones son el último componente de la plataforma de UP.Link. Las aplicaciones residen en los servidores de Web y generan un lenguaje dinámico para las colas de las bases de datos.

Las aplicaciones típicas son las siguientes:

- UP.Homepage, provee la localización de la pagina hogar
- UP.Mail , Con esta aplicación los subscriptores pueden usar sus UP.Phones para enviar, recibir y grabar correos.
- UP.Organizador, Es un aplicativo que administra la información personal que entregan subscriptores tales como calendario, libro de direcciones, lista de tareas y URL favoritos.
- UP.Web, interfase web que interactúa con varias de las tareas que las realizas del UP.Phone.

### 4.2.8 Seguridad plataforma UP.Link

Uno de los más importantes trabajos como sistema de administración es la implementación de la seguridad como una medida de proteger la comunicación de datos del servidor UPLink. En particular tu deberías implementar la seguridad para los siguientes tramos de la comunicación:

- Desde el teléfono hacia Internet (ida y vuelta). Esta comunicación ocurre cuando el subscritor pide o recibe contenidos Internet. La comunicación en mención esta compuesta de dos tramos, el primero entre teléfono y el servidor UP.Link (ida y vuelta) y la segunda entre el servidor UP.link e Internet (ida y vuelta). La primera están protegidas por el Protocolo de Aplicaciones Inalámbricas (WAP) o el Protocolo de Transferencia para Dispositivos Portátiles (Handheld Devive

Transfer Protocol, HDTP), El segundo es protegido por la Capa de Seguridad de Conexión (Secure Sockets layer, SSL)

- Desde la sincronización del cliente de correo hasta el servidor UP.Link. Esta comunicación ocurre cuando los subscriptores sincronizan sobre su PC sus mensajes de correo con los mensajes de correo de la base de datos del servidor UP.Link. Esta comunicación es protegida con SSL.
- Desde el servidor Web hasta el UP.Web. Esta comunicación ocurre cuando el subscriptor actualiza sus plantillas como alias de correo y firmas empleando la interfase UP.Web. Comúnmente esta información no es muy importante pero lo puede ser. Por tanto la comunicación de esta información puede estar protegida con SSL

Seguridad de la comunicación del Servidor UP.Link, para proteger la información del servidor UP.Link se hace uso de los certificados digitales y servicios de seguridad, esto protege la comunicación entre el servidor UP.Link y los proveedores de contenidos en Internet y el servidor UP.Link con los clientes que realizan la sincronización de sus mensajes de correo.

Cuidar la comunicación entre el UP.Link y los proveedores de contenidos en Internet es solo la mitad del trabajo.

Seguridad de la comunicación de los teléfonos

Proteger la comunicación entre el servidor UP.Link y el teléfono es el paso final en salvaguarda de la comunicación entre el teléfono e Internet. Para manejar como trabajan estos protocolos, se deben tomar las siguientes acciones

- Autenticación fuera de la banda

- Cambiar el estado de las sesiones de los subscriptores
- Encriptación disponible

Seguridad en la comunicación con el UP.Web, los subscriptores del servidor UP.Link tienen sus conexiones seguras con el UP.Web, ya que se ha instalado un certificado digital en el UP.Web.

A continuación se muestran los diagramas topológicos de tres redes diferentes que permiten la comunicación vía WAP

- Comunicación WAP sobre una red de Paquetes (ver fig. 4.12)
- Comunicación WAP sobre una red de Circuitos (ver fig. 4.13)
- Comunicación WAP sobre una red de SMS (ver fig. 4.14)

**Conmutación por Paquetes IP**

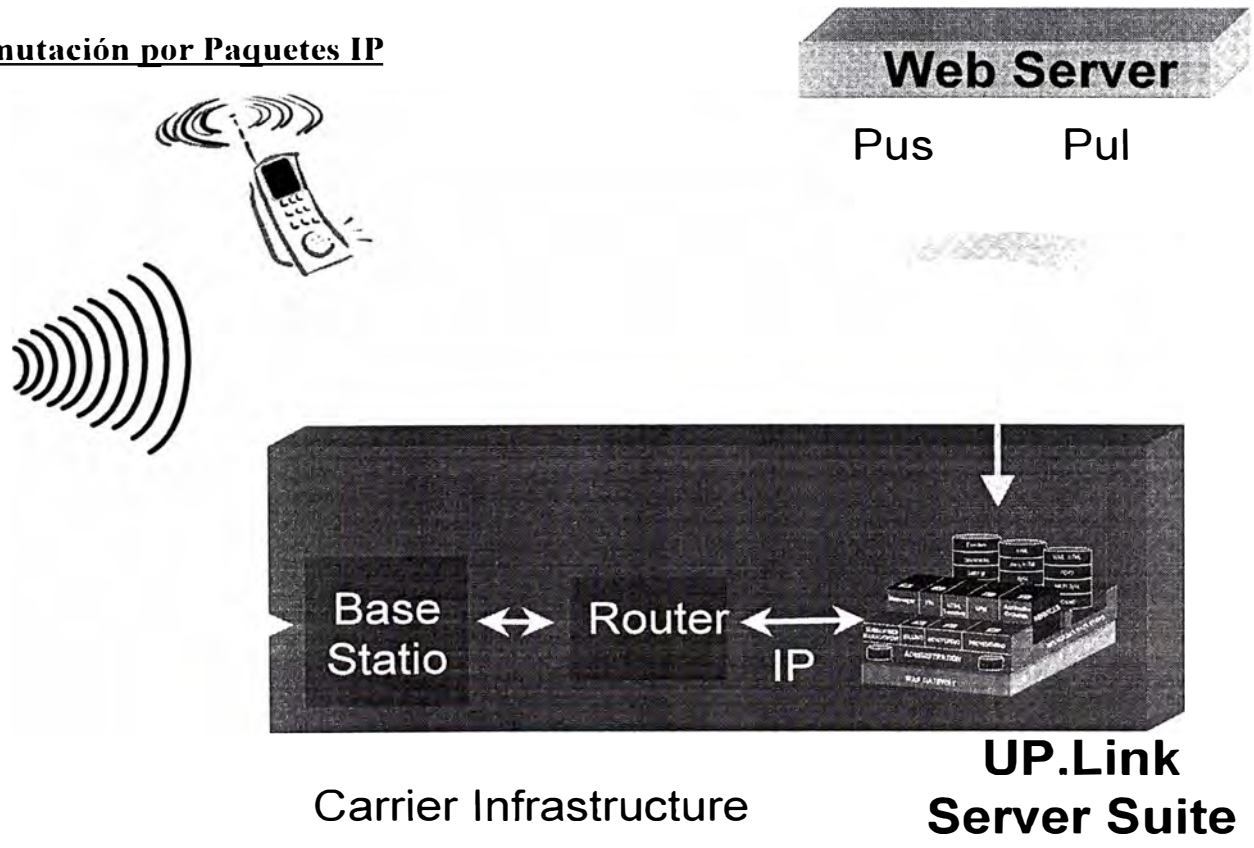



Figura 4.12 Comunicación WAP sobre una red de Paquetes

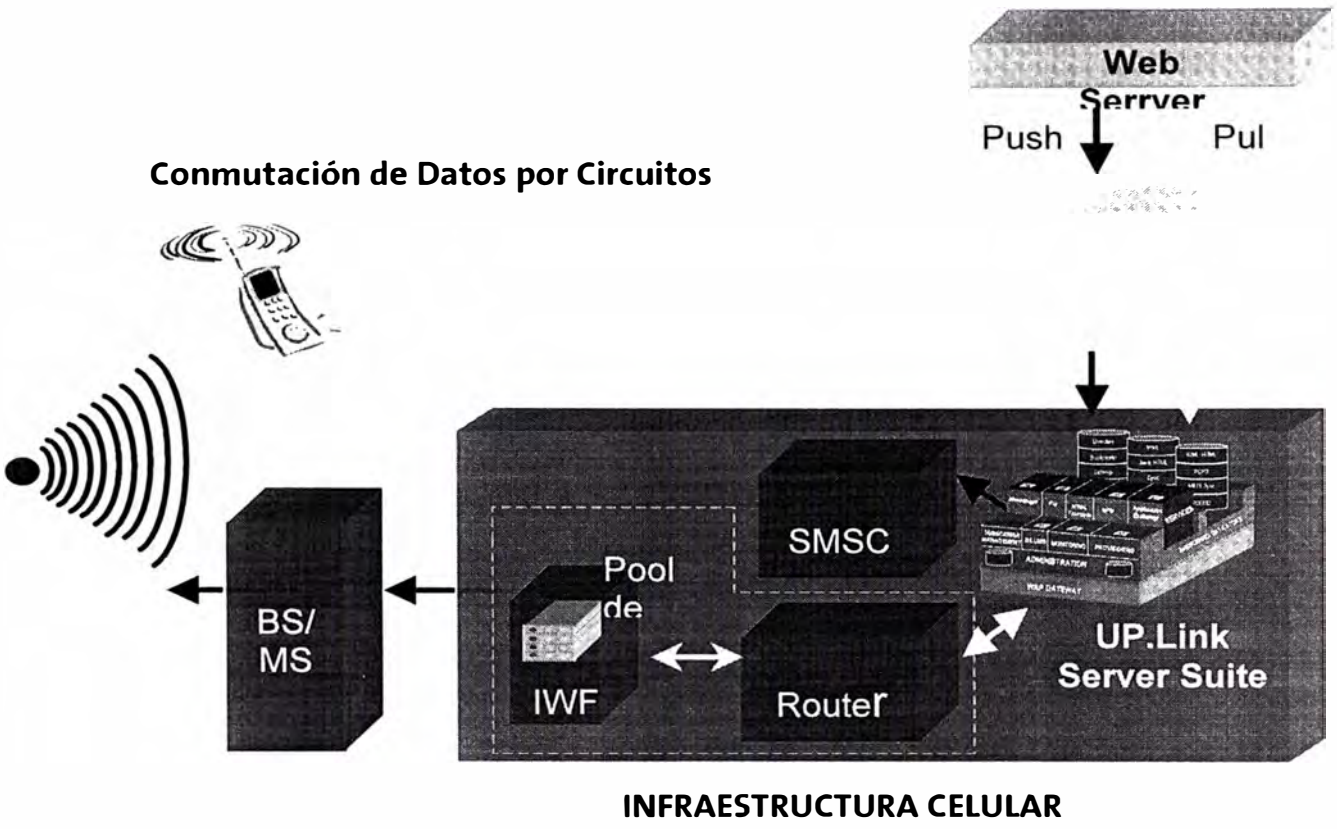



Figura 4.13 Comunicación WAP sobre una red de circuitos

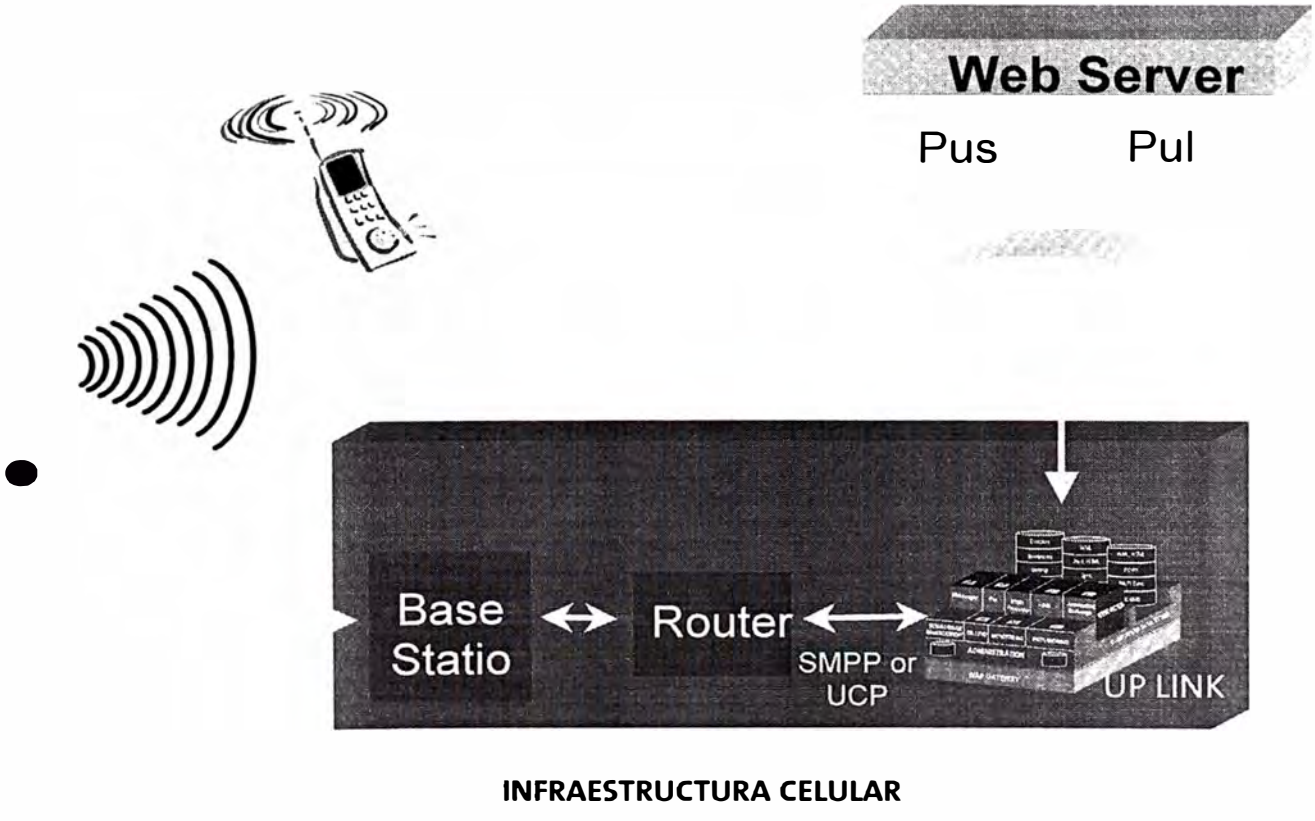



Figura 4.14 Comunicación WAP sobre una red de SMS

Seguridad UP.LINK tramo a tramo ("End-to-End-to-End")

La seguridad de la información en una comunicación WAP se realiza entre los puntos finales del protocolo (ver fig. 4.15), vale decir:

- Comunicación entre el Browser (Terminal celular) y el gateway WAP
- Comunicación entre el Gateway WAP y el aplicativo destino

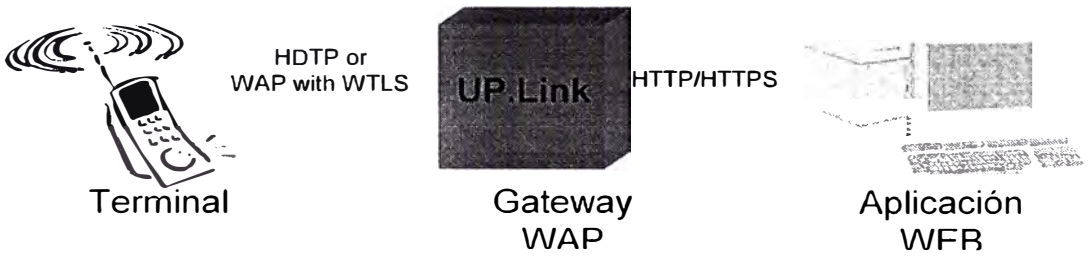



Figura 4.15 Seguridad tramo a tramo

- Teléfono - Servidor UP.Link, eeste tramo permite la encriptación entre el teléfono celular y el servidor UP.Link ubicada en la red del operador celular, la seguridad se realiza a través de: encriptación de los protocolos HDTP ó WAP, empleando algoritmos de cifrados estándares (RSA Data security)
- Servidor UP.Link – Internet, la comunicación en este tramo se puede realizar bajo las siguientes modalidades:
  - http (típico servidor WEB)
  - http con autenticación básica (usuario & clave)
  - https con autenticación (Comunicación certificada a través de IDs; encriptación de los nombres de usuarios, claves y datos de la comunicación).

Seguridad en la Comunicación del teléfono y UP.Link

Descripción de sesión segura WTLS (negociación completa, ver figura 4.16)

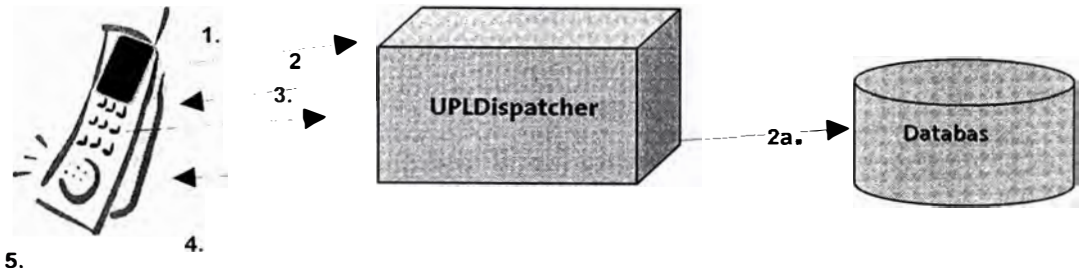



Figura 4.16 Negociación Completa

1. WTLS : Client Hello

Cuando se realiza la sesión con el servidor UP.Link conocido también como gateway Wap, esta se puede realizar en forma segura o no, si la comunicación es segura la sesión incluye una comunicación entre las pilas de protocolos WTP y WTLS y el terminal celular provee el client ID, Key-exchange y los algoritmos de encriptación que soporta, esta es una sesión típica empleada por los terminales WAP que funcionan sobre una red de comunicación por circuitos o paquetes.

Los puertos a conectar en el gateway Wap para un terminal con micronavegador 3.x ó 4.x varían

Sesión HDTP:

Todas las sesiones que se realizan con este protocolo son seguras y emplean el puerto UDP 1905 para establecer la misma

Sesión WAP

Terminal con browser 4.x  Port UDP  9201 (no segura)

Terminal con browser 4.x  Port UDP  9203 (segura)

2.Server Hello

El servidor (gateway WAP) verifica el client ID en su base de datos, envía el key-exchange y algoritmo de encriptación aceptado

3. El celular recibe el Server Hello y computa las llaves públicas y privadas enviando su llave pública.

4.El Dispatcher (modulo del gateway Wap) genera el ID de la sesión WTLS, el par de llaves SSK (en base a la llave privada y pública del celular), luego envía el ID de la sesión y su llave pública

5.Finalmente el celular usa su llave privada y llave pública del servidor para generar el SSK

Descripción de sesión segura WTLS (negociación abreviada, ver Figura 4.17)

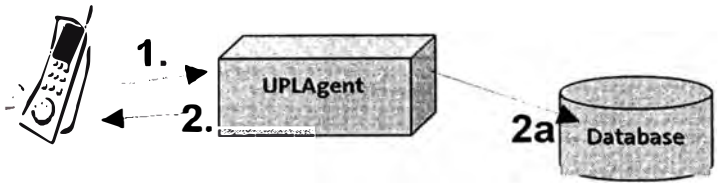



Figura 4.17 Negociación Abreviada

1.Client Hello: El celular conecta al puerto del agente provista por el ID de la sesión WTLS

2.Server Hello: El agente revisa la sesión WTLS en la DB. Si la sesión existe la conexión segura es creada. Luego el celular y el servidor utilizan la "llaves de conexión" (llamada también Shared Secret Keys) para encriptar la comunicación.

# CAPÍTULO V
# SEGURIDAD EN EL MÓDELO TCP/IP

## 5.1 Protocolo de Seguridad en el modelo TCP/IP

### 5.1.1 Definición

El protocolo de seguridad es la parte visible de una aplicación, es el conjunto de programas y actividades programadas que cumplen con un objetivo específico y que usan esquemas de seguridad de cifrado (criptográfica), cualquier protocolo de seguridad procura resolver algunos de los problemas de la seguridad como la integridad, la confidencialidad, la autenticación y el no rechazo, mediante sus diferentes características. Las características de los protocolos se derivan de las múltiples posibilidades con que se puede romper un sistema, es decir, robar información, cambiar información, leer información no autorizada, y todo lo que se considere no autorizado por los usuarios de una comunicación por red.

### 5.1.2 Esquemas de seguridad en los niveles TCP/IP

A continuación describiremos los protocolos de seguridad en los niveles TCP/IC.

a. Extensiones Multipropósito para Correo en Internet (S- MIME)

El protocolo seguro MIME (Multi-purpose Internet Mail Extensions) se ha desarrollado para poder transmitir mensajes multimedia a través de las redes IP. Es pues una ampliación del correo electrónico (e-mail) para la transmisión de información multimedia, que convierte en texto cualquier clase de información y que la regenera al formato original en el destino. MIME es, actualmente, el protocolo

más utilizado para enviar textos con formato no ASCII a través de Internet. Se conserva todo tipo de información y se muestra íntegramente el contenido al receptor. S-MIME que se utiliza para hacer seguro el envío de mensajes y las transacciones electrónicas incluye firma digital y cifrado basado en el algoritmo RSA de llave pública, es un competidor de otras técnicas como PGP (Pretty Good Privacy), y PEM (Privacy Enhanced Mail), también conocidos como PGP-MIME y PEM-MIME o MOSS/Mime Object Security Standard, respectivamente.

El estándar MIME fue creado en junio de 1992 por IETF (Internet Engineering Task Force). El objetivo de MIME es permitir a los clientes de correo electrónico enviar y recibir mensajes de texto plano y, también, textos con formatos y figuras, ficheros ejecutables, sonidos, imágenes, etc. El protocolo anterior a MIME, SMTP (Simple Mail Transfer Protocol), estaba limitado al juego de caracteres ASCII americano, y causaba problemas a los usuarios de otros países que necesitaban caracteres con tilde y símbolos especiales. Sin embargo, con MIME los mensajes de correo electrónico pueden contener:

Múltiples objetos en un mensaje simple, texto de longitud ilimitada, conjuntos de caracteres permitiendo lenguajes diferentes al inglés (distintos de ASCII), mensajes con fuentes múltiples, archivos binarios o de aplicación específicos, mensajes con imágenes, audio, vídeo y multimedia y campos de encabezado.

MIME define los siguientes campos de encabezado, que son utilizados por los clientes de correo electrónico para enviar/recibir los mensajes: El campo de versión MIME, que especifica la versión del estándar MIME que se ha utilizado en el mensaje y El campo de Content type, que se utiliza para especificar el tipo y subtipo de los datos en el cuerpo del mensaje.

b. Protocolo de autenticación Kerberos

Kerberos es un servicio de autenticación desarrollado en MIT (Massachusetts Institute of Technology) y diseñado por Miller y Neuman en el contexto del Proyecto Athena en 1987. Esta basado en el protocolo de distribución de llaves presentado por Needham y Schroeder en 1978.MIT. Utiliza criptografía de llave en lugar de contraseñas en texto plano. Kerberos ofrece una capa de seguridad del sistema y dificulta que un usuario no autorizado logre interceptar las contraseñas de usuario. La seguridad de Kerberos descansa en la seguridad de varios servidores de autenticación.

b.1 Funcionamiento : Cada usuario y cada servidor tendrán una llave, y Kerberos tiene una base de datos que las contendrá a todas. En el caso de ser de un usuario, su llave será derivada de su contraseña y estará cifrada, mientras que en el caso del servidor, la llave se generará aleatoriamente. Los servicios de red que requieren autenticación y los usuarios que requieran estos servicios, se deben registrar con Kerberos. Las llaves privadas se negocian cuando se registran. Como Kerberos sabe todas las llaves privadas, puede crear mensajes que convenzan a un servidor de que un usuario es realmente quien dice ser y viceversa. La otra función de Kerberos es generar las llamadas llaves de sesión, que serán compartidas entre un cliente y un servidor, y nadie más. La llave de sesión podrá ser usada para cifrar mensajes que serán intercambiados entre ambas partes. El almacenamiento de la base de datos y la generación de llaves, se lleva a cabo en un servidor que se denomina Servidor de Autenticación (AS por las siglas en inglés de Authentication Server).

b.2 Niveles de protección: Kerberos provee tres niveles distintos de protección. El programador de la aplicación determinará cual es apropiado, de acuerdo a los requerimientos de la aplicación.

Autenticación: Prueba que el usuario es quien dice ser. Puede ser que la autenticidad se establezca al inicio de la conexión de red y luego se asuma que los siguientes mensajes de una dirección de red determinada se originan desde la parte autenticada.

Integridad de datos: Asegura que los datos no se modifican en tránsito. Se requiere autenticación de cada mensaje, sin importar el contenido del mismo. Éstos se denominan mensajes seguros.

Privacidad de datos: Asegura que los datos no son leídos en tránsito. En este caso no sólo se autentica cada mensaje sino que también se cifra. Éstos son mensajes privados.

c. Protocolo de Transacción Electrónica Segura

Conocido como SET (Secure Electronic Transactions), protocolo creado para proporcionar mayor seguridad a los pagos on-line con tarjetas de crédito verificando la identidad de los titulares de las tarjetas con "certificados digitales" y cifrando los números de las tarjetas durante todo el trayecto, desde el navegante, el vendedor y el centro de proceso de datos. Este estándar ha sido creado por VISA y Master Card y tiene un amplio apoyo de la comunidad bancaria mundial.

En el proyecto SET participan actualmente empresas como IBM, Microsoft, Netscape, RSA, Verisign y otras, y se esperan nuevas incorporaciones. SET busca un entorno seguro para el comercio en Internet, a base de autentificar a todas las partes implicadas en la compra mediante certificados digitales y autoridades certificadoras,

emplea diversos algoritmos criptográficos para garantizar la seguridad de la transacción.

Los objetivos del SET son de, proporcionar la autentificación necesaria entre compradores, comerciantes e instituciones financieras. Garantizar la confidencialidad de la información sensible (número de tarjeta o cuenta, fecha de caducidad, etc.). Preservar la integridad de la información que contiene tanto la orden de pedido como las instrucciones de pago. Definir los algoritmos criptográficos y protocolos necesarios para los servicios anteriores.

Para poder realizar pagos mediante el protocolo SET es necesario que el comprador disponga de una cartera electrónica (Wallet), que puede descargarse de forma On-Line, la cual deberá llenar con los certificados SET de las tarjetas que vaya a utilizar para realizar los pagos. Estos certificados también pueden ser descargados de forma On-Line, en la figura 5.1.1 encontramos el esquema de transacción SET que a continuación vamos ha describir.

c.1 Esquema de transacción SET

1. El titular haciendo uso de su wallet se conecta con el servidor de comercio que dispone del Payment Server y le envía los datos necesarios para realizar la compra.

2. El comercio envía a la pasarela de pagos los datos necesarios para llevar a cabo el cobro de la transacción iniciada por el titular.

3. La pasarela de pagos descifra los datos que previamente han cifrado comercio y titular y compone un mensaje que envía a través de las redes bancarias tradicionales para la autorización de la transacción.

4. El banco del titular procede a autorizar la transacción.

5. El banco del comercio procede a abonar en su cuenta el importe de la transacción.

d. Seguridad del protocolo de Internet (IPSec)

IPSec es un grupo de extensiones de la familia del protocolo IP. Provee servicios criptográficos de seguridad. Estos servicios permiten la autenticación, integridad, control de acceso, y confidencialidad. IPSec provee servicios similares a SSL, pero a nivel de redes, de un modo que es completamente transparente para sus aplicaciones y mucho más robusto. Es transparente porque sus aplicaciones no necesitan tener ningún conocimiento de IPSec para poder usarlo. Se pueden crear túneles cifrados (VPN), o simple cifrado entre computadoras. Se puede usar como túnel de tráfico para conexiones de redes privadas virtuales (VPN, *Virtual Private Networks*). Sin embargo, su utilidad va más allá de las VPN. Con un registro central de "intercambio de claves de Internet" (IKE, *Internet Key Exchange*), cada máquina en Internet podría comunicarse con otra y usar cifrado y autenticación de alto grado.

d.1 Servicios del IPSec: El protocolo de Internet, IP, también conocido como IPv4, no provee por sí mismo de ninguna protección a las transferencias de datos. Ni siquiera puede garantizar que el remitente sea quien dice ser. IPSec intenta remediarlo. Estos servicios vienen tratados como dos servicios distintos y ofrece soporte para ambos de un modo uniforme.

Confidencialidad: Es necesario asegurarse de que los datos enviados sean difíciles de comprender para todos excepto para el receptor, que nadie pueda leer las contraseñas cuando se ingresa en una máquina remota a través de Internet.

Integridad: Hay que garantizar que los datos no puedan ser cambiados durante el trayecto. Si alguien se encuentra en una línea que lleve datos sobre facturación, querrá estar seguro de que las cantidades y cifras de contabilidad son las correctas, y que no han podido ser alteradas durante el tránsito.

Autenticidad: Los datos deben firmarse para que otros puedan verificar quién es realmente quien los ha enviado.

Protección a la réplica: Necesitamos modos para asegurarnos de que una transacción sólo se puede llevar a cabo una vez, a menos que autoricemos que la repitan. Nadie debería poder grabar una transacción, y luego replicarla al pie de la letra con el propósito de hacer que parezca como si se hubieran recibido múltiples transacciones del remitente original.

d.2 Protocolos que conforman IPSec: IPSec provee confidencialidad, integridad, autenticidad, y protección a la réplica a través de dos nuevos protocolos. Estos protocolos se llaman "Cabecera de Autenticación" (AH, *Authentication Header*) y Carga Útil de Seguridad Encapsulada (ESP, *Encapsulated Security Payload*).

AH: Provee auntenticación, integridad, y protección a la réplica (pero no confidencialidad). Su principal diferencia con ESP es que AH también asegura partes de la cabecera IP del paquete (como las direcciones de origen o destino).

ESP: Proveer autenticación, integridad, protección a la réplica, y confidencialidad de los datos (asegura todo lo que sigue a la cabecera en el paquete). La protección a la réplica requiere autenticación e integridad (estas dos van siempre juntas). La confidencialidad (cifrado) se puede usar con o sin autenticación y/o integridad. Del mismo modo, se puede usar la autenticación y/o la integridad con o sin la confidencialidad.

e. Protocolo SOCKS

El uso de cortafugos ha permitido separar estructuras de redes internas del exterior de la misma. Muchos de estos cortafuegos no son equipos fisicos sino aplicaciones que

actúan sobre la capa de aplicación del modelo OSI, actuando como proxy entre las computadoras que se comunican entre sí. El protocolo SOCKS fue creado para satisfacer esta necesidad que cada vez era mayor, permitiendo una mejor autentificación entre computadores dentro de un entorno (Cliente – Servidor) y logrando así un mejor y mas fuerte control sobre el acceso. SOCKS es un sistema Proxy equipado con seguridad, auditoria, administración, tolerancia a fallas y notificación de alarmas. Generalmente la aplicación cliente envía la petición al servidor SOCKS, con la dirección de la computadora destino, el tipo de conexión, y la identidad del usuario. SOCKS 5 realiza cuatros operaciones básicas que son negociacion, autentificación, petición de conexión, establecimiento del circuito, reenvió de datos. Incluye el protocolo TCP, también soporta UDP y el formato de direcciones IP V6.

f. Protocolo Secure Sockets Layer (SSL)

Para la transmisión de información confidencial a través de la red utilizaremos el protocolo SSL. El objetivo de SSL es proporcionar autenticación tanto del servidor como del cliente y asegurar la confidencialidad en la comunicación cliente-servidor. La comunicación entre el cliente y el servidor se produce de la siguiente manera:

f.1 Saludo del cliente: tiene por objetivo informar al servidor de los algoritmos de criptografía y compresión que soporta y solicitar el certificado del servidor para verificar su identidad.

f.2 Saludo del servidor: responde al cliente enviando su llave pública del certificado y el conjunto de algoritmos de criptografía y compresión que se van a usar. En algunas situaciones el servidor puede requerir la identificación del cliente mediante su llave pública.

f.3 Aprobación del cliente: El cliente verifica la validez del identificador digital o certificado enviado por el servidor. Para ello desencripta el certificado utilizando la llave pública del servidor y determinando si este proviene de una entidad certificadora de confianza. Después hace una serie de verificaciones sobre el certificado, tales como la fecha, URL del servidor. Una vez verificada la autenticidad del servidor el cliente genera una llave aleatoria y la cifra con la llave pública del servidor y el algoritmo criptográfico y de compresión seleccionado anteriormente. Esta llave se envía al servidor y será utilizada para el envío de mensajes entre ambos.

f.4 Verificación: Ambas partes conocen la llave secreta que van a utilizar para el envío de mensajes. Es importante tener en cuenta que esta llave tan solo es conocida por el cliente y por el servidor. El cliente la conoce ya que la generó y el servidor porque se le ha enviado utilizando la llave pública de su certificado y es el único capaz de descifrarla, ya que solo es posible con la llave privada que tan solo conoce él. Para comprobar que todo el proceso no ha sido alterado en ningún momento se envían una copia de la conversación cifrada con la llave secreta. Si ambos confirman que todo es correcto entonces se iniciará el intercambio de información de manera segura. De lo contrario volverían a iniciar el proceso.

f.5 Intercambio de información: A partir de este momento toda la información que intercambien cliente y servidor estará cifrada con la llave secreta y, por tanto solo podrán descifrarla y leerla ellos.

f.6 Fin de la conexión segura: cuando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiendo que la comunicación no es segura y confirma que el cliente efectivamente desea abandonar la sesión SSL.

5.1.3 Redes privadas virtuales VPN

a. Definición

El uso de Internet por parte de las entidades financieras está llevando a nuevas formas de comunicación y de gestión de la información. Las redes privadas virtuales (del término inglés Virtual Private Network, VPN), consiste en dos máquinas (una en cada "extremo" de la conexión, ver figura 30) y una ruta o "túnel" que se crea dinámicamente en una red pública o privada. Para asegurar la privacidad de esta conexión los datos transmitidos entre ambas máquinas son cifrados por el Point-to-Point protocol (PPP), un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN) por un dispositivo PPTP. Una Red Privada Virtual es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones geográficas. Es una red de datos de gran seguridad que permite la transmisión de información confidencial entre la entidad financiera y sus sucursales, proveedores, distribuidores, empleados y clientes, utilizando Internet como medio de transmisión. Aunque Internet es una red pública y abierta, la transmisión de los datos se realiza a través de la creación de túneles virtuales, asegurando la confidencialidad e integridad de los datos transmitidos.

Así, las VPNs constituyen una combinación entre la seguridad y garantía que ofrecen las costosas redes privadas y el gran alcance, lo asequible y escalable del acceso a través de Internet. Esta combinación hace de las VPNs una infraestructura confiable y de bajo costo que satisface las necesidades de comunicación de cualquier entidad financiera. Las VPNs permiten:

La administración y ampliación de la red corporativa al mejor costo-beneficio.

La facilidad y seguridad para los usuarios remotos de conectarse a las redes corporativas de la entidad financiera.

Los requisitos indispensables para esta interconectividad son:

Políticas de Seguridad.

Requerimiento de aplicaciones en tiempo real.

Compartir Datos, aplicaciones y recursos.

Servidor de Acceso y Autenticación.

Aplicación de Autenticación.

b. Protocolos que Utiliza una VPN

b.1 Protocolo punto a punto (PPP): El PPP fue diseñado para enviar datos a través de conexiones de punto a punto de marcación o dedicadas. El PPP encapsula paquetes de IP, IPX, y NetBEUI dentro de las tramas del PPP, y después los transmite a través de un enlace de punto a punto.

b.2 Protocolo de túnel punto a punto (PPTP): El PPTP es un protocolo de nivel de enlace del modelo de referencia OSI, encapsula las tramas de PPP (protocolo punto a punto) en datagramas de IP las cuales van a ser transmitidas a través de una red interna de IP, como Internet. El protocolo de túnel de punto a punto (PPTP) utiliza una conexión de TCP para el mantenimiento del túnel y las tramas de PPP encapsuladas con encapsulación de enrutamiento genérico (GRE) destinadas a los datos en el túnel. Las cargas de pago de las tramas de PPP encapsuladas pueden codificarse y/o comprimirse. También proporcionan autenticación de usuario, control de acceso y la oportunidad de aplicar perfiles de acceso telefónico para restringir cuidadosamente el uso de ciertos tipos de acceso remoto por parte de usuarios

específicos. PPTP proporciona al cliente remoto una configuración de dirección interna, de modo que pueden participar en la red interna como si estuvieran conectados directamente. PPTP ofrece compresión y opciones de cifrado RC4 estándar y seguro (una llave de secuencia simétrica) para el tráfico que es llevado al interior del túnel.

b.3 Transmisión de nivel 2 (L2F): Es un protocolo de transmisión que permite a los servidores de acceso por marcación estructurar el tráfico de marcación en un PPP y transmitirlo a través de enlaces WAN a un servidor L2F. Después, el servidor L2F "abre" los paquetes y los transmite a través de la red. A diferencia del PPTP y del L2TP, el L2F no tiene un cliente definido. Asimismo, el L2F sólo funciona en túneles obligatorios.

b.4 Protocolo de tunneling de nivel 2 (L2TP): Este es un protocolo de red que encapsula las tramas de PPP para enviarlas a través de redes de IP, X.25, Relé de trama o de modo de transferencia asíncrona (ATM). Cuando se configura para utilizar el IP y su transporte de datagrama, el L2TP puede utilizarse como un protocolo de túnel a través de Internet. El L2TP a través de redes internas de IP utiliza el UDP y una serie de mensajes L2TP para mantener el túnel. El L2TP también utiliza al UDP para enviar tramas de PPP encapsuladas L2TP como los datos en el túnel. Las cargas de pago de las tramas de PPP encapsuladas pueden codificarse y/o comprimirse.

c. Requerimientos Básicos de una VPN

Por lo general, cuando se desea implantar una VPN hay que asegurarse de que esta proporcione lo siguiente:

c.1 Autenticación del usuario: La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Asimismo, debe proporcionar registros de auditoria y contabilidad que muestren quién acceso, qué información y cuándo.

c.2 Administración de direcciones: La VPN debe establecer una dirección de cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

c.3 Codificación de datos: Los datos que se van a transmitir a través de la red pública deben ser previamente cifrados para que no puedan ser leídos por clientes no autorizados de la red.

c.4 Administración de llaves: La VPN debe generar y renovar las llaves de codificación para el cliente y el servidor.

c.5 Soporte a protocolos múltiples: La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet (IPX), entre otros.

5.1.4 Cortafugos (Firewalls) y proxies

a. ¿Qué es un cortafuegos?

Un Cortafuegos o Firewall es un sistema o grupo de sistemas que hace cumplir una política de control de acceso entre dos redes. Se utiliza para proteger la red interna (red local). Lo que hace el cortafuegos es cortar o dejar pasar los intentos de comunicación que tiene todo el mundo (Internet) hacia nuestro computador o hacia nuestra red, según la situación del cortafuegos. El cortafuegos también puede controlar el tráfico generado desde nuestro computador o red hacia Internet. El cortafuegos actúa a base de normas que establece el administrador de seguridad o en

su defecto el administrador de red, o bien el usuario final. Estas reglas definen lo que tiene que hacer el cortafuegos cuando encuentre un paquete que cumpla las características que nosotros le digamos. Aquí es donde se diferencian la mayoría de cortafuegos.

Para poder entender mejor el tipo de políticas (reglas) que se podrían definir en el cortafuegos serían necesarios conocimientos de protocolos, por lo menos de la estructuración de niveles del modelo de referencia OSI. La mayoría de cortafuegos personales nos permiten filtrar tramas creando reglas de nivel 3 (IP), 4 (TCP/UDP) ó 7 (Aplicaciones). Por ejemplo, podríamos definir una regla que no dejara pasar ningún paquete proveniente de Internet, cuyo destino fuese nuestro computador y, más concretamente, el puerto 80 (HTTP) de nuestro computador.

b. ¿Qué es un proxy?

Un Proxy es un programa (trabajando en el nivel de aplicación de OSI) que permite o niega el acceso a una aplicación determinada entre dos redes. Hace de intermediario entre los usuarios, normalmente de una red local, e Internet. Lo que hace realmente un Proxy es recibir peticiones de usuarios y redirigirlas a Internet. La ventaja que presenta es que con una única conexión a Internet podemos conectar varios usuarios. Normalmente, un Proxy es a su vez un servidor de caché. La función de la caché es almacenar las páginas Web a las que se accede más asiduamente en una memoria. Así cuando un usuario quiere acceder a Internet, accede a través del Proxy, que mirará en la caché a ver si tiene la página a la cual quiere acceder el usuario. Si es así le devolverá la página de la caché y si no, será el Proxy el que acceda a Internet, obtenga la página y la envíe al usuario. Con la caché se aceleran en gran medida los accesos a Internet, sobre todo si los usuarios suelen acceder a las mismas páginas.

El Proxy es "transparente" al usuario, lo pongo entrecomillado porque el usuario tendrá que configurar su navegador diciéndole que accede a Internet a través de un Proxy (deberá indicar la dirección IP del proxy y el puerto por el que accede), pero una vez realizado esto, el usuario actuará de la misma manera que si accediera directamente a Internet. Los últimos Proxies que han aparecido en el mercado realizan además funciones de filtrado, como por ejemplo, dejar que un usuario determinado acceda a unas determinadas páginas de Internet o que no acceda a ninguna. Con esta función podemos configurar una red local en la que hayan usuarios a los que se les permita salir a Internet, otros a los que se les permita enviar correo, pero no salir a Internet y otros que no tengan acceso a Internet. Esta característica muchas veces hace que se confundan con un cortafuegos.

Los proxies se clasifican según la aplicación de trabajo y estos son: Proxy WWW, Proxy http (servidor con caché, soporta peticiones HTTP, FTP y SSL), proxy FTP (proporciona acceso a servidores FTP), proxy POP3 (permite el acceso a servidores POP3 de Internet para recoger correo electrónico), proxy RealAudio (permite escuchar ficheros de servidores RealAudio),

c. Diferencias entre un cotafuegos y un proxy

El cotafugos (firewall) y el proxy son diferentes, pero deberían estar siempre combinados. El firewall sin embargo, es únicamente un método de protección de la red local o de un computador personal, con el que podemos cerrar o dejar abiertos ciertos puertos, IPs, aplicaciones, etc. El Proxy se usa para redirigir las peticiones que recibe de varios usuarios a Internet de forma transparente y se encarga de

devolverles las respuestas (las páginas Web). También se puede utilizar para FTP, POP3, SMTP, IMAP, TELNET, etc.

## 5.2 Criptografía

### 5.2.1 Definición

La tecnología utilizada para mantener confidencialidad de datos y comunicaciones se llama criptología (es una técnica heurística). La técnica heurística es el método de resolver operaciones matemáticas complejas, utilizando exploración y métodos de ensayo y error las cuales se aplican a los datos cuya confidencialidad se desea mantener. Las raíces etimológicas de la palabra criptología son Kriptós, que significa oculto y logías, que se traduce como estudio, ciencia. Tiene dos componentes criptografía y criptoanálisis:

a. Criptografía: Es la técnica de transformar los datos inteligible, denominado texto en claro (plaintext o cleartext), en otro que sólo puedan entender las personas autorizadas a ello, que llamarenos criptograma o texto cifrado. Las raíces etimológicas de la palabra critografía son Kriptós, que significa oculto y Graphos, que se traduce como escribir.

b. Criptoanálisis: Es la ciencia de determinar la llave (analizan los métodos de cifrado) o descifrar los datos sin conocer la llave con el objetivo de encontrar una debilidad, es decir, realizar una especie de criptografía inversa. Las raíces etimológicas de la palabra critoanálisis son Kriptós, que significa oculto y Análisis, se traduce como descomposición.

La base de la Criptografía es la aplicación de problemas matemáticos de difícil solución a aplicaciones específicas, denominándose criptosistema o sistema de

cifrado (encriptado) a los fundamentos y procedimientos de operación involucrados en dicha aplicación.

5.2.2 Llaves criptográficas

Entre ellas tenemos a las llaves secreta, pública y privada.

a. La llave secreta: Es el código básico de cifrado (encriptación), se utiliza para poner en claro un datagrama. Lo necesitan tanto el emisor como el receptor en los algoritmos simétricos.

b. La llave pública: Es un tipo de llave que es propia de cada usuario y que es necesaria para enviarle un datagrama, deben de estar disponibles en un directorio público electrónico residente en un servidor.

c. La llave privada: Solamente la conoce su dueño, es necesaria para descifrar (desencriptar) los mensajes que le envían cifrados con su llave pública.

5.2.3 Algoritmos criptográficos simétricos

Para que un algoritmo de este tipo sea considerado fiable debe cumplir los siguientes requisitos básicos: Conocido el criptograma (texto cifrado) no se pueden obtener de él ni el texto en claro ni la llave. Conocidos el texto en claro y el texto cifrado debe resultar más caro en tiempo o dinero descifrar la llave que el valor posible de la información obtenida por terceros. Las limitaciones de la criptografía Simétrica es la autenticación (si se deduce la llave se podría descifrar los datos), el cambio de llave (origina distribuir esa nueva llave a todos los usuarios que deseemos comunicarnos por algún medio electrónico ó físico para distribuir esa nueva llave) y la dificultad de almacenar y proteger muchas llaves diferentes.

Todos los sistemas criptográficos clásicos se pueden considerar simétricos, y los principales algoritmos simétricos actuales son DES, TDES, IDEA SAFER, y BLOWFISH. Actualmente se está llevando a cabo un proceso de selección para establecer un sistema simétrico estándar, que se llamará AES (Advanced Encryption Standart), que se quiere que sea el nuevo sistema que se adopte a nivel mundial, y el algoritmo que utilice se denominará AEA (Advanced Encryption Algorithm), ver figura 5.2.3.

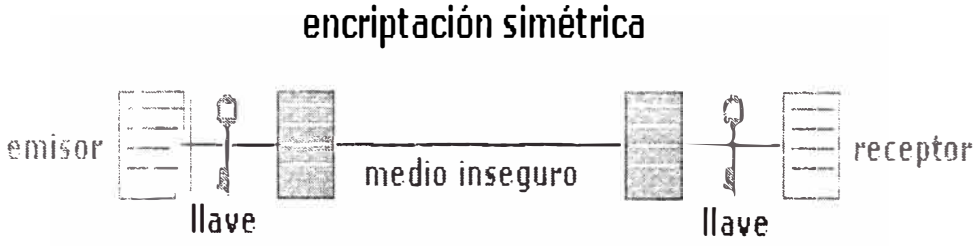



***Fig.5.2.3 Encriptación simétrica.***

a. Norma de cifrado de datos (DES): Es el más estudiado y utilizado de los algoritmos de llave simétrica, fue diseñado por IBM y utilizado desde los años 70. Es un método de cifrado altamente resistente frente ataques criptoanalíticos diferenciales (utiliza los conceptos de transposición y sustitución), Su tamaño de llave (56 bits) la hace vulnerable a ataques de fuerza bruta. El algoritmo cifra bloques de información de 64 bits con una llave de 56 bits, realmente la llave inicial es de 64 bits, pero los bits menos significativos de cada byte se utilizan como bits de paridad, por ello se pueden eliminar al no aportar ninguna información adicional, por lo que nos queda la llave de 56 bits. Dependiendo de la naturaleza de la aplicación DES tiene 4 modos de operación para poder implementarse: ECB (Electronic Codebook Mode) para mensajes cortos, de menos de 64 bits, CBC (Cipher Block Chaining Mode) para mensajes largos, CFB (Cipher Block Feedback) para cifrar bit por bit ó

byte por byte y el OFB (Output Feedback Mode) el mismo uso pero evitando propagación de error.

b. Triple Norma de cifrado de datos (TDES): Una mejora del algoritmo DES, que siempre había sido muy criticado debido a la pequeña longitud de la llave, es Triple-DES. Con este procedimiento, el mensaje es cifrado tres veces. Existen varias implementaciones:

b.1 DES-EEE3: Se cifra tres veces con una clave diferente cada vez.

b.2 DES-EDE3: Primero se cifra, luego se descifra y por último se vuelve a cifrar, cada vez con una clave diferente.

b.3 DES-EEE2 y DES-EDE2: Similares a los anteriores con la salvedad de que la llave usada en el primer y en el último paso coinciden.

Se estima que las dos primeras implementaciones, con llaves diferentes, son las más seguras, como podemos ver en la figura 5.2.

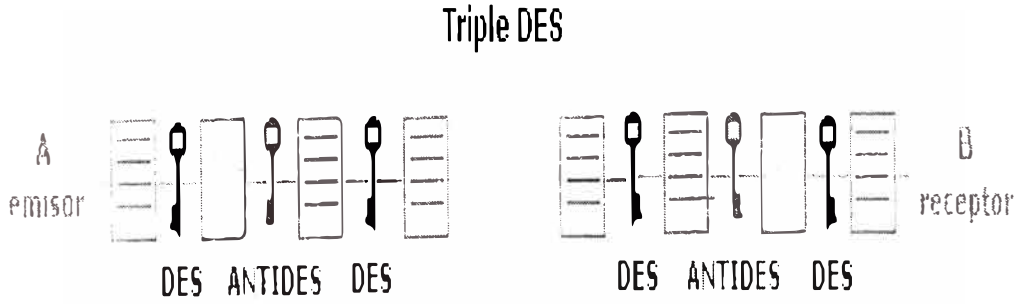



***Fig.5.2 Triple DES.***

c. IDEA (International Data Encription Algorithm): Ha sido desarrollado por Xuejia Lay y James Massey. Utiliza llave de 128 bits y es resistente al criptoanálisis. Se encuentra bajo patente de Ascom-Tech, Este algoritmo es de libre difusión y no está

sometido a ningún tipo de restricciones, por lo que se ha difundido ámpliamente, utilizándose en sistemas como UNÍX y en programas de cifrado de correo como PGP (programa Pret ty Good Privacy).

d. SAFER: Es un algoritmo diseñado por Robert Massey. Tiene llaves de hasta 128 bits y, a pesar de algunas debilidades en la primera versión y de ciertos ataques, parece un algoritmo seguro. Este programa fue desarrollado para la empresa Cylink, que algunos relacionan con la Agencia de Seguridad Nacional Norteamericana (NSA).

e. Blowfish: Fue creado por Bruce Schneier, utiliza llaves de hasta 448 bits y, hasta el momento, ha resistido con éxito todos los ataques. Por ello y por su estructura se le considera uno de los algoritmos más seguros, a pesar de lo cual no se utiliza masivamente.

Como futuro estándar del algoritmo simétrico se denominará Rijndael, creado por los belgas Vincent Rijmen y Joan Daemen. Rijndael es un cifrador de bloque que opera con bloques y llaves de longitudes variables, que pueden ser especificadas independientemente a 128, 192 ó 256 bits. El resultado intermedio del cifrado se denomina Estado, que puede representarse como una matriz de bytes de cuatro filas.

5.2.4 Algoritmos Criptográficos Asimétricos

También se les llama algoritmo de llave pública. La criptografía asimétrica es por definición aquella que utiliza dos llaves diferentes para cada usuario, una para cifrar que se le llama llave pública y otra para descifrar que es la llave privada. La criptografía de

llave pública es una importante tecnología para las aplicaciones de comercio electrónico, intranet, extranet y otras aplicaciones Web. Sin embargo, para poder

beneficiarse de la tecnología de llave pública, es necesario una infraestructura de llave pública (PKI) que la soporte.

La ventaja de los algoritmos de llave pública es que eliminan la necesidad que tienen los algoritmos simétricos de tener un secreto compartido entre los usuarios que desean usar un sistema criptográfico. La principal desventaja es que son más costosos temporalmente. Mientras que en los algoritmos simétricos la generación de la llave puede ser aleatoria, en los asimétricos (llave pública) debe hacerse siguiendo un procedimiento determinado debido a la relación existente entre las dos llaves.

Las tres aplicaciones principales de los algoritmos de llave pública son el cifrado de mensajes, la firma digital y el intercambio de llaves, como podemos ver en la figura 5.3.

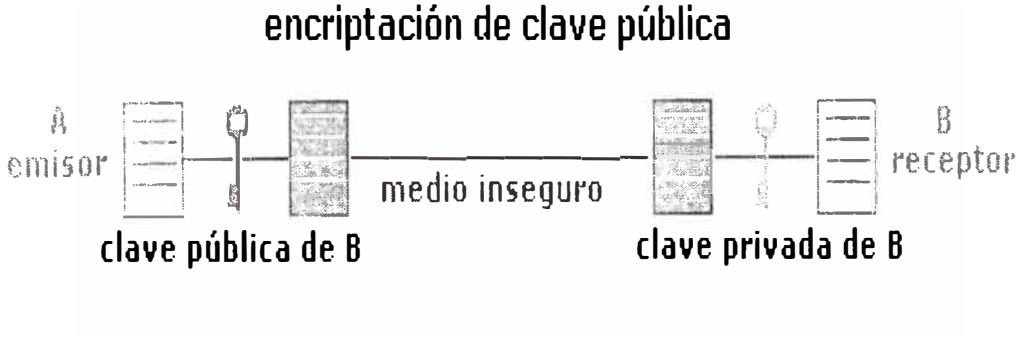



***Fig.5.3 Encriptación de clave pública.***

a. El cifrado de mensajes: Se realiza cifrando el mensaje con la llave pública y descifrándolo con la llave privada correspondiente. Otra posible forma de cifrar un mensaje es combinar un algoritmo de llave privada con uno de llave pública. Se utiliza el algoritmo de llave secreta para cifrar el mensaje y el de llave pública para transmitir la llave secreta utilizada. Así se alivia parte del alto coste computacional provocado por el cifrado mediante llave pública.

b. La firma de mensajes: Consiste en aplicar una función hash sobre el mensaje original, y cifrar el resultado mediante la llave privada. El resultado de esta operación es la firma. Para comprobarla lo que se hace es aplicar la misma función hash sobre el mensaje y compararla con el resultado de descifrar la firma usando la llave privada.

c. Intercambio de llaves: Consiste en utilizar algún algoritmo de llave pública para negociar una llave privada entre dos partes.

Los tres algoritmos de llave pública más relevantes son:

a. Rivest Shamir y Adleman (RSA): Es un Algoritmo que utiliza llaves de cualquier longitud, aunque actualmente de 1024 bits consideradas lo bastante largas como para resistir ataques de fuerza bruta. Su seguridad se basa en la dificultad de factorizar números primos de gran tamaño. No fué sino hasta 1978 que Rivest, Shamir y Adleman patentan y publican el método más popular, el RSA.

b. Diffie-Hellman (DH): Este algoritmo de cifrado de Whitfield Diffie y Martin Hellman es el punto de partida para los sistema asimétricos, basados en dos llaves diferentes, la pública y la privada. En la práctica sólo es válido para el intercambio de llaves simétricas, y con esta funcionalidad es muy usado en los diferentes sistemas seguros implementados en Internet, como SSL (Secure Socket Layer) y VPN (Virtual Private Network).

c. Digital Signature Algorithm DSA: Este algoritmo fue propuesto en 1,991 por el NIST (National Institute of Standards and Technology) para ser usado en su estándar para firma digital, el Digital Signature Standard DSS. Su uso está limitado a la firma

digital de mensajes. Se basa en la dificultad computacional del problema del logaritmo discreto.

## 5.3 Aplicación de tecnologia de encriptación

El avance de la Tecnología, fundamentalmente en lo que a Comunicaciones electrónicas e Información electrónica se refiere y a las nuevas tecnologías como firma digital, certificados digitales y la infraestructura de llave pública, se aplican cada día más en las empresas, entidades financieras que tienden fundamentalmente al incremento de la Eficiencia, la Eficacia, y al ahorro de Costos.

5.3.1 Firma Digital

a. Definición

La firma digital es un bloque de caracteres que acompaña a un mensaje o fichero acreditando quién es su emisor (autenticación) y que no ha existido ninguna modificación de los datos (integridad). Para firmar un documento digital, el emisor utiliza su propia llave privada (sistema criptográfico asimétrico), a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría (no revocación). De esta forma, el emisor queda vinculado al texto de la firma. Por último la validez de dicha firma podrá ser comprobada por cualquier usuario que disponga de la llave pública del emisor. En la Figura 5.3.1, se encuentra el esquema básico de una firma digital, en la cual se realiza de la siguiente manera:

El software del emisor (firmante) aplica un algoritmo hash sobre el texto del mensaje a firmar (algoritmo matemático unidireccional, es decir, lo cifrado no se puede descifrar), obteniendo un extracto de longitud fija (según el algoritmo utilizado oscila entre 128 y 160 bits), y absolutamente específico para ese texto. Se somete a

continuación al cifrado mediante la llave privada del emisor. De esta forma obtenemos un extracto final cifrado con la llave privada del emisor el cual se añadirá al final del texto para que se pueda verificar la autoría e integridad del texto del mensaje por aquel usuario interesado que disponga de la llave pública del emisor.

Sin embargo, es necesario comprobar que la firma realizada es efectivamente válida. Para ello es necesario, la llave pública del emisor. El software del receptor, previa introducción en el mismo de la llave pública del emisor (obtenida a través de una autoridad de certificación), descifraría el extracto cifrado del emisor; a continuación calcularía el extracto hash que le correspondería al texto del mensaje, y si el resultado coincide con el extracto anteriormente descifrado se consideraría válida, en caso contrario significaría que el documento ha sufrido una modificación posterior y por tanto no es válido.

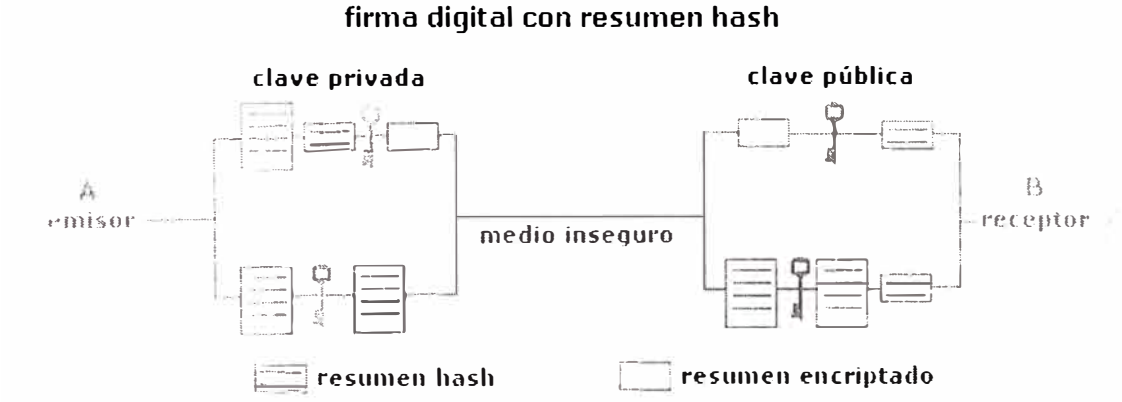



Fig.5.3.1 Firma digital.

b. Funciones Hash

Si imaginamos el envío de un texto extenso que queremos firmar digitalmente, nos daremos cuenta que cifrar el texto entero es una pérdida de tiempo, ya que los

medios de cifrado de llave pública son lentos, porque precisan un gras proceso de cómputo. Para solventar éste aspecto aparecen las funciones hash, que son unas funciones matemáticas que realizan un resumen del texto a firmar. Su forma de operar es comprimir el texto en un único bloque de longitud fija, bloque cuyo contenido es ilegible y no tiene ningún sentido real. Tanto es así que por definición las funciones hash son irreversibles, es decir, que a partir de un bloque comprimido no se puede obtener el bloque sin comprimir, y si no es así no es una función hash. Estas funciones son además de dominio público. A un texto del mensaje resumido mediante una función hash y cifrado con una llave privada es lo que en la vida real se denomina firma digital. Las funciones hash y la firma digital son elementos indispensables para el establecimiento de canales seguros de comunicación, basados en los Certificados Digitales.

c. Algoritmos Hash

Los algoritmos hash más conocidas y usadas son:

c.1 Message Digest 5 (MD5): Desarrollado por Ron Rivest, y ha sido ámpliamante usado como autenticador de mensajes en el protocolo secure sockets layer (SSL) y como firmador de texto de mensajes en el programa de correo Pretty Good Privacy (PGP).

c.2 Secure Hash Algorithm (SHA-1): Desarrollado como parte integrante del Secure Hash Standar (SHS) y el Digital Signature Standar (DSS) por la Agencia de Seguridad Nacional Norteamericana, NSA. Es muy utilizada en el algoritmo de firma, como en el programa PGP en sus nuevas llaves DH/DSS (Diffie-Hellman/Digital Signature Standar).

c.3 RIPEMD-160: Desarrollada por un grupo de investigadores europeos, entre los que se encuentra Hans Dobbertin. Maneja llaves normalmente de 160 bits, aunque existen versiones de 128 y se están planteando nuevas de 256 y 320 bits. Es muy rápido, no está patentado y su código fuente es abierto, de libre acceso.

5.3.2 Certificado Digital

Debido al creciente auge en el uso de Internet para aplicaciones como el correo y el comercio electrónico, aparece la necesidad de ofrecer nuevos servicios a las empresas y entidades financieras (usuarios). Estos nuevos servicios deben proporcionar al usuario confianza al utilizar estas aplicaciones. Para ofrecer esta confianza aparecen los certificados digitales o electrónicos.

Los certificados digitales son elementos que permiten identificar las partes intervinientes en una transacción telemática. Así mismo y gracias a sus funcionalidades y características, permiten el proteger la información intercambiada mediante mecanismos de cifrado y ofrecen el soporte necesario para implementar firma electrónica, los certificados contienen además la siguiente información:

a. Un identificador del propietario del certificado, que consta de su nombre, sus apellidos, su dirección e-mail, datos de su empresa como el nombre de la organización, departamento, localidad, provincia y país, etc.

b. Otro identificador de quién asegura su validez, que será una Autoridad de Certificación.

c. Dos fechas, una de inicio y otra de fin del período de validez del certificado, es decir, cuándo un certificado empieza a ser válido y cuándo deja de serlo, fecha a

partir de la cual la clave pública que se incluye en él, no debe utilizarse para cifrar o firmar.

d. Un identificador del certificado o número de serie, que será único para cada certificado emitido por una misma Autoridad de Certificación. Esto es, identificará inequívocamente a un certificado frente a todos los certificados de esa Autoridad de Certificación.

e. Firma de la Autoridad de Certificación de todos los campos del certificado que asegura la autenticidad del mismo.

Para que las entidades financieras y bancos estén completamente seguros de cualquier transacción electrónica es necesario utilizar, al menos dos tipos de certificados, uno general para comunicaciones seguras (X.509) y otro especifico para transacciones económicas (SET). Además de servir como mecanismo confiable y seguro de identificación en la red, el certificado de identidad digital le permite enviar y recibir información confidencial, asegurándose que sólo el remitente pueda leer el mensaje enviado; puede acceder a sitios Web de manera segura con su identidad digital, sin tener que usar el peligroso mecanismo de contraseña; puede firmar digitalmente documentos, garantizando la integridad del contenido y autoría del documento; y todas aquellas aplicaciones en que se necesiten mecanismos seguros para garantizar la identidad de las partes y confidencialidad e integridad de la información intercambiada, como comercio electrónico, declaración de impuestos, pagos provisionales, uso en la banca. Ver figura 5.3.2.

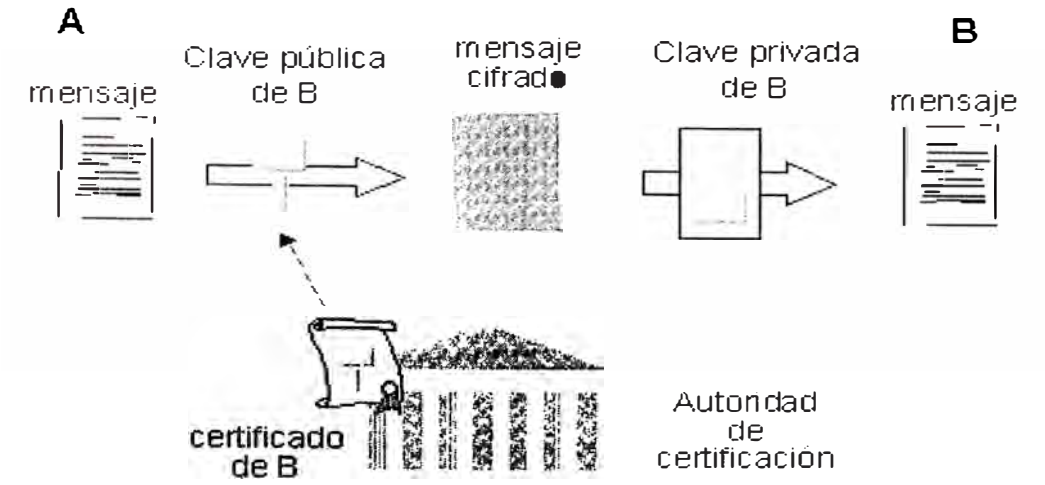



Fig.5.3.2 Certificado Digital.

5.3.3 Infraestructura de llave pública PKI

a. Definición

La infraestructura de llave pública (Public Key Infrastructure PKI) es la infraestructura técnica, legal y comercial que permite el amplio despliegue de la tecnología de llaves públicas y se usa para crear firmas digitales y para gestionar llaves simétricas.

El objetivo de la infraestructura PKI es dotar de los mecanismos básicos de seguridad para mantener la integridad del negocio, la disponibilidad del s e rvicio y la confidencialidad del cliente para, en última instancia, generar confianza.

La autentificación de la clave pública es un requisito indispensable y, por este motivo, las llaves públicas se almacenan en certificados de llaves públicas. Un certificado contiene la llave pública y sus datos identificativos, y una Autoridad de Certificación (CA) que certifica que el propietario de una llave pública es quien realmente dice ser.

b. Componentes de una PKI

En una PKI encontramos dos tipos de componentes principales: las autoridades certificadoras (Certificate Authority CA) y las entidades finales. En algunos casos puede aparecer un tercer tipo de componentes, que son la autoridades de registro (RA). A continuación describiremos los componentes mencionados:

b.1 Autoridad de certificación (Certificate Authority CA): Las CA son entidades capaces de certificar la correspondencia entre una entidad y una llave pública. Para ello deben ofrecer un grado de seguridad que haga que el usuario pueda depositar su confianza en ellas. Cuando un usuario confía en una CA considera que todos los certificados emitidos por la misma son auténticos y correctos.

b.2 Usuario final: Representan al usuario del PKI, utilizan los servicios ofrecidos por las CA para poder obtener las posibilidades que ofrece la criptografía de llave pública. El Usuario no debe de realizar ninguna función de gestión de los certificados. Son simples usuarios, que obtienen los certificados desde una CA y los utilizan. Sí deben tener la posibilidad de almacenar los certificados, para no tener que obtenerlos cada vez que los necesiten. En cuanto a las llaves sí deben ofrecer varias posibilidades. Por una parte, en algunos casos es más interesante la generación de la llave en la entidad final que en la CA. Por otra parte es necesario que las llaves se puedan almacenar de forma segura, para mantener la seguridad de la PKI.

b.3 Autoridad de registro (Registration Authority RA): Una RA es una entidad que se comunica tanto con las entidades finales como con la CA, y que realiza funciones de autentificación de usuarios y gestión de llaves. La RA aparece como un puente entre la entidad final y la CA. Para todos los procesos relacionados con autentificación de usuarios y gestión de llaves la entidad final interactuará con la RA, mientras que para

los procedimientos relacionados con certificados interactuará directamente con la CA.

La infraestructura PKI y los certificados digitales son una herramienta fundamental para la seguridad en las entidades financieras. Permiten autenticar las identidades online y cifrar los mensajes de correo electrónico y otra información comercial confidencial a las empresas y entidades financieras que utilizan la red para realizar negocios. De este modo, se ofrece la confianza necesaria para establecer comunicaciones y realizar negocios con total seguridad en un entorno basado en Internet.

b.4 Políticas de Certificación: Deben diseñarse una serie de políticas, o procedimientos operativos, que rigen el funcionamiento de la PKI y establecen los compromisos entre la Autoridad Certificadora y los Usuarios Finales. Estos documentos tendrán un carácter tanto técnico como legal. El Proceso de Construcción de una PKI deberá siempre partir de la definición de las Políticas Operativas y contemplar como requerimiento esencial el asegurar la calidad y seguridad de las operaciones que los usuarios finales realizan con sus llaves privadas (p.e. Firma Digital de Documentos).

b.5 Publicación de Certificados: El repositorio de certificados permite a los usuarios operar entre ellos (p.e. Para la validación de una Firma Digital), y es un requisito legal que cuente con una total disponibilidad de acceso.

b.6 Soporte de la llave Privada. La elección de un buen soporte para que los usuarios custodien su llave privada es un punto esencial y complejo en si mismo (p.e. si la llave está en una SmartCard, es necesario diseñar el Sistema de Gestión de SmartCards que permita la emisión y distribución de las tarjetas a los usuarios).

b.7 Aplicaciones "PKI-Enabled": Se denomina así a las aplicaciones software capaces de operar con certificados digitales. Estas aplicaciones son las que dan el valor real de la PKI de cara al usuario.

c. Aplicaciones del PKI

c.1 Servicios financieros on-line: autenticación y transacción con firma para aplicaciones y actividades de banca electrónica y de bolsa.

c.2 Acceso a Extranets/Intranets.

c.3 Servicios estatales on-line: información de ciudadanos, registro de vehículos, declaraciones de impuestos y sanidad.

c.4 Servicios de comercio electrónico B2B y B2C: autenticación y transacción con firma para aplicaciones de comercio electrónico.

c.5 Autenticación en Servidores de Acceso Remoto.

c.6 Conexión segura a la red: en comunicaciones por correo electrónico, cifrado y firma digital.

# CAPÍTULO VI
# INGENIERÍA DEL PROYECTO

## 6.1 Objetivos

En el esquema o diseño topológico de la red para la Implementación del servicio de transmisión de datos a través del Sistema de Telefonía Celular en Empresas, en general se fundamenta en una conexión inalámbrica para 80 usuarios móviles con cobertura a nivel Nacional para realizar las siguientes tareas:

- Consultar un servidor de aplicaciones para obtener información sobre el stock de productos, lista de precios, ofertas y promociones de productos, línea de crédito del cliente, histórico de pedidos realizados por clientes etc., para los vendedores
- Conexión al servidor de correo corporativo para enviar y recibir correos para los vendedores y Gerentes
- Operación y mantenimiento de los enrrutadores y plataformas Unix para los usuarios del área técnica
- Consultas rápidas vía WAP para los vendedores
- Control y reporte diario de vigilantes de seguridad

## 6.2 Dimencionamiento de Equipos y Aplicaciones

Equipamiento

Relación de equipos relevantes.

Oficina principal

Harware y software:

- 01 Computador (PC) + Servidor de Autenticación (Servidor de Control de Acceso, ACS)
- 01 Concentrador VPN de Cisco

Usuarios Móviles:

Hardware y software

- 80 Celulares Kyocera 2135
- 80 PDA + cable para datos + software cliente del aplicativo

Se debe considerar además el alquiles de un enlace dedicado de 256 KPSS para conexión con el Operador Celular.

### 6.3 Descripción de la Red de Datos de la EMPRESA – Condición Inicial

En la figura 6.1 se muestra la topología de Red de Datos de la EMPRESA que presenta las necesidades planteadas:

La topología Inicial muestra una red con conexión a Internet y protegida por un Firewall (Firewall-1, marca Checkpoint). En el Firewall se han definido 3 zonas:

Zona Protegida<>Red Interna

Zona Intermedia<>DMZ1

Zona Peligrosa<>Internet

Red Interna, es la red local donde se encuentran los servicios de la red, PCs de escritorio de empleados y altos directivos de la empresa.

DMZ1, es la red de datos que albergan los diferentes servidores de servicio de la empresa tales como:

Servidores de Correo

Servidores WEB

Servidor de Aplicaciones

Servidores de Base de Datos

El direccionamiento IP de la EMPRESA es como sigue:

IP RED DMZ1: 10.0.1.0Mask: 255.255.255.0

IP Servidores de Correo: 10.0.1.1

IP Servidores WEB: 10.0.1.2

IP Servidor de Aplicaciones: 10.0.1.3

IP Servidores de Base de Datos: 10.0.1.4

Internet, es la red externa o red mundial a la cual esta conectada la EMPRESA, dicha conexión se efectúa a través de un enruteador Cisco 2610 que tiene 1 tiene un puerto Ethernet y 2 puertos seriales asíncrono/síncrono V35

EMPRESA

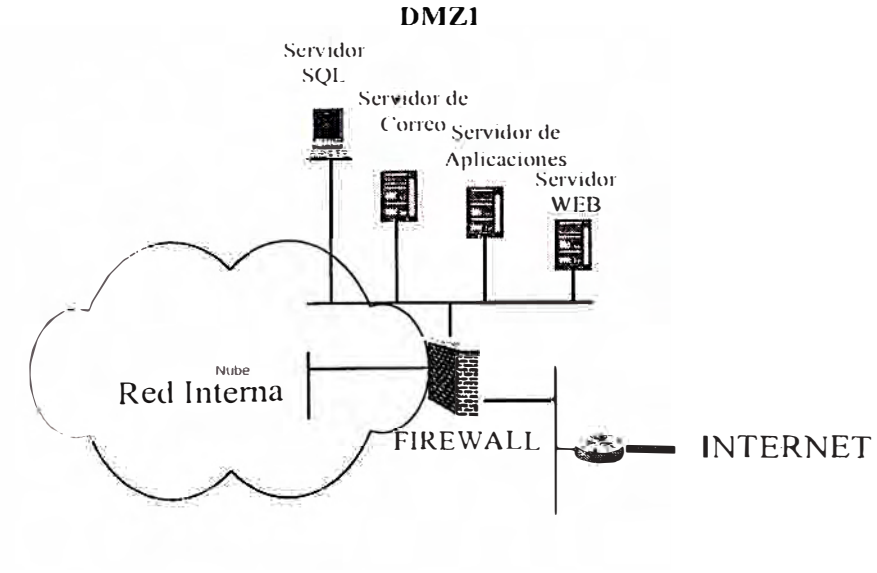



Fig. 6.1 topología de la red de la EMPRESA- condiciones iniciales

## 6.4 Descripción de la Red de Datos de la EMPRESA – Condición Final

En la topología de red final se observa (Fig. 6.2) que se han definido una conexión WAN a la red de datos del operador Celular a, además se ha definido una segunda (DMZ2) en la red del cliente e instalado dos equipos:

01 Servidor de Autenticación (Servidor de Control de Acceso, ACS)

01 equipo de Encriptación (Concentrador VPN Cisco)

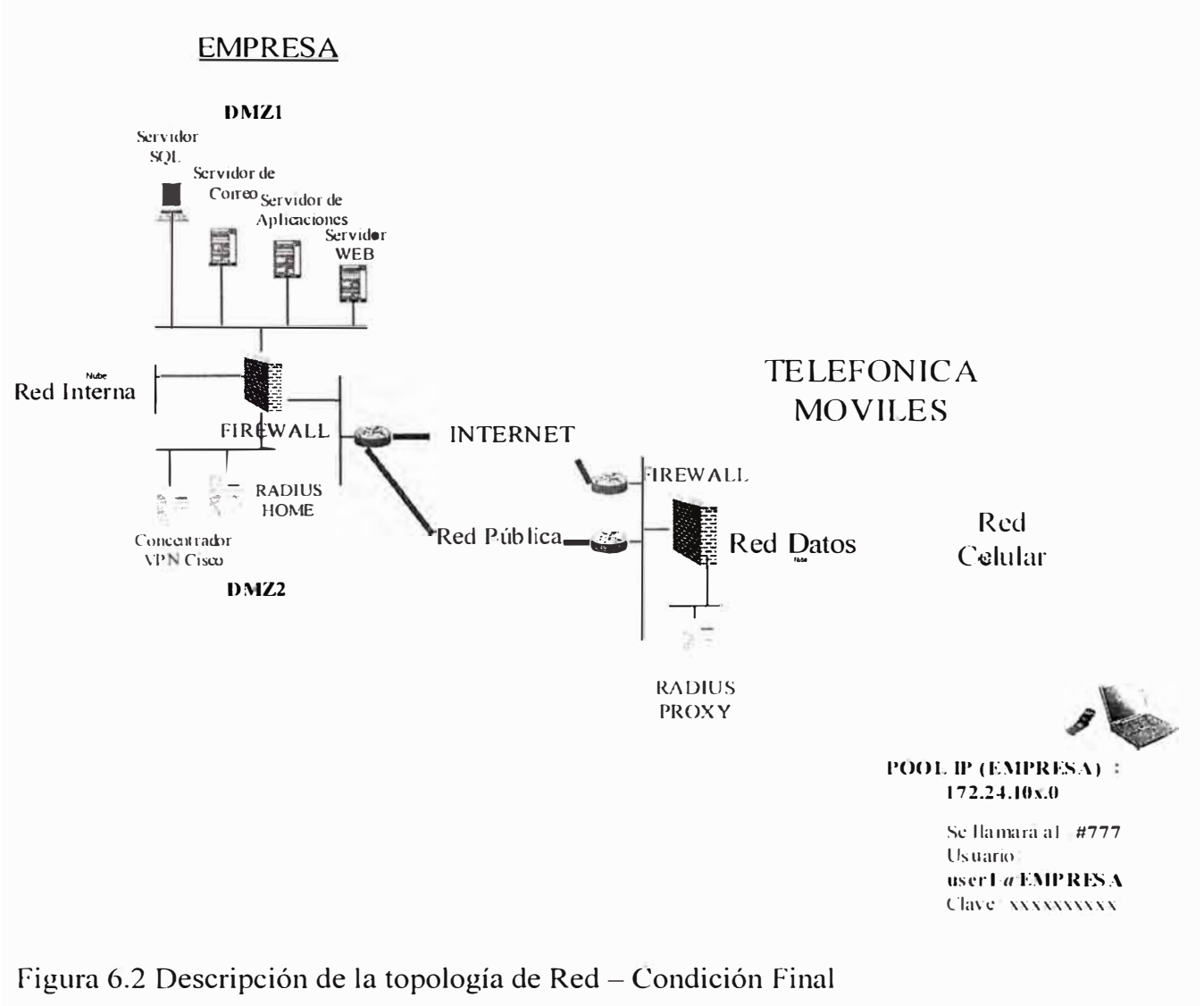



Figura 6.2 Descripción de la topología de Red – Condición Final

6.4.1 Interconexión entre las redes del Cliente y Operador Celular

Enlace punto a punto, se estableció un enlace punto a punto a través de una red pública con un ancho de banda igual a 256 kbps, considerando en el peor de los casos 8 conexiónes simultaneas a una velocidad de 32 KPSS.

Asignación del direccionamiento IP para la comunicación local de la EMPRESA

Direccionamiento IP DMZ2: 10.0.2.xMask:255.255.255.0

IP Home Radius: 10.0.2.1

IP concentrador VPN cisco: 10.0.2.2

Asignación del direccionamiento IP por el Operador Celular

El operador Celular asigna dos rangos de direcciones IP, el primer rango de direcciones IP (POOL1) es para la red local del cliente, DMZ1 y DMZ2, de esta manera el operador Celular evita los conflictos de direccionamientos IP mediante el uso de traslación de direcciones IP (NAT) que serán efectuadas en la red de la EMPRESA y la asignación del segundo rango de direcciones IP (POOL2) se encontrarán por el lado de la red del operador ya que estas direcciones son las que se asignarán a las Laptop ó PDAs mediante la comunicación inalámbrica.

Rango IP POOL1: 172.26.51.0mask: 255.255.255.0

Rango IP POOL2: 172.24.51.0mask: 255.255.255.0

Conectividad entre la red de los Usuarios Móviles y la red del Cliente

Para que los usuarios móviles puedan hacer uso de los servicios de la red Interna de la EMPRESA es necesario que los PDAs o Laptops puedan tener conectividad con el Home Radius y el equipo de encriptación (Concentrador VPN).

La EMPRESA debe configurar las tablas de ruteo para que sus paquetes de datos IP puedan alcanzar las direcciones del rango IP POOL2 (172.24.51.X) y 192.168.40.0 ubicadas en la red del Operador Celular y el Operador Celular debe configurar también sus tablas de ruteo para que los paquetes de datos IP con destino al rango de direcciones IP POOL1 pueden llegar a la red de datos del cliente (EMPRESA).

Una vez realizada esta configuración solo quedaría efectuar los NAT en el enrrutador de perímetro ó en el Firewall del cliente, tal y como sigue:

EquipoIP FísicaIP Lógica

Home Radius 10.0.2.1---- NAT --- >172.26.51.1

Concentrador VPN cisco10.0.2.2---- NAT --- >172.26.51.2

Configuración NAT

La configuración de la traslación de dirección IP la realizaremos en el enrrutador (NAT):

Comando Cisco:

ip nat inside source static 10.0.2.1 172.26.51.1

ip nat inside source static 10.0.2.2 172.26.51.2

Sesiones de los usuarios móviles

Establecimiento de las sesiones inalámbricas:

Una vez realizada la conectividad entre la red LAN de la red del cliente "EMPRESA" y el direccionamiento IP de los usuarios móviles, para que un usuario pueda hacer uso de los aplicativos o servicios de la red interna del cliente se deben de realizar las siguientes sesiones:

- Sesión de datos por paquetes

➢Sesión VPN

Sesión de datos por paquetes, para establecer una sesión de datos por paquetes el usuario debe realizar una llamada desde el PDA o Laptop con el usuario y clave asignado, por ejemplo:

Llamar al :#777

Ingresar

Usuario:user1@EMPRESA

Clave:xxxxxxxxxxxxxx

La llamada será atendida por la red celular del operador y la misma es conmutada a una comunicación de datos, después de progresar la llamada a nivel de la red celular luego tiene que validarse en la red de datos. Para validar al usuario user1@}EMPRESA, la petición de autenticación llega primero al Proxy Radius, este servidor revisa a que dominio pertenece el usuario y retransmite el pedido al servidor radius que valida este dominio (Home Radius), la comunicación entre el Proxy Radius y el Home Radius se efectúa a través de la dirección IP trasladada del Home Radius (IP:172.26.51.1). Si el usuario es validado por este servidor, al usuario se le asignará la dirección IP definida en su perfil de usuario (IP perteneciente al POOL2). En este nivel de la comunicación el usuario móvil tiene conectividad TCP/IP desde su nodo remoto hasta los servidores de la EMPRESA, luego será necesario efectuar una sesión VPN para encriptar la información que transmita o reciba por este medio.

Sesión VPN, para establecer estas sesiones se deben de validar primero los usuarios creados en esta plataforma, el usuario móvil debe de efectuar una llamada al concentrador VPN a la dirección IP traslada (IP 172.26.51.2), Por ejemplo:

Llamar al IP:172.26.51.2

Ingresar

Usuario :user1-vpn

Clave:yyyyyyyy

Después de la validación en el concentrador VPN, este equipo le asignará una dirección IP lógica perteneciente a clase de la dirección IP física del concentrador VPN (rango IP :10.0.2.x), y todas las comunicaciones del usuario móvil se efectuarán desde este segmento hacia los servidores de servicio que estén permitidos acceder.

6.4.2 Seguridad sobre la Información

Para garantizar la seguridad de la red de la EMPRESA y la confidencialidad de la información se hace uso de los equipos:

Servidor de Autenticación (ACS) o Home Radius, para que la EMPRESA pueda validar los usuarios de transmisión de datos por paquetes que ingresarán a su red de datos, el operador Celular define un dominio (por ejemplo @EMPRESA) en el servidor de autenticación principal (Proxy Radius) que le permite redireccionar todos los requerimientos de autenticación de los usuarios con el dominio "@EMPRESA", especificado previamente, a otro servidor de autenticación (Home Radius, ver figura 6.3) validando o denegando la petición de autenticación, si la autenticación es aceptada el servidor Home Radius le asignara una dirección IP correspondiente al rango de direcciones IP POOL2 con todas las características definidas en el servidor de autenticación del cliente.

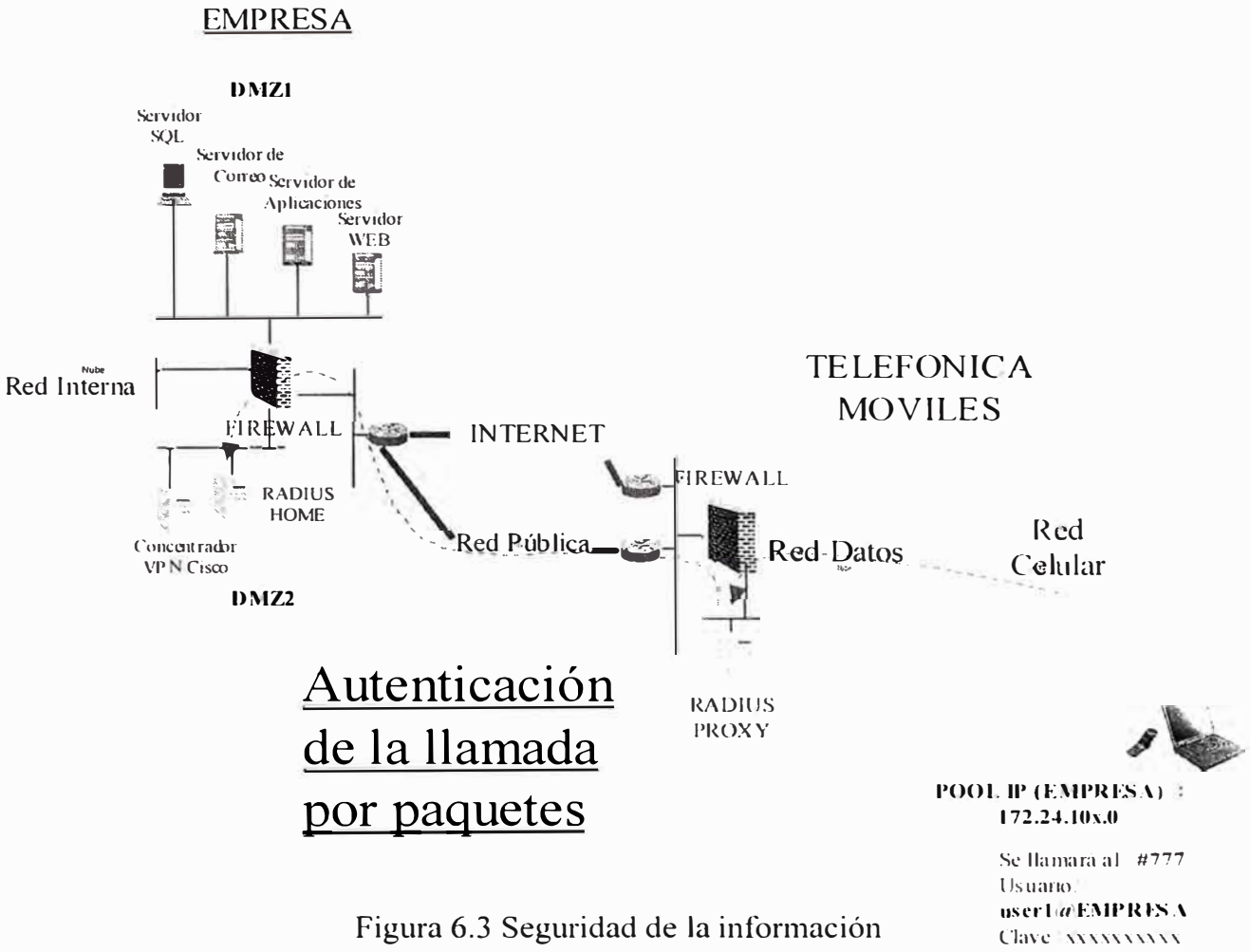



Figura 6.3 Seguridad de la información

Concentrador VPN Cisco, equipo de encriptación o servidor VPN, hasta el nivel anterior solo se ha establecido la conectividad desde el usuario móvil con la red de datos del cliente, sin embargo la información que viaja por esta redes no esta protegidas, para proteger los datos se necesita establecer una segunda comunicación pero esta vez con un equipo que haga VPN (Concentrador VPN Cisco, ver figura 6.4) para poder realizar esta encriptación es necesario instalar un cliente VPN en el PDA o Laptop con esto se asegura la confidencialidad de la información desde el dispositivo móvil hasta la red local de la EMPRESA.

En este equipo de definirá un USER y CLAVE para cada usuario inalámbrico y el perfil de usuario de cada uno de estos usuarios tendrá una dirección IP estática. esta asignación permanente de la dirección IP permitirá definir las políticas de seguridad en el Firewall.

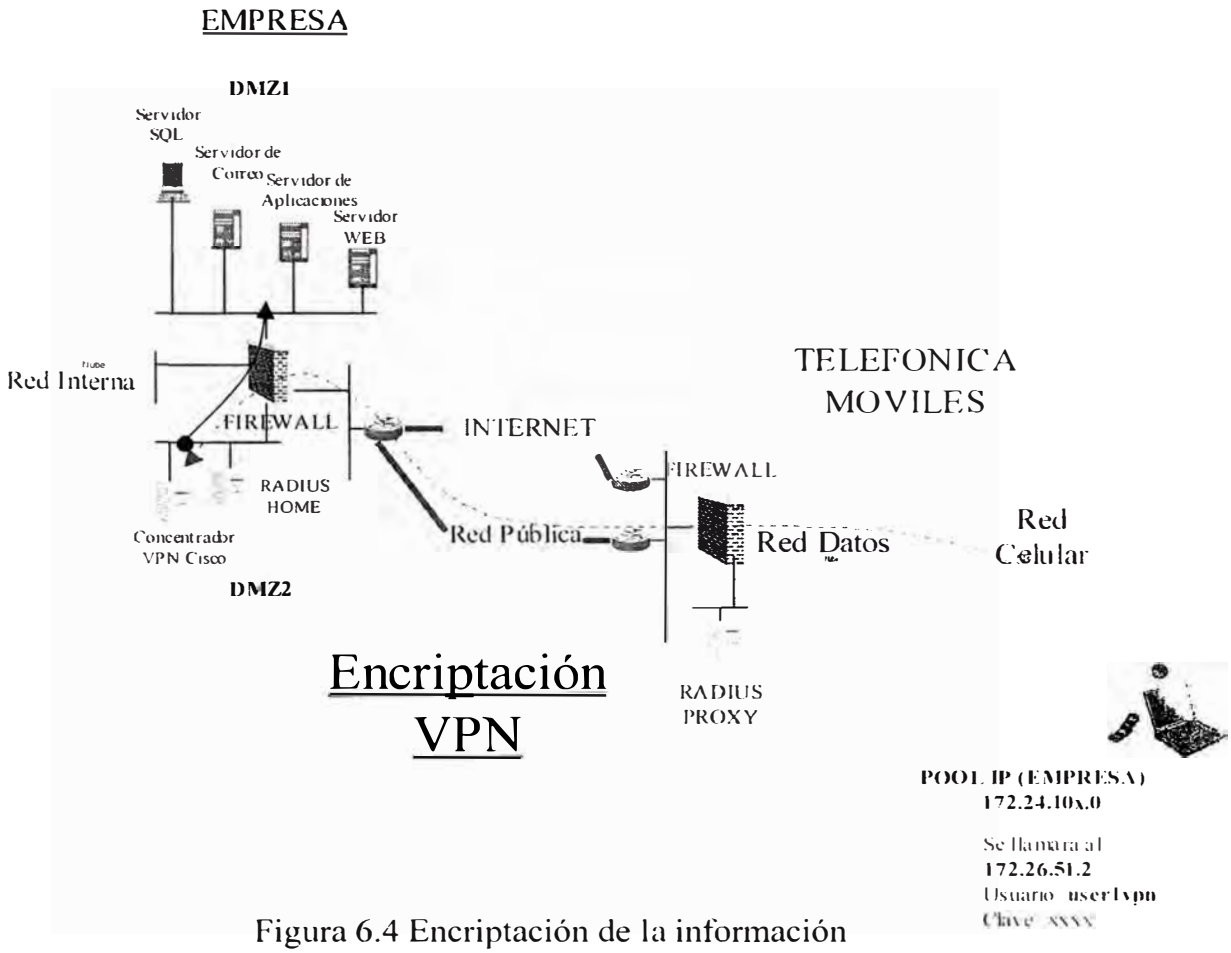



Figura 6.4 Encriptación de la información

Los niveles de encriptación con el concentrador VPN de Cisco se detallan en el anexo A

6.4.3 Control de accesos

Para controlar quienes ingresan a la red de la EMPRESA se empleará un Firewall o cortafuego, para proteger la red de la EMPRESA de cualquier ataque a las plataformas que alberga en su interior (dañar su operatividad, acceder a información

importante de la empresa etc.), por consiguiente para poder realizar los requerimientos planteados es necesario realizar las siguientes configuraciones en esta plataforma de seguridad

a. Definición de objetos del firewall

Es la denominación que se le da a la representación de cualquier elemento que participa en un proceso de comunicación, tales como estaciones de trabajo, servidores, redes, protocolos etc.)

Definición de Servidores

Nombre:Srv mail

Descripción :Servidor de Correo

Dirección IP: 10.0.1.1

Mask :255.255.255.0

Nombre:Srv web

Descripción :Servidor de Web

Dirección IP: 10.0.1.2

Mask :255.255.255.0

Nombre:Srv_app

Descripción :Servidor de Apliaciones

Dirección IP: 10.0.1.3

Mask :255.255.255.0

Nombre:Srv db

Descripción :Servidor de Base de Datos

Dirección IP: 10.0.1.4

Mask :255.255.255.0

Nombre:Srv radius

Descripción :Servidor Home Radius

Dirección IP: 10.0.2.1

Mask :255.255.255.0

Nombre:Srv_vpn

Descripción :concentrador VPN Cisco

Dirección IP: 10.0.2.2

Mask :255.255.255.0

Nombre:Srv_proxy_radius

Descripción :Servidor Proxy Radius

Dirección IP: 192.168.40.201

Mask :255.255.255.0

Nombre:Srv_wap

Descripción :Servidor Gateway Wap

Dirección IP: 192.168.40.100

Mask :255.255.255.0

Definición de grupos de IPs

Nombre:POOL2

Descripción :Direcciones IP de los usuarios móviles

IP network: 172.24.51.0

Mask :255.255.255.0

Nombre:G-ventas

Descripción :Direcciones IP de los vendedores con VPN

Inicio IP: 10.0.2.101

Fin IP:10.0.2.170

Nombre:G-gerentes

Descripción :Direcciones IP de los vendedores con VPN

Inicio IP: 10.0.2.171

Fin IP:10.0.2.175

Nombre:G-operacion

Descripción :Direc. IP de los usuarios de operación&manten. con VPN

Inicio IP: 10.0.2.181

Fin IP:10.0.2.185

Definición de Servicios

Nombre:Serv-radius

Descripción:Puerto UDP de autenticación

UDP port:1645

Nombre:Serv-1646-radius

Descripción:Puerto UDP de autenticación

UDP port:1645

Grupo de Servicios:G-Serv-Autent.

Mienbros : Serv-radius, Serv-1646-radius

Nombre:Serv-vpn

Descripción:Puerto TCP para PPTP

TCP port:1723

Nombre:Serv-db

Descripción:Puerto TCP para Base de Datos

TCP port:1521

Nombre:Serv-web

Descripción:Puerto TCP para el servicio WEB

TCP port:80

Nombre:Serv-pop3

Descripción:Puerto TCP lectura de correo

TCP port:110

Nombre:Serv-smtp

Descripción:Puerto TCP envio de correo

TCP port:25

Nombre:Serv-telnet

Descripción:Puerto TCP para telnet

TCP port:23

Nombre:Serv-app-pedido

Descripción:Puerto TCP para la aplicación de toma de pedidos

TCP port: 5002

b. Definición de las reglas de Seguridad

Reglas en el Firewall

Regla 1

Todos los usuarios móviles deben poder autenticarse y luego establecer una sesión VPN, por tanto de añadirse la siguiente regla en la política de seguridad.

| Regla | Fuente | Destino | Servicio | Acción |
|---|---|---|---|---|
| 1 | Srv_proxy_radius | 172.26.51.1 (Home Radius) | G-Serv-Autent | Aceptar |
| 2 | POOL2 | Srv_radius | Serv-vpn | Aceptar |

Regla 2

"Consultar un servidor de aplicaciones para obtener información sobre el stock de productos, lista de precios, ofertas y promociones de productos, línea de crédito del cliente, histórico de pedidos realizados por clientes etc., para los vendedores"

| Regla | Fuente | Destino | Servicio | Acción |
|---|---|---|---|---|
| 3 | G-ventas | Srv_app | Serv-app-pedido | Aceptar |

Regla 3

"Conexión al servidor de correo corporativo para enviar y recibir correos para los vendedores y Gerentes"

| Regla | Fuente | Destino | Servicio | Acción |
|---|---|---|---|---|
| 4 | G-ventas | Srv mail | Serv_pop3,Serv_smtp | Aceptar |
| 5 | G-gerentes | Srv_mail | Serv_pop3, Serv_smtp | Aceptar |

Regla 4

"Operación y mantenimiento de los enrrutadores y plataformas Unix para los usuarios del área técnica"

| Regla | Fuente | Destino | Servicio | Acción |
|---|---|---|---|---|
| 6 | G-operacion | cualquiera | Serv_telnet | Aceptar |

Regla 5

"Consultas rápidas vía WAP para los vendedores"

| Regla | Fuente | Destino | Servicio | Acción |
|---|---|---|---|---|
| 7 | Srv_wap | Srv web | Serv web | Aceptar |

Regla 6

"Control y reporte diario de vigilantes de seguridad"

| Regla | Fuente | Destino | Servicio | Acción |
|---|---|---|---|---|
| 8 | Srv_wap | Srv web | Serv web | Aceptar |

Por tanto las reglas de seguridad que se deben añadir son las siguientes:

| Regla | Fuente | Destino | Servicio | Acción |
|---|---|---|---|---|
| 1 | Srv_proxy_radius | 172.26.51.1 | G-Serv-Autent | Aceptar |
| 2 | POOL2 | Srv_radius | Serv-vpn | Aceptar |
| 3 | G-ventas | Srv_app | Serv-app-pedido | Aceptar |
| 4 | G-ventas | Srv_mail | Serv_pop3, Serv_smtp | Aceptar |
| 5 | G-gerentes | Srv_mail | Serv_pop3, Serv_smtp | Aceptar |
| 6 | G-operación | cualquiera | Serv_telnet | Aceptar |
| 7 | Srv_wap | Srv_web | Serv_web | Aceptar |
| 8 | Srv_wap | Srv_web | Srv_web | Aceptar |

## 6.5 Aplicaciones

La software que se describe es la Aplicación WAP para el área de vigilancia y seguridad de locales.

### 6.5.1 Introducción

Señalar los datos que describan al producto o servicio en lo que se refiere a su naturaleza, funcionamiento, usos y aplicaciones posibles.

El control de los agentes de una empresa de seguridad (SEGURIMAX) es de mucha importancia para garantizar tanto la protección de la instalación que se encuentran resguardando así como la seguridad de su personal.

### 6.5.2 Antecedentes

Para Segurimax la comunicación permanente con su personal es una necesidad. Saber si los agentes se encuentran alertas, en sus posiciones y seguros, es vital para poder socorrerlos en alguna emergencia o llamarles la atención en caso de falta, pues es responsabilidad de Segurimax la seguridad de muchos locales en Lima y a nivel nacional.

Anteriormente Segurimax manejaba los reportes de sus vigilantes mediante llamadas esporádicas por radio a su central de control o invertía en vehículos y personal que recorrían los locales de los clientes supervisándolos.

Conforme se iban recibiendo las llamadas, los reportes eran registrados manualmente para luego descargarse en su sistema de gestión al final del día. No se contaba con una aplicación de gestión e interacción de eventos en tiempo real.

Esta forma de trabajo le ocasionaba a Segurimax algunos problemas :

- Falta de control adecuado y respuesta oportuna, no tenían un control certero sobre la ubicación de los agentes. Si bien los agentes se reportaban por radio, manualmente era imposible determinar a tiempo si es que algún agente no lo había hecho. Por ende, se corría el riesgo de que el personal no se encuentre en sus puestos, que se queden dormidos, que hayan tenido una emergencia y que ellos no lo hayan notado, etc.
- Horas-Hombre, requerimiento excesivo de personal administrativo para el seguimiento a los agentes a través de llamadas por radio, en los vehículos de supervisión y destinados al ingreso de reportes manuales en el sistema.
- Errores de Tipeo, se derivan del traslado de data manual al sistema informático.
- Comunicación deficiente, la comunicación por radio truncking era de baja calidad, con altos niveles de ruido, sin cobertura nacional, con retardos en el envío de

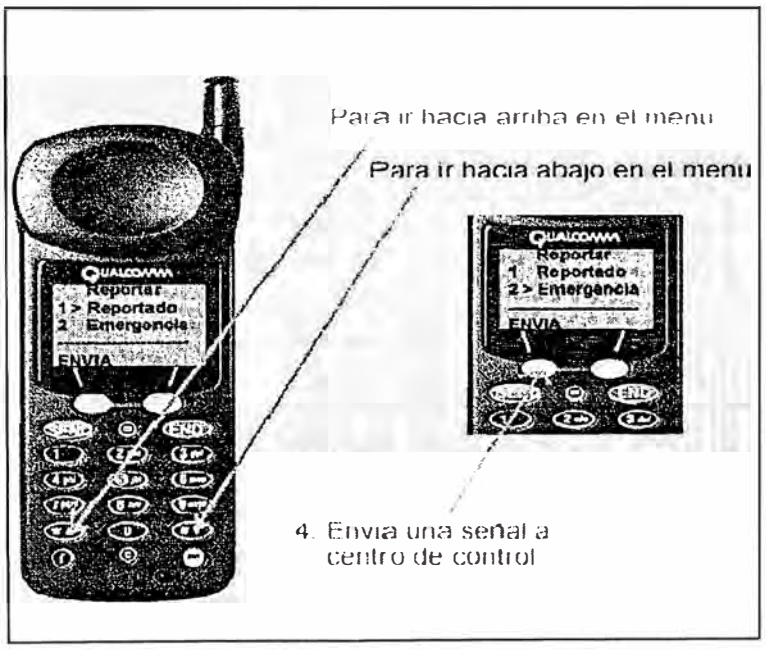
información y sin confidencialidad ni privacidad en las conversaciones de altavoz por radio.

6.5.3 Desarrollo de la aplicación: DATA ALARM SYSTEM (DAS)

Segurimax encargó la optimización de su sistema de control de vigilantes a un Operador Celular. La solución se basó en desarrollar una comunicación eficiente entre la empresa y sus agentes, utilizando la transmisión de datos celular a través de la tecnología WAP.

El aplicativo WAP desarrollado, el Data Alert System, ha sido creado para ser manejado por el personal de Segurimax (vigilantes y supervisores, ver figura 6.5). Ellos enviarán información valiosa para Segurimax presionando ciertos comandos (teclas) desde un menú de navegación muy sencillo instalado en sus celulares. Cuenta con dos funciones principales: Reportes y Emergencias.

Figura 6.5 Menú de navegación de pantallas del DAS:




Cuando el agente presiona la opción **Reporte,** ésta envía un mensaje de manifiesto a la central de control de Segurimax, vía transmisión de datos, en señal de

conformidad. Los reportes deben ser generados las 24 horas del día, los 365 días del año y de forma periódica, con un intervalo de 30 minutos entre cada uno.

La data viaja automáticamente hasta el Centro de Control de Segurimax, en donde genera automáticamente un registro del reporte en la base de datos, identificando el nombre del cliente vigilado, el local, el numero único del equipo móvil que identifica al agente, la fecha y hora.

La información recibida es visualizada en una consola de supervisión tipo página WEB que permite revisar los datos de cada reporte de una forma sencilla y explícita. Las consultas pueden realizarse por cliente. En caso un agente no se haya reportado, la consola web avisará con una señal de omisión.

La opción **Emergencia** es utilizada para generar un reporte de alerta. Cuando el agente selecciona esta opción, la aplicación crea automáticamente un registro en la base de datos de Segurimax identificando al cliente, local, equipo móvil del agente, fecha y hora de la ocurrencia. Dicha señal es plasmada en la consola de supervisión web con una alerta de sonido y efectos visuales que destacan la emergencia. En el Centro de Control, los operadores responsables visualizarán la alerta fácilmente por lo que podrán ponerse en contacto de forma inmediata con las fuerzas del orden con las que se encuentra interconectados (comisarías o bomberos, etc.) y sus supervisores zonales, para atender la emergencia con rapidez.

Consola de Supervisión WEB:

En el caso de clientes corporativos, como un servicio de valor agregado para su mayor tranquilidad, Segurimax les ofrece poder accesar por Internet a su consola de supervisión web. Ellos también pueden monitorear a los agentes de seguridad desde

sus propias instalaciones y contar con información oportuna en caso de ocurrir alguna eventualidad.

Búsqueda por cliente:


Figura 6.6 Busqueda de clientes

Reportes de agentes visualizados en la consola web:

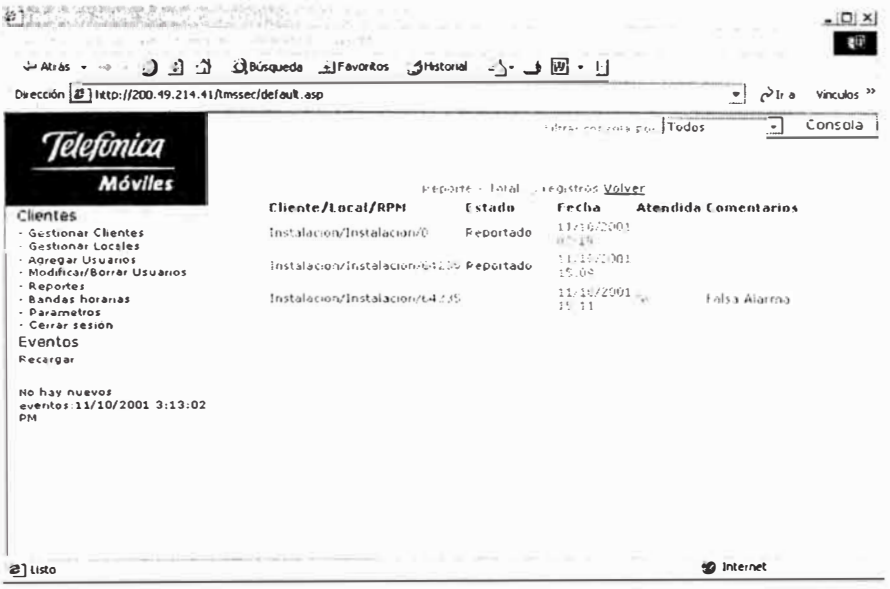



Figura 6.7 Consola Web

La Consola de Supervisión permite generar reportes históricos por clientes y retransmitir la información por correo electrónico.


Figura 6.8 Interface de reportes

Requerimientos para la instalacion del aplicativo:

oSistema de Acceso: Operador Celular con protocolo WAP.

oHardware: Pentium III, 128MB RAM y 100MB de disco, tarjeta de red ethernet.

oSoftware: Windows 2000, Internet Information Server, Base de datos Access 2000.

6.5.4 Arquitectura de la solución

En el siguiente diagrama se visualiza la arquitectura de la solución(ver fig. 6.9)

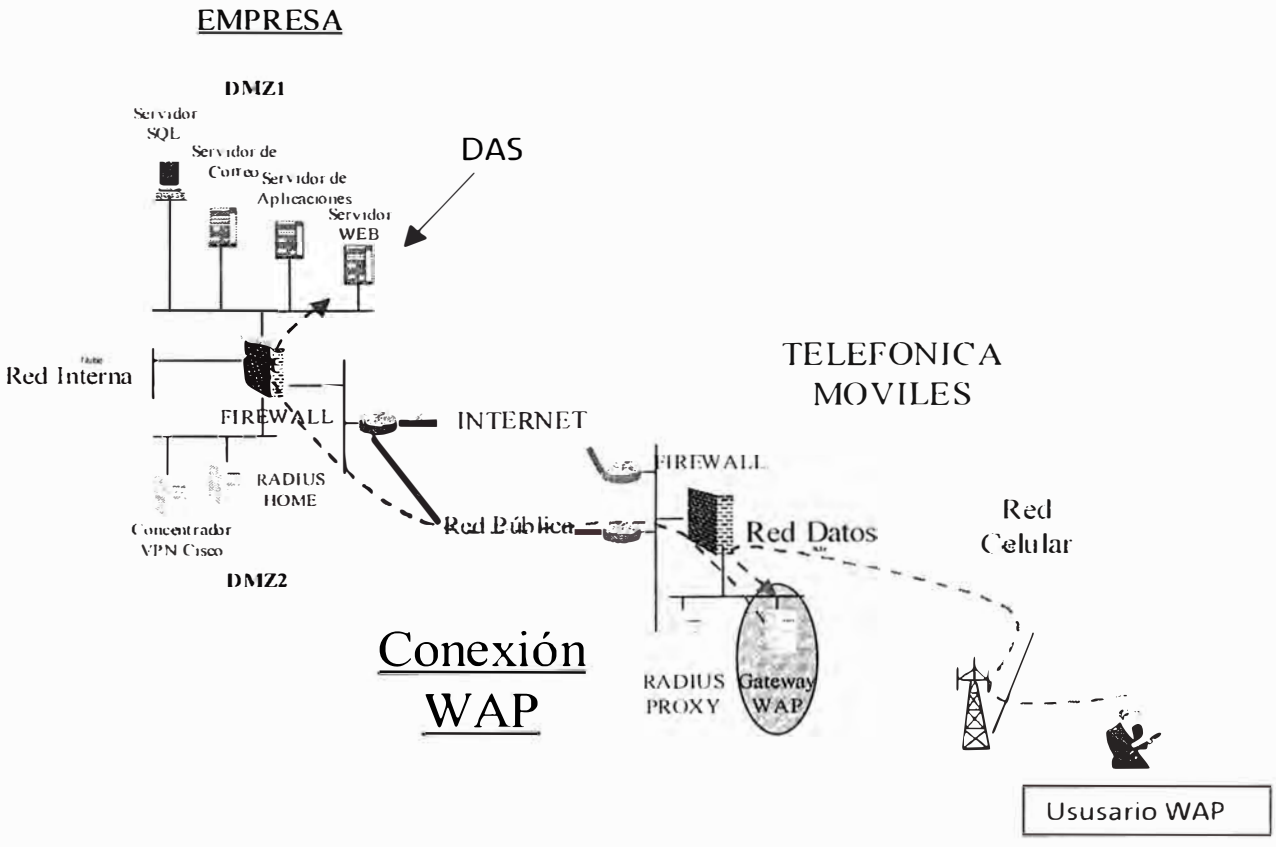



Figura 6.9 Arquitectura de la solución : DATA ALARM SYSTEM (DAS)

# CONCLUSIONES Y RECOMENDACIONES

## CONCLUSIONES

1) La infraestructura propuesta en el proyecto tiene las mejores posibilidades de expansión, crecimiento y evolución.
2) La red IP implementada sobre la infraestructura del operador Celular es compatible con plataformas actuales y la arquitectura de red de los usuarios (empresas en general), que está diseñada para migrar hacia futuras tecnologías.
3) La red propuesta esta soportada por un sistema de alta capacidad con conexiones dedicadas de bajos costos de conexión, seguridad, confiabilidad, escalabilidad y flexibilidad.
4) El proyecto contempla una solución con posibilidad de expandirse a nivel nacional, ventaja que sería aprovechable por la infraestructura del operador actual.
5) El modelo presentado permitirá mejorar la performance para la transferencia de información de los servicios tradicionales tales como WWW, correo electrónico, o la transferencia de archivos, acceso a las bases de datos.
6) La Interconexión permitirá compartir recursos entre las oficinas permitiendo desarrollar mayor valor agregado y calidad de servicios.
7) Las aplicaciones desarrolladas sobre la red Celular permitirán un control preciso y eficiente sobre usuarios móviles.

8) Comunicación en línea con cada uno de los usuarios móviles.

9) Reportes oportunos, registrados en el sistema en menos de tres segundos de ocurrido el evento.

10) Menor riesgo de contar con usuarios que se dediquen a otras labores, debido al control de los accesos que se pueden efectuar.

11) Se evitan procesos lentos e imprecisos de registros manuales. Procesos administrativos automatizados, logrando simpleza y rapidez.

12) Con respecto a la solución planteada para las fuerzas de venta de las empresas podemos mencionar las siguientes:

- Aumenta la productividad de la fuerza de ventas.
- Mayor rapidez en la atención de pedidos y cconsultas.
- Información siempre actualizada, lo que disminuye la posibilidad de pedidos errados (Stock no disponible).
- Fidelización del cliente gracias a la mejora de su atención.

13) Con respecto a la solución planteada vía wap para los vigilantes del área de seguridad tenemos:

- Reducción de Gastos de la Supervisión Física, ya no se invierte en gastos de combustible y mantenimiento de vehículos de supervisión, comunicación por radio y grupal de operadoras de atención.
- Reducción de Horas – Hombre, gracias a la automatización de procesos, disminución de carga de trabajo en call centers (operadoras telefónicas) y rondas de supervisión.
- Mayor productividad, el porcentaje de agentes dormidos en el turno nocturno se ha reducido, lo que significa menor riesgo para los clientes.

- Crecimiento en las Ventas, a partir de un sistema de seguridad más eficiente y con mayores posibilidades y servicios para los clientes.

## RECOMENDACIONES

1) La implantación de este proyecto es recomendable para empresas que cuenta con empleados que se dedican a las ventas o se encuentran fuera de la oficina constantemente y requieren disponer de la información en línea de los productos en stock, promociones, mensajería de correo electrónico etc.
2) Con la finalidad de garantizar la seguridad de la información es recomendable que la empresa realice la autenticación local de los usuarios que van a ingresar en forma inalámbrica a la red interna de la empresa (red LAN).
3) Se recomienda establecer un sistema de encriptación de la información ya sea empleando aplicaciones sobre protocolos HTTPS o añadiendo un equipo encriptador de la información (Servidor VPN), para garantizar la confidencialidad de la información.

## ANEXO A: GLOSARIO

**A**

**B**

| | |
|---|---|
| Bearers | Portador e.g. Circuitos Paquetes, SMS |
| BSS | (Base Station System) Sistema de Estación Base, representa la red celular CDMA |
| BTS | Estación Base Transreceptora |

**C**

| | |
|---|---|
| CBSC | Controlador Centralizado de la Estación Base |
| CDMAServiceOptionList | Lista de opciones de servicio CDMA, son los servicios disponibles dentro de la red celular CDMA |

**D**

**E**

**F**

| | |
|---|---|
| Gateway WAP | Equipo que sirve de pasarela entre la red Celular y la red TCP/IP |

**H**

| | |
|---|---|
| Handoff | Son los procesos que obtiene un móvil (terminal celular) para "hablar" con otra estación base |
| Hard Handoff | Se produce cuando un la comunicación de móvil pasa de una estación base digital a otra estación base analógica o cuando la comunicación pasa de una portadora a otra en un CBSC |
| HTML | (Hypertext Markup Language) Lenguaje usado para la escritura de páginas y sitios web en internet |

**I**

| | |
|---|---|
| IMSI | (International Moble Subscriber Identifier) Identificador de subscriptor Móvil Internacional |
| IP | Protocolo Internet |
| IS-95 | Es el estándar de la interface aire para sistema digital CDMA |
| IS-95B | Es el estándar de la interface aire para sistema digital CDMA que soporta transacciones multicanales |
| IWF | Internetwork Function , El equipo para interconectar redes |
| IWU | Motorola llama así al IWF |

**J**

**K**

**L**

**M**

| | |
|---|---|
| MIN | (Mobile Identificación Number) Número Identificador del Móvil |
| MM | Dispositivo Administrador de las Unidades Móviles |
| MTS | Mobile Telephony Subsystem ,Subsistema de Telefonía Móvil |
| MSC | Centro Móvil de Conmutación |
| MSS | (Mobil Station Signaling) Señalización de la Estación Móvil, representa la red de comunicación analógica |

**N**

**O**

| | |
|---|---|
| OMC-R | Centro de Operación y Mantenimiento Centralizado de Radio |

**P**

| | |
|---|---|
| PSTN | Red Telefónica Pública de Conmutación |

| | |
|---|---|
| PDA | (Personal Digital Asisten) Digitales de Asistencia Personal |

**Q**

**R**

**S**

| | |
|---|---|
| SID | (System Identification) Identificador del Sistema |
| Smart phones | Teléfonos ligeros |
| Subscriptores | Abonados o usuarios móviles de la red celular |
| SS QNC | (Single Stack Quick Net Connect ) Conexión Rápida de Red de Pila Simple |
| SSL | (Secure Sockets layer) Capa de Seguridad de Conexión |
| Soft Handoff | Se produce cuando un móvil se comunica de una BTS a otra BTS bajo el mismo controlador centralizado |

**T**

| | |
|---|---|
| TCP/IP | Protocolo de Control de Transmision |

**U**

| | |
|---|---|
| UNO | Centro de Operación de Red |

| | |
|---|---|
| UP.Link | Provee el armazón para la distribución de aplicaciones sobre redes de datos inalámbricas para teléfonos celulares y dispositivos digitales de asistencia personal (gateway WAP) |

**V**

**W**

| | |
|---|---|
| WAP | (Wireless Application Protocol) Protocolo de Aplicaciones Inalámbrica |
| WAE | (Wireless Application Environment) Entorno de Aplicación Inalámbrica |
| WSP | (Wireless Session Protocol ) Protocolo de Sesión Inalámbrica |
| WTP | (Wireless Transaction Protocol) Protocolo de Transacción Inalámbrica |
| WTLS | (Wireless Transport Layer Security) Capa de Seguridad de Transporte Inalámbrico |
| WDP | (Wireless Datagram Protocol) Protocolo Datagrama Inalámbrico |

**X**

**Y**

**Z**

## ANEXO B: DESCRIPCIÓN DEL EQUIPO CONCENTRADOR VPN CISCO

**Concentradores de la serie** *Cisco VPN 3000*

LOS CONCENTRADORES DE LA SERIE CISCO VPN 3000 PERMITEN A LAS EMPRESAS OBTENER EL MÁXIMO PARTIDO DEL AHORRO EN COSTOS, LA FLEXIBILIDAD, LAS PRESTACIONES Y FIABILIDAD SIN PRECEDENTES DE LAS CONEXIONES VPN DE ACCESO REMOTO

Las empresas utilizan las redes privadas virtuales (VPN) para establecer conexiones de red globales seguras sobre las infraestructuras públicas de red. Las VPN se han convertido en la solución lógica para la conectividad de acceso remoto por dos razones principales:

• El despliegue de una VPN de acceso remoto permite a las empresas reducir sus gastos de comunicaciones y potenciar las infraestructuras de acceso telefónico de los proveedores de servicio de Internet.

• Las VPN de acceso remoto permiten que los trabajadores móviles, teletrabajadores y subcontratados saquen partido de la conectividad de banda ancha. Para descubrir todas las ventajas de las VPN de acceso remoto y altas prestaciones, una empresa debe desplegar una solución VPN potente y de gran disponibilidad, y los dispositivos VPN dedicados son la alternativa óptima para este propósito. Los concentradores de la serie

su despliegue en la empresa. Se incluyen dispositivos de terminación con capacidad de ampliación para el túnel VPN y un cliente VPN fácil de usar y basado en los estándares, así como un sistema de gestión que permite a las empresas una sencilla instalación, configuración y control de sus VPN de acceso remoto. Mediante la incorporación de una arquitectura de acceso remoto avanzada, de altas capacidades y gran disponibilidad y construida con un solo propósito, el Concentrador Cisco VPN 3000 permite a las empresas construir infraestructuras VPN potentes, de altas prestaciones, con gran capacidad de ampliación para dar soporte a sus aplicaciones críticas de acceso remoto. Es la única plataforma en la industria con capacidad de ampliación que ofrece componentes que se pueden intercambiar en actividad y que puede ser ampliada por el cliente. Estos componentes, llamados módulos SEP (Scalable Encryption Processing),permiten a los usuarios añadir fácilmente capacidad y tráfico. El concentrador Cisco VPN 3000 admite el más amplio rango de implementaciones del software cliente para VPN, incluyendo Cisco VPN 3000 Client, Microsoft Windows 2000 L2TP/Ipsec Client y Microsoft PPTP para Windows 95, Windows 98, Windows NT 4.0, y Windows 2000.

- **Cinco modelos**

El concentrador Cisco VPN 3000 está disponible en cinco modelos diferentes para adaptarse a cualquier negocio:

**Concentrador Cisco VPN 3005**

El concentrador Cisco VPN 3005 es una plataforma VPN diseñada para pequeñas y medianas empresas con requisitos de ancho de banda hasta de T1/E1 a dúplex completo (con un rendimiento máximo de 4 Mbps) y hasta 100 sesiones simultáneas. El proceso de cifrado se lleva a cabo por software. Cisco VPN 3005 no incorpora capacidad de ampliación.

**Concentrador Cisco VPN 3015**

El concentrador Cisco VPN 3015 es una plataforma VPN diseñada para pequeñas y medianas empresas con requisitos de ancho de banda hasta de T1/E1 a dúplex completo (con un rendimiento máximo de 4 Mbps) y hasta 100 sesiones simultáneas. Al igual que Cisco VPN 3005, el proceso de cifrado se realiza por software, pero Cisco VPN 3015 es además ampliable en la instalación a los modelos Cisco VPN 3030 y 3060.

**Concentrador Cisco VPN 3030**

El concentrador Cisco VPN 3030 es una plataforma VPN diseñada para medianas y grandes empresas con requisitos de ancho de banda variables de T1/E1 a T3/E3 a dúplex completo (con un rendimiento máximo de 50 Mbps) y hasta 1.500 sesiones simultáneas. Unos módulos SEP especializados se encargan de la aceleración por hardware. Cisco VPN 3030 se puede ampliar al modelo Cisco VPN 3060 en la instalación. Se encuentran disponibles configuraciones redundantes y no redundantes.

**Concentrador Cisco VPN 3060**

Cisco VPN 3060 es una plataforma VPN diseñada para empresas grandes que requieren los más altos niveles de prestaciones y fiabilidad, con necesidades de gran ancho de banda que van de T3 fraccional a T3/E3 completo o superiores (con un rendimiento

máximo de 100 Mbps) y hasta 5.000 sesiones simultáneas. Unos módulos SEP especializados se encargan de la aceleración por hardware. Se encuentran disponibles configuraciones redundantes y no redundantes.

**Concentrador Cisco VPN 3080**

El concentrador Cisco VPN 3080 está optimizado para cubrir las necesidades de grandes empresas que requieren el más alto nivel de prestaciones junto con la necesidad de admitir hasta 10.000 sesiones de acceso remoto de forma simultánea. Unos módulos SEP especializados se encargan de la aceleración hardware. El VPN 3080 está disponible sólo en configuración totalmente redundante.

- **Cliente Cisco VPN 3000**

El cliente Cisco VPN 3000 es fácil de desplegar, de funcionamiento sencillo y se utiliza para establecer túneles cifrados seguros y globales hasta el concentrador Cisco VPN 3000. Esta implementación de diseño ligero y compatible con IPSec se proporciona con el concentrador Cisco VPN 3000 y su licencia es válida para un número ilimitado de usuarios. El cliente se puede configurar para despliegues masivos y los primeros inicios de sesión necesitan muy poco trabajo de configuración. Las normativas de acceso VPN se crean y almacenan de forma centralizada en Cisco VPN 3000 Concentrator y se mandan al cliente cuando se establece una conexión.

- **Cisco VPN 3000 Monitor**

Cisco VPN 3000 Monitor es una aplicación software basada en Java para el control, aviso y recopilación de datos en uno o varios concentradores VPN 3000. La aplicación basada en Java es compatible con Windows 95, Windows 98, Windows NT 4.0, y Windows 2000. Se utiliza un sondeo SNMP para recopilar las estadísticas de cada uno de los dispositivos. Enterprise View muestra el estado a alto nivel de cada dispositivo de la red. El administrador puede además obtener datos más o menos detallados de cada dispositivo. Además, Cisco VPN 3000 Monitor almacena los datos recopilados, las interrupciones, y los ficheros de eventos para posteriores análisis históricos, planificación de capacidad, y resolución de problemas. También suministra tablas y gráficos estándares.

Características de los concentradores de la serie Cisco VPN 3000

| | Cisco VPN 3005 | Cisco VPN 3015 | Cisco VPN 3030 | Cisco VPN 3060 | Cisco VPN 3080 |
|---|---|---|---|---|---|
| Usuarios simultáneos | | | | | |
| Sesiones LAN a LAN máximas | | | | | |
| Caudal descifrado | Mbps | Mbps | Mbps | Mbps | Mbps |
| Método de cifrado | | | | | |
| Módulo SEP de cifrado | | | | | |
| SEP redundante | No disponible | No disponible | | | |
| Ranuras de expansión disponibles | | | | | |
| Capacidad de ampliación | | | | | |
| Memoria del sistema | MB | MB | MB | MB | MB |
| Módulo WAN T1 | | | | | |
| Configuración del hardware | | | | | |
| Fuente de alimentación doble | | | | | |
| Detección de cliente | | | | | |

La serie de concentradores Cisco VPN 3000 admite todo el rango de aplicaciones empresariales.

## Características y ventajas de los concentradores de la serie Cisco VPN 3000

### Aspectos destacados del producto

Arquitectura de procesamiento distribuido de alto rendimiento

• Los módulos SEP de Cisco proporcionan cifrado por hardware, garantizando un rendimiento consistente en toda la gama de capacidades (Cisco VPN 3030 - 3080).

• Compatible con túnel de gran tamaño para conexiones IPsec, PPTP y L2TP/IPsec.

Capacidad de ampliación (Cisco VPN 3015-3060)

• El diseño modular (cuatro ranuras de expansión) proporciona protección de la inversión, redundancia y una forma fácil de ampliar los equipos.

• La arquitectura del sistema está diseñada para proporcionar un rendimiento consistente y una alta disponibilidad.

• El diseño completamente digital proporciona la más alta fiabilidad y un funcionamiento continuo las 24 horas.

• El potente paquete de instrumentación proporciona control en funcionamiento y alertas.

• La compatibilidad con Microsoft ofrece el despliegue de clientes a gran escala y la integración de forma transparente con sistemas relacionados.

### Seguridad

• La compatibilidad con todos los estándares de seguridad, tanto actuales como emergentes, permite la integración de sistemas externos de autenticación y la interoperatividad con productos de otros fabricantes.

• Las características de firewall incluyen el filtrado de paquetes sin estado y la conversión de direcciones para garantizar los requisitos de seguridad de una LAN empresarial.

• La gestión a nivel de usuario y de grupo ofrece la máxima flexibilidad.

**Gran nivel de disponibilidad**

• Los subsistemas redundantes y las capacidades de recuperación ante fallos de su configuración con varios chasis aseguran el máximo tiempo de actividad del sistema.

• Las completas capacidades de instrumentación y control ofrecen a los administradores de redes alertas y avisos en tiempo real del estado del sistema.

**Gestión potente**

• Los concentradores de la serie Cisco VPN 3000 se pueden gestionar utilizando cualquier navegador Web estándar (vía HTTP o HTTPS), así como mediante Telnet, Secure Telnet, y a través de un puerto de consola.

• Proporcionan capacidad de configuración y control tanto a las empresas como a los proveedores de servicio.

• Se pueden configurar los niveles de acceso por usuarios o por grupos, facilitando las tareas de configuración y el mantenimiento de las normativas de seguridad.

**Ficha técnica de los concentradores de la serie Cisco VPN 3000**

**Hardware**

Procesador

• Procesador Motorola PowerPC Memoria

• Imágenes redundantes del sistema (Flash)

• Opciones de memoria variables (ver gráfico) Cifrado

• Cisco VPN 3005, 3015: cifrado por software

• Cisco VPN 3030-3080: cifrado por hardware Interfaces LAN integradas

• Cisco VPN 3005: dos puertos Fast Ethernet 10/100BaseTX a dúplex completo con detección automática (público/no fiable, privado/fiable)

• Cisco VPN 3015-3080: tres puertos Fast Ethernet 10/100BaseTX a dúplex completo con detección automática (público/no fiable, privado/fiable y DM2) Instrumentación

• Panel frontal Cisco VPN 3005: indicador del estado de la unidad

• Panel posterior Cisco VPN 3005: indicadores LED de estado para los puertos Ethernet

• Panel frontal Cisco VPN 3015-3080: indicadores LED de estado para el sistema, módulos de expansión, fuentes de alimentación, módulos Ethernet, ventilador

• Panel posterior Cisco VPN 3015-3080: indicadores LED de estado para los módulos Ethernet, los módulos de expansión,las fuentes de alimentación

• Cisco VPN 3015-3080: el monitor de actividad muestra el número de sesiones, el caudal de tráfico agregado o la utilización de la CPU, seleccionables mediante pulsadores

**Software**

Compatibilidad del software cliente

• Cisco VPN 3000 Client (IPsec) paraWindows 95,Windows 98, Windows NT 4.0. Control centralizado de la división del túnel

• Microsoft PPTP/MPPE

• Microsoft L2TP/IPsec para Windows 2000

Protocolos de tunneling

• IPsec, PPTP, L2TP, L2TP/IPsec, Ipsec con NAT transparente Cifrado/autenticación

• IPsec Encapsulating Security Payload (ESP) utilizando DES/3DES (56/168 bits) con MD5 o SHA, MPPE utilizando RC4 de 40/128 bits Gestión de llaves

• Internet Key Exchange (IKE)

Protocolos de enrutamiento

• RIP, RIP2, OSPF, descubrimiento automático de extremo, conversión de direcciones de red (NAT), enrutamiento entre dominios sin clases (CIDR)

Compatibilidad con otros fabricantes

• iPass Ready, Funk Steel Belted RADIUS certified, NTS TunnelBuilder VPN Client (Mac y Windows), Microsoft Internet Explorer, Netscape Communicator, Entrust, GTE Cybertrust, Baltimore, RSA Keon, Network Associates PGP VPN

Gran nivel de disponibilidad

• Protocolo VRRP para recuperación ante fallos y redundancia con chasis múltiples

• Sondeo de destinos para recuperación para la recuperación de fallos y restablecimiento de conexiones basándose en el cliente

• Módulos SEP (opcionales), fuentes de alimentación y ventiladores redundantes (Cisco VPN 3015-3080)

**Gestión**

Configuración

• La interfaz de gestión integrada es accesible vía puerto de consola, Telnet, y Secure HTTP

• El acceso del administrador se puede configurar para cinco niveles de autorización

• La política de gestión basada en roles separa las funciones de administración para el proveedor de servicios y para el usuario final

Supervisión

• Registro y notificación de eventos por correo electrónico (SMTP)

• Copia de seguridad automática de los ficheros de eventos por FTP

• Compatibilidad con SNMP MIB-II

• Interrupciones SNMP configurables

• Salida del syslog

• Estado del sistema

• Datos de sesión

• Estadísticas generales Seguridad

Servidores de autenticación y contabilidad

• Compatibilidad con servidores externos de autenticación redundantes:

– RADIUS (Remote Authentication Dial-In User Service)

– Autenticación de dominio Microsoft NT

– RSA Security Dynamics (SecurID Ready)

• Servidor interno de autenticación para un máximo de 100 usuarios

• Certificados digitales X.509v3

• Contabilidad RADIUS

Filtrado de paquetes basados en Internet

• Dirección IP de fuente y destino

• Tipo de puerto y protocolo

• Protección de los fragmentos

• Filtrado de sesión FTP

Gestión de normativas

• Por usuario individual o por grupo de usuarios

– Perfiles de filtrado

– Temporizadores de sesión en espera y valor máximo

– Control de acceso por hora y fecha

– Protocolo para la conexión en túnel y perfiles de autorización de seguridad

## BIBLIOGRAFÍA

**[1]** Karanjit Siyan, Chris Hare. "Firewalls y la Seguridad en Internet". Prentice-Hall, Segunda Edición. 1997.

**[2]** John R. Vacca. "Los secretos de la Seguridad en Internet". Ediciones Anaya Multimedia, S.A, 1997.

**[3]** Marcus Goncalves and Steven Brown. Check Point Firewall-1 Administration Guide. McGrawHill, 1999.

**[4]** Douglas E. Comer. "Internetworking with TCP/IP. Volume 1: Principles, Protocols & Architecture". Prentice Hall, 3rd edition, 1995.

**[5].** Robert L. Ziegler. "Linux Firewalls". New Riders, 2nd edition, 2001.

**[6].** Tom Shaughnessy con Toby Velte. "Manual CISCO, Diseñe y Configure redes usando hardware y software de CISCO". Mc Graw Hill, 2000.

**[7]** Documentación propietaria de Motorola. "Manuel 4824o47b.pdf" Transmisión de Datos por circuitos y paquetes

**[8]** Información de la documentación Web de Cisco. Manual de Encriptación VPN (www.cisco.com/documentation/vpn )

**[9]** Información de la documentación Web de Checkpoint. Documentación sobre Firewall-1 (www.checkpoint.com/firewall-one), seguridad de la información empleando Firewall-1 (cortafuegos)