# REDES INTELIGENTES

# SERVICIO RED PRIVADA VIRTUAL

**GIOVANNA DELGADO HURTADO**

**POPAYAN**
**UNIVERSIDAD DEL CAUCA**
**FACULTAD DE INGENIERIA ELECTRONICA Y TELECOMUNICACIONES**
**GRUPO DE REDES INTELIGENTES**
**2002**

# REDES INTELIGENTES

# SERVICIO RED PRIVADA VIRTUAL

**GIOVANNA DELGADO HURTADO**

**Anexos del trabajo de grado presentado como requisito para optar al título de Ingeniero en Electrónica y Telecomunicaciones**

**Director:**
**Mg. RAFAEL RENGIFO**

**POPAYAN**
**UNIVERSIDAD DEL CAUCA**
**FACULTAD DE INGENIERIA ELECTRONICA Y TELECOMUNICACIONES**
**GRUPO DE REDES INTELIGENTES**
**2002**

# TABLA DE CONTENIDO

# LISTA DE FIGURAS

# LISTA DE TABLAS

# ANEXO A – EJEMPLO DE UN PLAN DE NUMERACION PRIVADO

## A.1. REDES PUBLICAS CON PBX

Una corporación tiene en su red PABXs con números de extensiones de 3 dígitos, 4 dígitos y 5 dígitos y quiere instalar un servicio VPN (VPN A) en su red. Para esto, le solicita al operador de red instalar una Red Privada Virtual con un Plan de Numeración Privado (PNP) que incluye números PNP abreviados de 3 dígitos y números PNP de longitud completa de 7 dígitos.

La VPN A recibe el código de identificación VPN 3000.

La asignación de números de identificación se realiza de la siguiente forma (Ver *Tabla A.1*):

| COMENTARIOS | NUMERO PNP | NUMERO DEL DIRECTORIO PUBLICO | NUMERO DE EXTENSION |
|---|---|---|---|
| PABX 1: | 22 2xxxx | 92 66 2xxxx | 2xxxx |
| (On-net) | 22 4xxxx | 92 66 4xxxx | 4xxxx |
| | 22 6xxxx | 92 66 6xxxx | 6xxxx |
| | | | |
| PABX 2: | 235 2xxx | 92 413 2xxx | 2xxx |
| (On-net) | 235 3xxx | 92 413 3xxx | 3xxx |
| | | | |
| PABX 3: | 2701 yxx | 92 4808 yxx | yxx |
| (On-net) | | | |
| | | | |
| PABX 4: | 8999 yxx | 91 3 711 yxx | yxx |
| (Virtual On-net) | | | |
| | | | |
| Número clave On-net/Off-net | 000 | | |
| | | | |
| Números PNP abreviados | 1xx a 9 xx | | |

(con x=0..9 y=1..9)

*Tabla A.1. Ejemplo de Plan de Numeración Privado.*

- A los números de extensiones de la PABX 1 de 5 dígitos se le asignan números de identificación de 2 dígitos (por ejemplo 22).
- A los números de extensiones de la PABX 2 de 4 dígitos se le asignan números de identificación de 3 dígitos (por ejemplo 235).
- A los números de extensiones de la PABX 3 de 3 dígitos se le asignan números de identificación de 4 dígitos (por ejemplo 2701 y 8999).

Cada número de identificación de la PABX seguido por el número de la extensión forma el número PNP de 7 dígitos de una extensión en la VPN A.

Los dígitos 000 son utilizados como números claves on-net (acceso) y off-net (escape) de la VPN A.

Los códigos de acceso a la VPN deben estar disponibles en la VPN. La mayoría de las veces esto es una ventaja para mantener el plan de numeración de la PABX separado del plan de numeración de la VPN, por ejemplo, para evitar cambios en un sistema de numeración ya existente de una PABX, cuando sea necesario una expansión. En este caso es necesario instalar en la PABX un código breve de acceso a la VPN. En este ejemplo, el código * denota el acceso a la VPN en las PABXs 1, 2 y 3 (*Tabla A.2*).

| COMENTARIOS | CODIGO | CONVERTIDO AL NUMERO (PARCIAL) DE DIRECTORIO PUBLICO |
|---|---|---|
| Acceso a la VPN | * | 9907-3000 |
| Clave Off-net | 0 | 9907-3000-000 |

*Tabla A.2. Códigos de Acceso a la VPN.*

Para un usuario de la VPN en la red A, el plan de numeración puede ser representado tal como se muestra en la *Fig. A.1.*

La VPN A debe ser accesada desde una de las PABXs marcando el símbolo *. Opcionalmente, después de que el símbolo * ha sido marcado desde una PABX, un segundo tono de marcación debe ser enviado, para indicarle al usuario VPN que un número PNP puede ser marcado. Si el destino se encuentra dentro de otra PABX, el usuario VPN debe marcar el respectivo código de identificación de la PABX seguido por el número de la extensión.

Si un usuario VPN quiere alcanzar una línea pública (llamada on-net a off-net), se debe marcar el dígito 0 primero. La PABX convierte este número en un número de directorio de la Red Inteligente, la cual direcciona la lógica del servicio para llamadas on-net a off-net en la VPN. En este momento, la Red Inteligente le pregunta al usuario VPN el número del directorio público al que desea llamar. Alternativamente, el usuario podría marcar *000 en vez de 0.

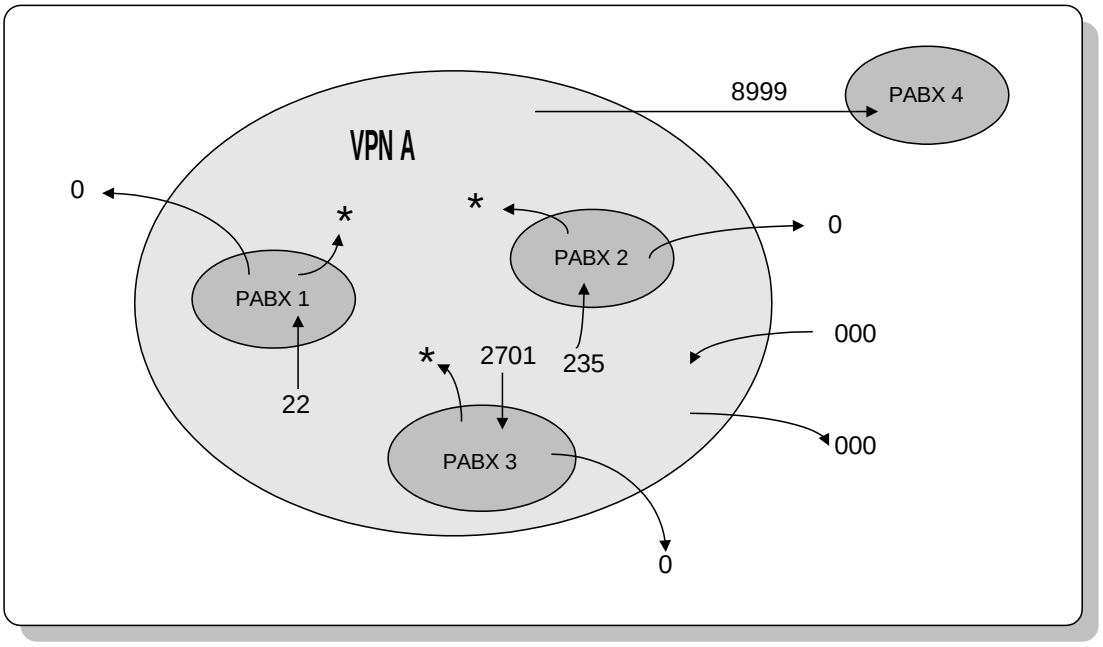



*Fig. A.1 Ejemplo de Plan de Numeración Privado.*

Si un usuario llama desde una línea off-net, la VPN puede ser accesada introduciendo el código de acceso, el código de identificación y el código de acceso remoto 000 seguido por el número PNP personal asignado y el PIN requerido para autenticación.

## A.2. SECUENCIAS DE MARCACION

A continuación, se describen algunas secuencias de marcación necesarias para establecer conexiones para los diferentes tipos de llamadas VPN, basados en el ejemplo dado en la sección A.1.

En los siguientes ejemplos, se utiliza el sistema de anuncios de la Red Inteligente, el cual puede ser adicionado por el proveedor del servicio.

### *A.2.1. CONEXIONES ON-NET A (VIRTUAL) ON-NET*

Un usuario VPN quiere llamar a la extensión 23456 de la PABX 1 (código de acceso 22), desde una línea on-net de la PABX 2. La marcación del usuario, la marcación real de la PABX y las acciones tomadas por la Red Inteligente se pueden observar en la *Tabla A.3*.

| MARCACIÓN USUARIO | MARCACION PABX | ACCION RI | SISTEMA ANUNCIOS RI |
|---|---|---|---|
| * 22 23456 | 9907 3000 22 23456 | Reconoce el número como on-net. | |
| | | Establecimiento de la conexión al número de directorio público 92 662 3456 | |

*Tabla A.3. Conexión on-net a (virtual) on-net.*

### *A.2.2. CONEXIONES ON-NET A OFF-NET*

Un usuario VPN quiere llamar al número de directorio público 97 620 8740 desde una línea on-net de la PABX 2. (Ver *Tabla A.4*)

| MARCACIÓN USUARIO | MARCACION PABX | ACCION RI | SISTEMA ANUNCIOS RI |
|---|---|---|---|
| 0 | 9907 3000 000 | Reconoce : número on-net acceso a VPN. | |
| | | Reconoce : código off-net 000.<br>El usuario tiene autorización para hacer la llamada off-net? Sí. | |
| | | | "Por favor introduzca el número de directorio público y presione la tecla #. |
| 97 62 08740#<br>(DTMF) | | Reconoce : destino nacional.<br>El usuario tiene autorización para realizar llamadas off-net nacionales? Sí. | |
| | | Conexión establecida. | |

*Tabla A.4. Conexión on-net a off-net.*

Un usuario VPN quiere llamar a una línea off-net 8895621 en la red local desde una línea on-net de la PABX 2. (Ver *Tabla A.5*).

| MARCACIÓN USUARIO | MARCACION PABX | ACCION RI | SISTEMA ANUNCIOS RI |
|---|---|---|---|
| 0 | 9907 3000 000 | Reconoce : número on-net. | |
| | | Reconoce : código off-net 000.<br>El usuario tiene autorización para hacer la llamada off-net? Sí. | |
| | | | "Por favor introduzca el número de directorio público y presione la tecla #. |
| 8895621#<br>(DTMF) | | Reconoce : número de directorio sin código local de área.<br>Extrae el código del área desde el número del abonado llamante. | |
| | | Conexión establecida 92 8895621 | |

*Tabla A.5. Conexión on-net a off-net, código de área local de línea off-net no marcado.*

El usuario VPN no necesita marcar el código de área en el caso de las llamadas off-net locales. El sistema de Red Inteligente reconoce que el código de área local ha sido omitido y lo adiciona analizando el número de abonado llamante. El uso de esta función es una opción del operador de la red y es fijada por el fabricante durante la configuración del servicio VPN. Si la función es utilizada, el SCP requiere una lista de todos los códigos de área local válidos.

Para establecer llamadas on-net a off-net, el usuario VPN necesita la autorización correspondiente. La autorización para alcanzar todos los destinos off-net puede también ser limitado a destinos locales, nacionales o internacionales. Para este propósito, el SCP requiere una lista de los puntos de código PNP, marcados respectivamente.

### *A.2.3. CONEXIONES OFF-NET A (VIRTUAL) ON-NET*

Un usuario VPN con el número PNP 235 2134 se encuentra en un viaje de negocios y quiere llamar a su superior cuyo número PNP es 235 3988, desde una línea off-net en el aeropuerto.

Como una opción del proveedor del servicio, se presentan dos diferentes procedimientos de acceso a la VPN desde líneas off-net:

- Acceso vía un número clave on-net (código de acceso remoto) (Ver *Tabla A.6*)
- Acceso implícito (Ver *Tabla A.7*).

El tipo de acceso utilizado es fijado por el fabricante (por ejemplo Siemens) durante la configuración del servicio VPN.

| MARCACIÓN USUARIO | ACCION RI | SISTEMA ANUNCIOS RI |
|---|---|---|
| 9907 3000 000 | Reconoce : número clave on-net 000. | |
| | | “Por favor introduzca su número PNP para identificación y presione la tecla #. |
| 235 2134# (DTMF) | | |
| | | “Por favor introduzca su PIN y presione la tecla #. |
| 9581# (DTMF) | Reconoce : números PNP y PIN son válidos.<br>El usuario tiene autorización para acceso remoto? Sí. | |
| | | “Por favor introduzca el número PNP deseado o la clave off-net y presione la tecla #. |
| 235 3988# (DTMF) | Conexión establecida:<br>92 413 3988 | |

*Tabla A.6. Conexión off-net a (virtual) on-net, acceso vía un número de clave on-net.*

Con acceso implícito, el usuario no requiere usar un número de clave on-net (código de acceso remoto), pero marca el número PNP deseado directamente como en el caso de una conexión on-net a on-net.

| MARCACIÓN USUARIO | ACCION RI | SISTEMA ANUNCIOS RI |
|---|---|---|
| 9907 3000 235 3988 | Reconoce: número de abonado llamado es off-net. | |
| | | “Por favor introduzca su número PNP para identificación y presione la tecla #. |
| 235 2134# (DTMF) | | |
| | | “Por favor introduzca su PIN y presione la tecla #. |
| 9581# (DTMF) | Reconoce: números PNP y PIN son válidos.<br>El usuario tiene autorización para acceso remoto? Sí. | |
| | Conexión establecida:<br>92 413 3988 | |

*Tabla A.7. Conexión off-net a (virtual) on-net, acceso implícito.*

### *A.2.4. CONEXIONES OFF-NET A OFF-NET*

Un usuario VPN con el número PNP 235 2134 se encuentra en un viaje de negocios y quiere llamar a un cliente con número de directorio público 901 635 7420421, a través de la VPN desde una línea off-net en el aeropuerto. Se presentan dos diferentes procedimientos de acceso a la VPN desde líneas off-net:

- Acceso vía un número clave on-net (código de acceso remoto) (Ver *Tabla A.8.*)
- Acceso implícito (Ver *Tabla A.9.)*

| MARCACIÓN USUARIO | ACCION RI | SISTEMA ANUNCIOS RI |
|---|---|---|
| 9907 3000 000 | Reconoce: número de abonado llamante es off-net.<br>Reconoce: Número de clave on-net 000. | |
| | | "Por favor introduzca su número PNP para identificación y presione la tecla #. |
| 235 2134# (DTMF) | | |
| | | "Por favor introduzca su PIN y presione la tecla #. |
| 9581# (DTMF) | Reconoce: números PNP y PIN son válidos.<br>El usuario tiene autorización para acceso remoto? Sí. | |
| | | "Por favor introduzca el número PNP deseado o la clave off-net y presione la tecla # ". |
| 000# (DTMF) | Reconoce: número clave off-net 000 | |
| | El usuario tiene autorización para establecer conexiones off-net a off-net? Sí. | |
| | | "Por favor introduzca el número de directo público deseado y presione la tecla # ". |
| 901 635 7420421# | El usuario tiene autorización para realizar llamadas a destinos internacionales? Sí. | |
| | Conexión establecida:<br>901 635 7420421 | |

*Tabla A.8. Conexión off-net a off-net, acceso vía números de clave on-net y off-net.*

Con acceso implícito, el usuario no tiene que utilizar un número de clave on-net (código de acceso remoto), simplemente marca el número de clave off-net (código de escape a off-net), como en el caso de una conexión on-net a off-net.

| MARCACIÓN USUARIO | ACCION RI | SISTEMA ANUNCIOS RI |
|---|---|---|
| 9907 3000 000 | Reconoce: número de abonado llamante es off-net. | |
| | | "Por favor introduzca su número PNP para identificación y presione la tecla #. |
| 235 2134# (DTMF) | | |
| | | "Por favor introduzca su PIN y presione la tecla #. |
| 9581# (DTMF) | Reconoce: números PNP y PIN son válidos.<br>El usuario tiene autorización para establecer conexiones off-net a off-net? Sí. | |
| | | "Por favor introduzca el número de directo público deseado y presione la tecla # ". |
| 901 635 7420421# | El usuario tiene autorización para realizar llamadas a destinos internacionales? Sí. | |
| | Conexión establecida:<br>901 635 7420421 | |

*Tabla A.9. Conexión off-net a off-net, acceso implícito.*

Similar al establecimiento de conexiones on-net a off-net, el usuario VPN no requiere introducir el código de área para destinos que se encuentran en la misma área donde fue originada la llamada. El sistema de Red Inteligente reconoce que el código de área local ha sido omitido y lo adiciona analizando el número de abonado llamante.

Para establecer conexiones off-net a off-net, el usuario VPN requiere las autorizaciones correspondientes. Las autorizaciones para alcanzar destinos off-net pueden ser limitadas a destinos locales, nacionales e internacionales.

### *A.2.5. ALTERNATIVAS PARA PROCECIMIENTOS DE AUTENTICACIÓN*

Como una opción del proveedor de servicios, el servicio VPN puede ser configurado por el fabricante de tal forma que el número PNP y el PIN sean entrados juntos en un sólo paso durante la autenticación del abonado llamante. Si esta opción se escoge, la autenticación en los diálogos anteriores pueden ser desarrollados como se muestra en la *Tabla A.10*.

| MARCACIÓN USUARIO | ACCION RI | SISTEMA ANUNCIOS RI |
|---|---|---|
| | | "Por favor introduzca su número PNP seguido por su PIN para identificación y presione la tecla #. |
| 23521349581# (DTMF) | Reconoce : número PNP y PIN son válidos. | |

*Tabla A.10. Alternativa de procedimiento de autenticación.*

## A.3. AUTORIZACION DE LLAMADAS

Cada usuario VPN puede tener asignadas autorizaciones las cuales definen los tipos de llamadas en la VPN que el usuario puede realizar.

Un suscriptor de servicio determina en que VPNs será utilizada la característica "autorización para tipos de llamadas".

### *A.3.1. AUTORIZACIÓN DE LLAMADAS SALIENTES DESDE LINEAS ON-NET*

Esta autorización es la autorización básica para llamadas salientes. Puede ser asignada en tres niveles: "completa", "limitada" y "ninguna". Las posibles autorizaciones para los diferentes tipos de llamadas se muestran en la *Tabla A.11*.

| | Autorización | | |
|---|---|---|---|
| | **Completa** | **Limitada** | **Ninguna** |
| On-net a on-net<br>On-net a virtual on-net | + | + | - |
| On-net a off-net | + | - | - |

+ : permitida -: no permitida

*Tabla A.11. Posibles autorizaciones para llamadas salientes desde líneas on-net.*

### *A.3.2. AUTORIZACIÓN DE LLAMADAS SALIENTES DESDE LINEAS OFF-NET*

Esta autorización es la autorización básica para llamadas de “acceso remoto”. Puede ser asignada en tres niveles: “completa”, “limitada” y “ninguna”. En la *Tabla A.12* se pueden observar las posibles autorizaciones para los diferentes tipos de llamadas.

| | **Autorización** | | |
|---|---|---|---|
| | **Completa** | **Limitada** | **Ninguna** |
| Off-net a on-net<br>Off-net a virtual on-net | + | + | - |
| Off-net a off-net | + | - | - |

+ : permitida -: no permitida

*Tabla A.12. Posibles autorizaciones para llamadas salientes desde líneas off-net.*

### *A.3.3. AUTORIZACIÓN DE RANGOS DE DESTINOS PARA LLAMADAS OFF-NET*

Esta autorización define el rango de destinos off-net con los cuales un usuario VPN puede establecer una conexión. La autorización para rangos de destinos es valida para conexiones on-net a off-net y off-net a off-net. En la *Tabla A.13* se muestran los rangos de destinos que pueden ser asignados.

| **Rango de destino** | **Explicación** |
|---|---|
| Internacional | Sin restricciones |
| Continental | Sólo se permiten destinos off-net continentales. |
| Nacional | Sólo se permiten destinos off-net nacionales. |
| Local | Sólo se permiten destinos en el área local. |

*Tabla A.13. Posibles rangos de destinos para llamadas off-net.*

El suscriptor del servicio determina en que VPNs es posible utilizar la característica “autorización para rangos de destinos para llamadas off-net”. Para esta característica, el SCP requiere una lista de puntos de código PNP, marcados adecuadamente.

### *A.3.4. AUTORIZACIÓN DE LLAMADAS ENTRANTES*

Esta autorización corresponde a la autorización básica para llamadas entrantes. Puede ser asignada en dos niveles: “Sí” o “No”. En caso de ser seleccionado “No”, el usuario VPN no puede recibir llamadas de ningún tipo.

# ANEXO B - TENDENCIAS EVOLUCIONARIAS EN RI

Como hemos visto hasta ahora, las Redes Inteligentes, ofrecen estándares abiertos para redes de telecomunicaciones, y entre sus objetivos se encuentra la creación rápida de servicios, así como de interfaces estandarizadas y abiertas para implementaciones de múltiples vendedores.

Aunque las RI ofrecen grandes ventajas competitivas a los proveedores de servicios, cada día son mayores los requerimientos de los usuarios de las redes de telecomunicaciones. Por ejemplo, la movilidad de los usuarios de servicios, la administración del subscriptor y de la red total y la distribución de la lógica y los datos del servicio dentro de una red de telecomunicaciones son temas que se están evaluando y desarrollando en múltiples compañías, originando nuevos estándares y tecnologías post-RI tales como UMTS (*Universal Mobile Telecommunication System*) y NGN (*Next Generation Networks*).

En este anexo se presenta una breve reseña de la evolución de los estándares de telecomunicaciones y se analizan las diferentes tendencias evolucionarias que buscan mejorar las Redes Inteligentes y que sirven como base para el desarrollo de las Redes de Próxima Generación, las cuales proveen un ambiente de control común, unificado y flexible para soportar múltiples tipos de servicios y aplicaciones sobre múltiples tipos de redes de transporte.

## B.1. ESCENARIOS DE ESTANDARIZACION FUTUROS

Las telecomunicaciones y las tecnologías de información continuarán evolucionando, creando posibilidades para aplicar nuevas tecnologías y nuevas líneas de estandarización *(Ver Fig. B.1.).*

Las principales tendencias de la computación, tal como la tecnología de objetos, y la computación distribuida, han sido verdaderamente reconocidos como las bases para las aplicaciones futuras de telecomunicaciones.

Las nuevas tendencias tecnológicas, tales como UMTS y NGN incorporan en sus arquitecturas los conceptos de las siguientes tecnologías:

- Tecnología distribuida de telecomunicaciones, estandarizada en las recomendaciones ODP (Procesamiento Abierto Distribuido) de la UIT-T.
- Tecnologías de administración de redes de telecomunicaciones, estandarizadas en las recomendaciones TMN (*Telecommunications Management Network*) de la UIT-T.

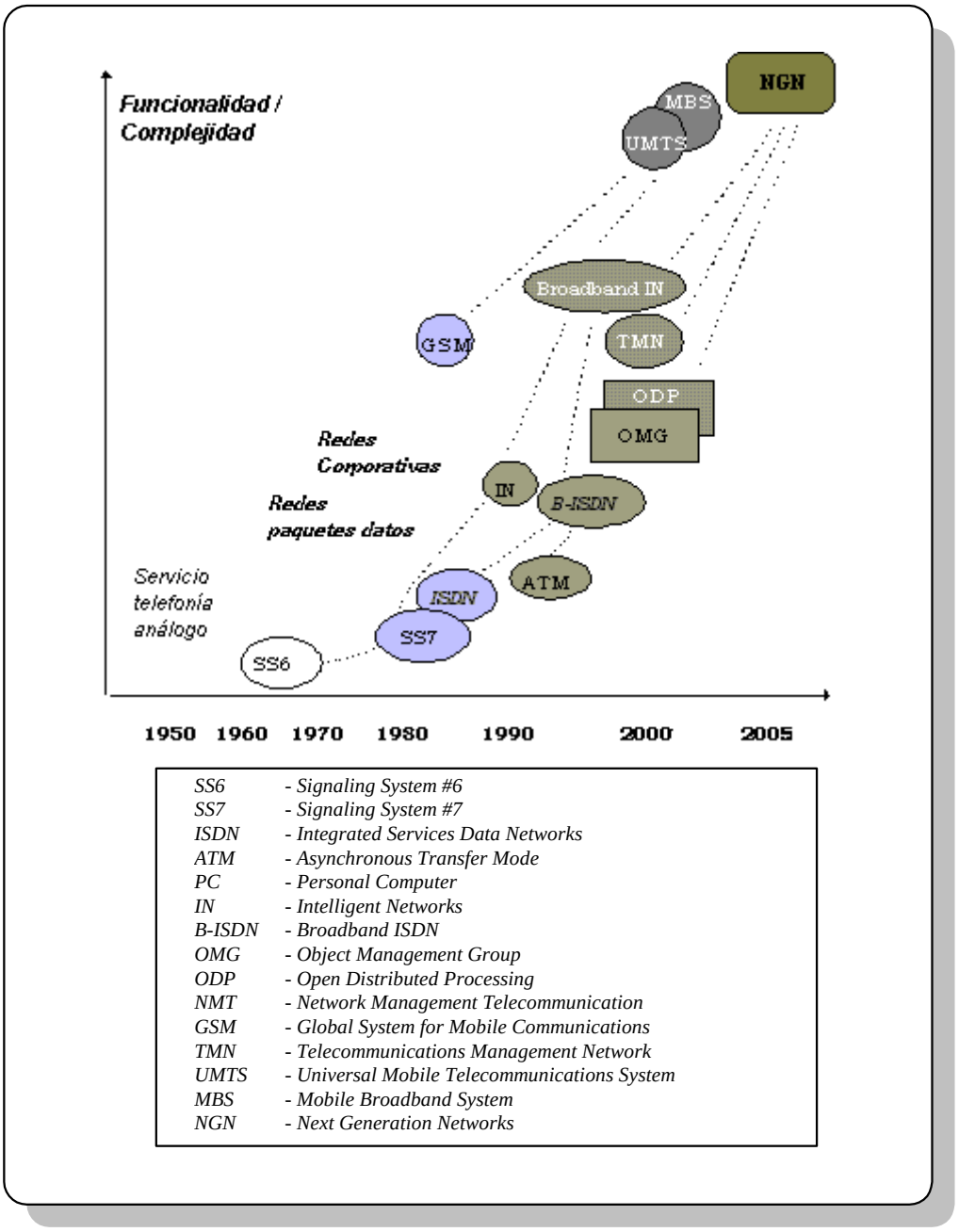



*Fig. B.1. La evolución de los estándares de telecomunicaciones y la incorporación de estándares de computación.*

- Tecnologías de banda ancha, estandarizadas en las recomendaciones RDSI-BA (Red Digital de Servicios Integrados de Banda Ancha) de la UIT-T e incorporándolas con la "Red Inteligente de Banda Ancha" – (*Broadband IN*).

- Tecnología TINA definida y consolidada por el Consorcio TINA (TINA-C). Aunque el consorcio fue disuelto en Diciembre de 2000, sus resultados fueron transferidos a los cuerpos de estandarización OMG, ITU-T y 3GPP (UMTS), para formar las bases de sus estándares / especificaciones o para ser incorporados como parte de ellas.

Las Tecnologías de Banda Ancha son una de las principales tendencias en telecomunicaciones. Con tecnologías de banda ancha tales como ATM (*Asynchronous Transfer Mode*), será posible crear avanzados servicios interactivos de telecomunicaciones, los cuales, hasta ahora, han sido imposibles debido a la insuficiencia de ancho de banda de las redes actuales.

El paso siguiente en el desarrollo de las Redes Inteligentes es la incorporación de la tecnología de conmutación ATM para formar la "Red Inteligente de banda Ancha" (BIN – *Broadband IN*). Además, simultáneamente, la tendencia en redes de telecomunicaciones es hacia la separación de las tecnologías de conmutación y de control de llamadas.

Las comunicaciones móviles han revolucionado la forma en que las personas se comunican. El rápido incremento en el número de subscriptores a la GSM (*Global System for Mobile Communications*) y otros sistemas celulares alrededor del mundo, ha indicado claramente que la movilidad será la base para las comunicaciones personales futuras.

Adicionalmente, estándares como UMTS *(Universal Broadband System)* están incorporando RDSI de banda ancha con tecnologías móviles y redes de telecomunicaciones fijas de tercera generación para formar sin mayor costo Redes Universales de Telecomunicaciones *(Ver Fig. B.1).*

## B.2. EVOLUCION DE LAS REDES INTELIGENTES

El increíble crecimiento de Internet, junto con el desarrollo de redes de alta velocidad, ha impulsado el cambio desde las redes de voz de circuitos conmutados, como PSTN, hacia redes conmutadas de paquetes basadas en las tecnologías ATM e IP. Estas redes de paquetes pueden manejar mucho más tráfico que la PSTN y también pueden soportar sofisticados servicios multimedia (incluyendo pesadas aplicaciones de video).

En esta tendencia hacia las redes de paquetes, las Redes Inteligentes juegan un papel fundamental en la evolución de las redes hasta llegar a las Redes de Próxima Generación (NGN – Next Generation Network).

Sin embargo, las Redes Inteligentes existentes cuentan con algunas limitaciones técnicas y comerciales que deben ser superadas para dar como resultado una arquitectura más abierta y flexible.

Entre las limitaciones principales podemos encontrar:

- La mayoría de las implementaciones de RI continúan estando basadas en los estándares CS-1, que limitan la lógica de los servicios de RI a controlar la configuración de la llamada de voz en respuesta a disparadores (*triggers*) activados en los conmutadores (*switches*) de la red. Es necesario implementar las capacidades de la RI CS-2 y CS-3 para permitir el control de llamadas a través de su duración y para introducir soporte para llamadas con múltiples conexiones y múltiples participantes, implicando el intercambio de datos multimedia.

- La manera en la que los servicios de RI son desplegados y accesados debe ser más abierta; por ejemplo, la lógica del servicio debería ser accesible desde terminales Internet, y tener componentes residiendo tanto en los Puntos de Control de Servicio (SCP) como en los nodos Internet.

- La lógica del servicio debería ser independiente de las arquitecturas de software / hardware (en muchos casos propietarias) y de las variaciones en las versiones de los protocolos de comunicaciones. Esto podría solucionarse utilizando soluciones de middleware (como CORBA) para la implementación de elementos de RI.

- Se requiere un desarrollo más rápido de nuevos servicios. Esto se ve limitado por la falta de madurez de las metodologías y las herramientas para la creación y la validación de los servicios y a la creación de los componentes de los servicios sin pensar en su reutilización o personalización.

- La falta de interfaces estandarizadas para la creación, administración y desarrollo de servicios, que puedan ser utilizadas por personas no especializadas para desarrollar servicios de RI utilizando métodos y herramientas de desarrollo de software comercial.

Todo lo anterior nos conduce a que los requerimientos claves para futuros desarrollos de RI son: que los clientes puedan tener acceso a una variedad más amplia de servicios, en una variedad más amplia de maneras, y que puedan personalizar servicios existentes o crear nuevos tan simple, rápida y rentablemente como sea posible. Esto requiere que los operadores tengan facilidades de administración, desarrollo y creación de servicios abiertos y eficientes que sean integrados en las plataformas de servicios de RI.

Las siguientes tendencias tecnológicas buscan mejorar las capacidades de las Redes Inteligentes y tendrán un rol importante en la evolución hacia las Redes de Próxima Generación:

- Integración entre las funcionalidades de RI y las capacidades de Internet, para producir Servicios Híbridos.

- Especificación de APIs de control de servicios orientados a objetos que facilitaran el acceso, control y configuración de los servicios de RI.

- Desarrollo de Redes Inteligentes Distribuidas mediante la utilización de nuevas tecnologías de middleware orientadas a objetos y las tecnologías de Agentes Móviles.

## B.3. REDES HÍBRIDAS (IN – INTERNET)

Uno de los primeros pasos evolutivos de las Redes Inteligentes hacia el desarrollo de los servicios del futuro, es su interrelación con Internet para ofrecer Servicios Híbridos.

Internet puede ofrecer a las Redes Inteligentes grandes mejoras en los siguientes temas, que a su vez ofrecen a los carriers nuevas e inmediatas fuentes de negocios:

- *Administración de Servicios Via Web* - La Función de Agente de Administración de Servicios (**SMAF** – *Service Management Agent Function*) en lugar de estar basada en un terminal dedicado, puede estar ubicada en un Servidor sobre Internet ofreciéndole al cliente una interfaz de administración del servicio más flexible y conveniente a través de un Web browser. Con esto, se puede extender la personalización de los servicios a cualquier persona con un computador y un acceso a Internet.

- *Explotación de los Recursos de Datos de Internet* – La Función de Datos de Servicio (**SDF** – *Service Data Function*) podría ser implementada en Internet. La Recomendación X.500 de la ITU-T define un servicio de directorio para la interconexión de sistemas abiertos, que puede ser accesado a través de protocolos abiertos como LDAP y X.519 DAP, convirtiendo a Internet en una ubicación viable para los datos de suscripción, de usuario y de servicio de una Red Inteligente. En el Conjunto de Capacidades CS-2 de RI de la ITU-T, se utiliza un subconjunto del protocolo X.519 DAP para definir la interfaz SCF-SDF.

- *Nuevas aplicaciones para Recursos Especializados* – Nuevas capacidades de la Función de Recursos Especializados (**SRF** – *Specialized Resource Function*) pueden ser proporcionadas a través de Internet. Por ejemplo, en el caso del acceso al contenido de una página Web a través de un teléfono de la PSTN, el contenido de la página Web podría ser proporcionado por medio de la síntesis del lenguaje (*speech sintesis*) desde un SRF.

- *Invocación de Servicios y Control de Llamadas desde y hacia Internet* - Dos grupos de la IETF están trabajando en la interacción de la Función de Control del Servicio (**SCF** – *Service Control Function*) con Internet, con el fin de invocar y controlar servicios de la PSTN desde Internet (PINT) o para invocar y controlar servicios de Internet desde la PSTN (SPIRITS). Ya que estos grupos han logrado una gran acogida en la implementación de nuevos servicios, vamos a describirlos en detalle a continuación.

### *B.3.1. PINT (PSTN / INTERNET INTERNETWORKING)*

El grupo de trabajo PINT es parte del Área de Transporte de la IETF, fue creado en 1997 y se enfoca en como las aplicaciones de Internet pueden requerir y enriquecer los servicios de telecomunicaciones PSTN.

El protocolo PINT permite la invocación de servicios de telefonía (PSTN) desde terminales en un ambiente de red basado en IP, por lo que los servicios son considerados servicios híbridos (involucran dos tipos de redes diferentes, una red IP y la PSTN).

El protocolo PINT representa servicios híbridos y constituye una solución intermedia hacia las Redes de Próxima Generación (NGN).

El escenario del servicio es como sigue (*Fig. B.2*): un host en la red IP transmite una petición de servicio a un servidor PINT, que retransmite la petición al recurso relevante de la red PSTN, tal como un nodo implementando una Función de Control de Servicio (SCF – Service Control Function), que entonces ejecuta el servicio solicitado, reportando posiblemente el estado de la sesión del servicio de nuevo al terminal IP que origina la petición.

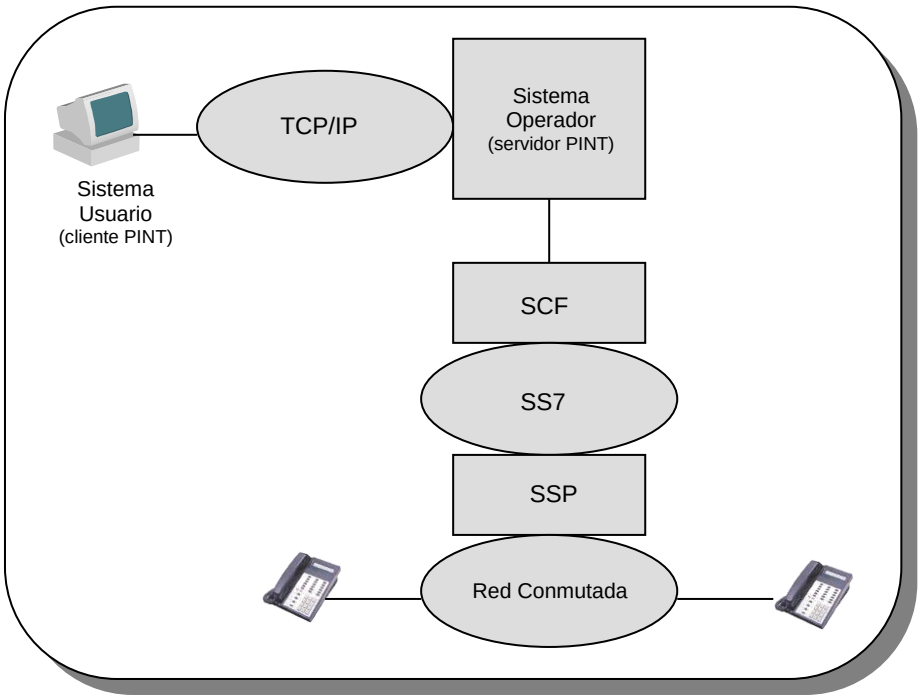



*Fig. B.2. La arquitectura PINT de IETF.*

### *B.3.1.1. Metas de PINT*

El objetivo global de la iniciativa PINT es permitir la integración de los recursos de Internet y de los servicios de Telefonía. Adicionalmente busca estandarizar eficientemente el acceso desde el Internet hasta los SCF de la RI. También permitirá el desarrollo de servicios que se ejecutan parcialmente en el dominio de Internet y parcialmente en el dominio de la telefonía tradicional.

Adicionalmente, PINT está siendo activamente considerado por ITU-T SG11 para su inclusión en la arquitectura funcional CS-4 de RI.

### *B.3.1.2. Servicios PINT*

El protocolo PINT se enfoca en un pequeño número de servicios significativos, los cuales pueden ser utilizados como bloques de construcción para muchos otros servicios:

- *Servicio Petición para Llamada (Request to Call)* – Permite a un usuario enviar una petición desde un host IP, el cual tiene el propósito de establecer una llamada de teléfono entre las dos partes. Este servicio se conoce con el nombre de "Click-to-Call".

- *Servicio Petición para Fax (Request to Fax)* – El requerimiento de un usuario para enviar un fax a una máquina de fax, se envía desde un host IP. Se dan muchas maneras para definir el contenido a ser enviado por fax. Podría ser por ejemplo, una página web localizada en algún lugar en la red o el contenido del mensaje SIP por si mismo. Por otra parte el contenido puede ser texto o imágenes. Es importante destacar que este servicio no es un servicio de Fax sobre IP (Fax over IP). Como todos los servicios PINT, la red IP se utiliza solamente para pedir el servicio, mientras que todos los detalles de la transmisión de fax son manejados por la red de teléfonos.

- *Servicio Petición para Hablar / Enviar / Escuchar Contenido* – También llamado *Petición para Escuchar Contenido (Request to Hear Content)*. Un requerimiento de un usuario es enviado desde un Host IP, lo que ocasiona que una llamada de teléfono sea hecha al usuario que realizó el requerimiento, con un cierto contenido para ser escuchado. Este contenido se puede designar a través de un URL por ejemplo, o puede estar contenido en el mismo requerimiento. Como para el servicio de Petición para Fax, el contenido puede ser texto o algún otro tipo de datos. Los detalles de la transmisión son manejados por la red telefónica PSTN. La manera en que se realiza la petición está fuera del alcance del protocolo PINT.

### *B.3.1.3. Arquitectura PINT*

De acuerdo con el RFC2848, los clientes y servidores PINT, son clientes y servidores SIP (Session Initiation Protocol – Protocolo de Iniciación de Sesión) de IETF.

En el modelo de llamada, un Host IP transmite una petición a un Servidor PINT para alcanzar un servicio telefónico. Esta petición se transporta de una manera segura y confiable hasta el servidor PINT mediante el protocolo SIP.

La invitación SIP contiene una descripción SDP (Session Description Protocol – Protocolo de Descripción de Sesión) de la sesión de red telefónica que es invocada o cuyo estado debe ser retornado.

Un sistema PINT está compuesto de 3 elementos básicos:

- Cliente PINT (Cliente Agente Usuario SIP).

- Gateway PINT (Servidor Agente Usuario SIP) – Corresponde a un servidor PINT capaz de interactuar con la red telefónica para proveer los servicios solicitados en una petición de un usuario.
- Sistema Ejecutivo.
- Adicionalmente se deben incluir Servidores Proxy SIP y Servidores de Redireccionamiento SIP.

El sistema de servidores PINT se representa como una nube, ya que una sencilla petición PINT podría pasar a través de una serie de servidores de localización, servidores proxy y servidores de redireccionamiento, antes de alcanzar el correcto Gateway PINT que pueda procesar la petición y entregarlo a la nube de la Red Telefónica PSTN.

Aunque el protocolo PINT es una extensión de SIP y SDP, las mejoras o adiciones especificadas por el protocolo PINT no intentan alterar la base de los protocolos SIP y SDP.

### *B.3.2. SPIRITS (SERVICE IN THE PSTN / IN REQUESTING INTERNET SERVICES)*

El grupo de trabajo SPIRITS "Servicios en PSTN/IN requiriendo servicios Internet" de la IETF, trabaja en como los servicios soportados por las entidades de red IP pueden ser inicializadas desde requerimientos de la RI.

Los servicios SPIRITS son aquellos que se originan en la PSTN y necesitan la interacción entre la PSTN e Internet. El servicio más importante es "Internet Call Waiting (ICW)", y otros servicios SPIRITS existentes son: "Caller-ID Delivery" y "Internet Call Forwarding".

- *ICW* – Permite a los suscriptores del servicio ser alcanzados por llamadas telefónicas entrantes mientras están navegando en Internet (a través de una conexión dial-up a su ISP). La llamada después de ser recibida puede ser enrutada a un casillero de mail, a una segunda línea, a una conexión de VoIP o a la línea actual. Esto significa que el servicio desarrolla una desconexión automática del ISP durante la llamada y la reestablece cuando la llamada es completada.

- *Caller-ID Delivery* – Permite al suscriptor ver el número, nombre, o ambos, de una llamada entrante, mientras está conectado a Internet.

- *Internet Call Forwarding* – Permite a un suscriptor del servicio enviar una llamada entrante a otro número telefónico mientras está conectado a Internet.

Si el suscriptor solo cuenta con una línea telefónica y la está utilizando para la conexión a Internet, entonces los dos últimos servicios mencionados corresponden a un sub-conjunto del servicio ICW.

### *B.3.2.1. Relación PINT – SPIRITS*

Existe una relación muy estrecha entre los protocolos PINT y SPIRITS, los cuales pueden complementar la implementación de sus servicios, y a su vez pueden ser combinados para proveer servicios mucho más poderosos.

Por ejemplo, en el caso del servicio ICW, PINT puede ser utilizado para propósitos de registro de usuarios al servicio; es decir, la personalización de los parámetros relacionados con el servicio. Cuando una conexión a Internet se hace, el usuario puede registrarse al servicio ICW, y el protocolo PINT es utilizado para invocar un servicio de RI que configura el estado actual del usuario.

Otro ejemplo, puede ser la utilización del servicio ICW (SPIRITS) después del servicio de "*Click-to-Call*" (PINT). El usuario utiliza el servicio Click to Call para solicitar información sobre un evento, continúa navegando y es informado de una llamada entrante a través del servicio ICW.

Estos dos protocolos dan una muy buena idea de los servicios de Próxima Generación que la convergencia entre las redes PSTN e IP puede ofrecer. Estas soluciones son muy útiles en los Ambientes Híbridos y constituyen un nivel intermedio hacia las Redes de Próxima Generación (NGN).

### *B.3.2.2. Arquitectura SPIRITS*

En la *Fig. B.3* se pueden observar las entidades involucradas en la arquitectura SPIRITS. A continuación se describen las entidades y las funciones involucradas en la arquitectura:

- *Función de Control de Servicio (SCF - Service Control Function)* – ejecuta la lógica del servicio, interactúa con las entidades en el dominio IP (por ejemplo, Gateway SPIRITS y Servidor PINT) a través del cliente SPIRITS, y da instrucciones a los switches de cómo completar la llamada.
- *Función de Conmutación de Servicio (SSF – Service Switching Function)* – es responsable por el reconocimiento de los triggers de RI y las interacciones con el SCF.
- *Cliente SPIRITS* – Es reponsable por recibir el requerimiento de la PSTN desde el SCF así como de enviar las respuestas de regreso.
- *Servidor PINT* – Recibe los requerimientos PINT desde el Cliente PINT y los envía a la PSTN para su ejecución sobre la interfaz E.
- *Gateway SPIRITS* – Está localizado con el Servidor PINT o Gateway PINT y sirve como un intermediario entre el Servidor SPIRITS y el Cliente SPIRITS a través de las interfaces B y C, respectivamente.
- *Cliente PINT* – Reside en el host IP del suscriptor y es responsable por todas las interacciones, (esto significa, notificación de llamada entrante y posterior tratamiento de la llamada) entre el suscriptor y el Gateway SPIRITS.

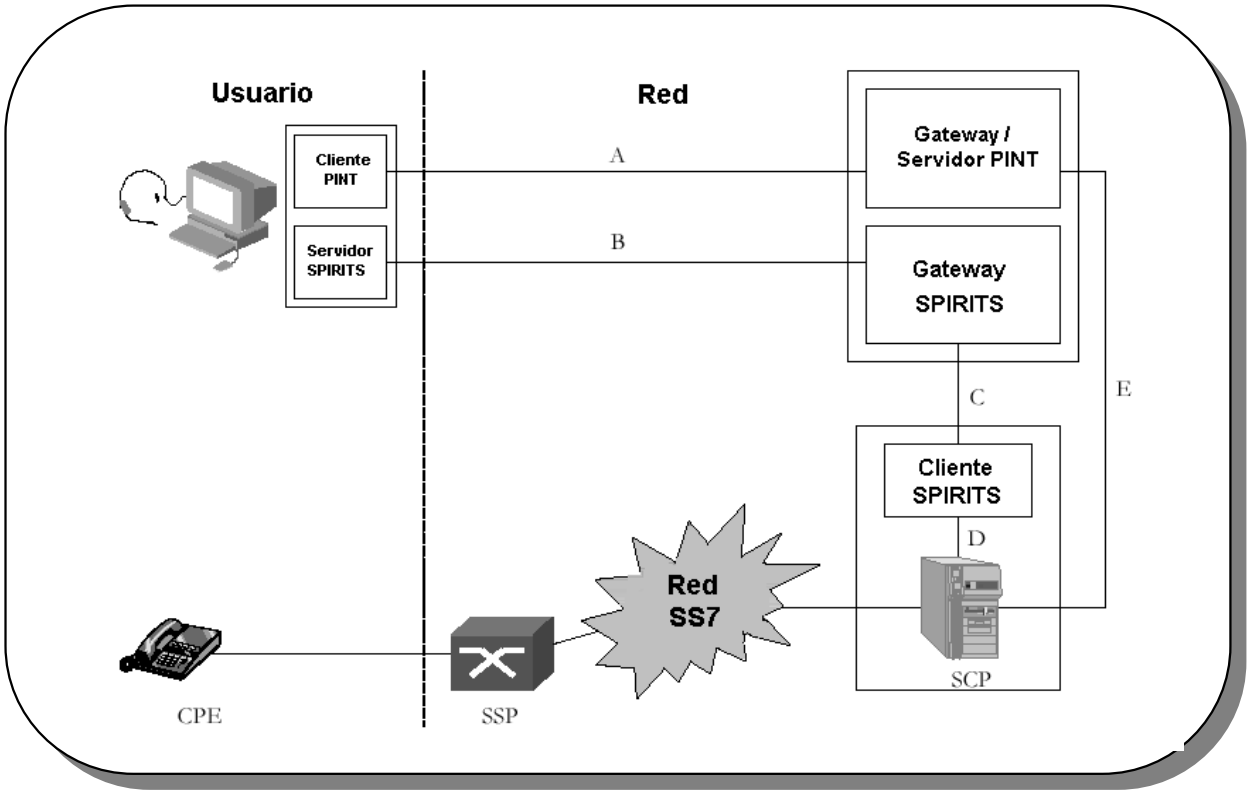



*Fig. B.3. Arquitectura SPIRITS.*

Considerando el ejemplo de ICW, el modelo de la llamada sería el siguiente:

- Un usuario A se encuentra navegando en Internet, y a través del protocolo PINT (cliente/servidor) se registra a un servicio ICW.
- Un usuario B inicia una llamada hacia B.
- Cuando el SSP detecta que el abonado llamado se encuentra ocupado, envía una pregunta (query) al SCP y espera por instrucciones del SCP.
- Cuando es activado (triggered) el SCP lanza el servicio ICW.
- La lógica del servicio gobierna la notificación de una llamada en espera para un suscriptor ICW en línea y las características de la llamada. Para hacer esto, puede instruir al cliente SPIRITS para desarrollar algunas otras acciones.
- Finalmente, el cliente/servidor SPIRITS son utilizados para decidir el futuro de la llamada dependiendo de la personalización del registro inicialmente realizada. Estas dos entidades pueden utilizar el protocolo SIP para comunicarse.
- Adicionalmente, el servidor SPIRITS puede monitorear el estado de la conexión de los clientes ICW registrados. Así, puede desactivar el servicio ICW para un cliente, tan pronto detecta que el cliente ha desactivado el servicio ICW o terminado la conexión Internet.

### *B.3.3. CS-3 / CS-4*

La ITU-T definió, por primera vez formalmente, la interacción de las Redes Inteligentes con las Redes IP en el Conjunto de Capacidades 3 (CS-3), en donde abordó de manera muy básica el estudio de los servicios de telecomunicaciones originados en una red IP y que requerían del soporte de la RI, pero con la restricción de que los servicios no estaban relacionados con contenido.

Las dos características de servicio definidas en esta recomendación fueron "Petición de Llamada – CSN" (RTCBC – Request to Call-CSN) y "Petición de Llamada de Consulta-CSN" (RQTCC – Request to Call Back-CSN), en las cuales un usuario podía iniciar una llamada telefónica pulsando un botón desde una sesión Web. En estos servicios se considera que ambas partes involucradas en la comunicación están conectadas a una Red con Conmutación de Circuitos (Circuit Switched Network – CSN).

Sin embargo, es en el Conjunto de Capacidades 4 (CS-4) en donde la ITU-T describe detalladamente la interoperabilidad entre las redes IP y las Redes Inteligentes. Para el desarrollo de las recomendaciones del CS-4 la ITU-T incluyó en su análisis los resultados del Grupo de Estudio 11 (Study Group 11) de la ITU-T, el estudio desarrollado por los grupos de trabajo PINT y SPIRITS de la IETF y las recomendaciones de la serie H de la ITU-T, H.323 y H.248.

#### *B.3.3.1. Características de Servicio CS-4*

Como ya se explicó en el Modelo Conceptual del Servicio definido por CS-3 y CS-4 en el Capítulo 1, las características de servicio describen la capacidad desde el punto de vista del usuario, y son aplicables no sólo a los usuarios finales del servicio sino, también, a todos los usuarios de la red inteligente, entre los que se cuentan los operadores de red o los proveedores de servicios de red.

El Conjunto de Capacidades 4 define las características de servicio, que se mencionan a continuación (algunas de las cuales fueron definidas como servicios por PINT y SPIRITS) para la Interacción entre las Redes Inteligentes y las Redes IP. Nota: Se presenta la descripción textual incluida en el CS-4.

- *Personalización de los Datos del Servicio de un Usuario Final vía una Red IP ("End User Service Data Customization via an IP network" – EUSDC)*

  Un usuario final del servicio puede personalizar sus datos del servicio, a través de una red IP. Nota: Esta característica puede ser soportada en PINT sobre un Nivel de Socket Seguro.

- *Petición de Retorno de Llamada IP ("Request to Call Back IP" – RTCBI)*

  Un usuario puede iniciar una llamada telefónica pulsando un botón durante una sesión Web. La llamada puede ser establecida en la dirección del solicitador de la llamada, o primero ser establecida en la dirección de la parte con la que se quiere comunicar el solicitador.

Se supone direccionamiento E.164 para las partes A y B, y también que una o ambas partes tienen un servicio de Voz sobre IP. Un usuario de VoIP podría ser también un usuario Móvil. (El mismo servicio fue definido en el CS-3 con la diferencia que ambas partes debían estar conectadas a la red de conmutación de circuitos)

Un ejemplo de la aplicación de esta característica es la telecompra, en la que un usuario que hojea un catálogo en línea, pulsa un botón que lo invita a recibir la llamada de un representante de ventas. En la RI, el tratamiento de la petición depende de la disponibilidad de agente, la hora del día, etc.

- *Petición de Llamada IP ("Request to Call IP" – RQTCI)*

  Un usuario puede iniciar una llamada telefónica pulsando un botón durante una sesión Web. La llamada solicitada se establece entre dos partes que se identifican por direcciones E.164, donde una o ambas partes tienen un servicio de Voz sobre IP. Un usuario de VoIP podría ser también un Usuario Móvil. La persona solicitante puede participar o no en la llamada que se va a establecer.

  Los posibles motivos de fallo (igual que en el servicio anterior) son: parte A ocupada, parte A no contesta, parte B ocupada, parte B no contesta. Al solicitador no se le envían notificaciones detalladas.

- *Llamada en Espera via Internet ("Internet Call Waiting" – ICW)*

  Un usuario es notificado de llamadas entrantes durante una sesión Web y, pulsando un botón puede instruir a la red en como esta llamada debe ser procesada más adelante. Por ejemplo, la llamada puede ser rechazada, enviada a un sistema de correo de voz, aceptada con o sin interrupción de la sesión Web (en caso de aceptación sin interrupción de la sesión Web se asume que es una llamada de VoIP).

  Un subconjunto de esta característica sería mantener un registro de las veces que un usuario recibe llamadas durante una sesión Internet.

- *Servicio de Conferencia PSTN/IP controlado via Web ("Web Controlled PSTN/IP Conferencing Service" - WCPCS)*

  Se consideran temas como: iniciación de la conferencia telefónica, conferencia telefónica básica PSTN/IP controlada via web, adición de participantes, etc.

- *Selección de Gateway IP ("IP Gateway Selection" – IPGWS)*

  Se proporciona un servicio involucrando una conexión CSN (Red de Circuitos Conmutados) a un gateway en una red IP, haciendo uso de una configuración de red con varios gateways hacia el dominio IP. Un servicio de RI se usa para decidir cual gateway físico utilizar, basado entre otras cosas en la disponibilidad del gateway, o en su carga. Este escenario es aplicable para Servidores de Acceso Internet así como para gateways de Voz sobre IP.

### *B.3.3.2. Arquitectura Plano Funcional Distribuido (DFP) para CS-4*

El modelo funcional distribuido definido por el CS-4 es una extensión del modelo funcional definido por el CS-2 y está planeado para soportar:

- Servicios básicos CS-4
- Personalización de servicios basados en Internet
- Terminación de VoIP para alcanzar usuarios en el dominio de teléfonos así como capacidades de RI generales.

El Plano Funcional Distribuido (DFP) para el CS-4 incluye las Entidades Funcionales definidas en el CS-1 (CCF, SSF, SCF, SDF, SRF, SMF) y en el CS-2 (CCAF, SCUAF, CUSF) e incluye nuevas Entidades Funcionales (PINT Server, SA-GF, GF, SM).

La arquitectura de red mostrada en la Fig. B.8 representa la distribución de la inteligencia de red e identifica el modelo del Plano Funcional Distribuido (DFP), sin embargo solo presenta las Entidades Funcionales y las Interfaces Funcionales requeridas para el soporte RI de las Redes IP.

A continuación se presenta la descripción de las principales Entidades Funcionales representadas en el lado de la Red IP en la *Fig. B.4*.

- **Servidor PINT** (PINT Server)**:** Aunque no está estandarizado por el ITU-T, el Servidor PINT es considerado como una Entidad Funcional. El Servidor puede ser configurado como un Servidor Proxy o un Servidor de Redireccionamiento. (Estos términos se usan en el sentido SIP ya que PINT está basado en señalización SIP.)

  El servidor PINT transmite al SCP una petición de iniciar una llamada PSTN. Se espera que el servidor PINT también transfiera datos de usuario entre la red IP y la PSTN/RI, por ejemplo en servicios que implican transferencia de fax.

- **Función Gateway – Aplicación de Servicio (SA-GF)** (Service Application – Gateway Function): Esta función permite la interacción entre el nivel de control de servicio en la RI y las Aplicaciones de Lógica de Servicio Distribuida (funciones basadas en APIs), y entre la Función Administrador de Llamada (CM) y la Lógica de Servicio Distribuida.

  Para CS-4, en el nivel de aplicación, los tipos de funcionalidades basadas en APIs pueden incluir: plataformas CORBA, plataformas JAVA, plataformas JAIN y plataformas basadas en otros APIs. (Ver capítulo B.B.)

- **Función Administrador de Sesión (SM)** (Session Manager): La función de Administración de Sesión es responsable por la administración de los servicios de la Red IP. Se encarga adicionalmente de pasar la información relacionada con admisión y registro hacia y desde el SCF.

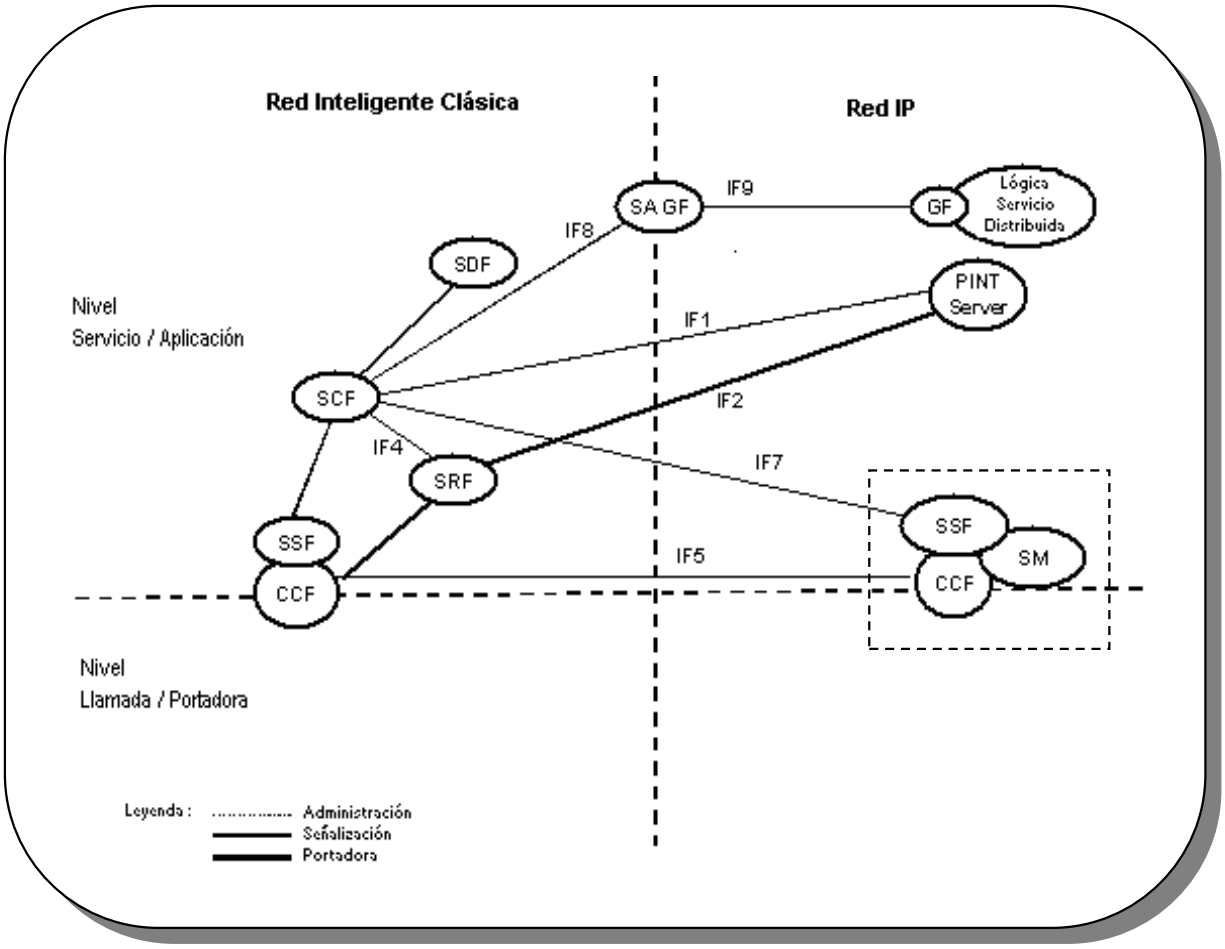



*Fig. B.4. Arquitectura Funcional Mejorada para Soporte RI de Redes IP (Q.1244).*

- **Función Control Llamada (CCF)** (Call Control Function): La CCF es una Entidad Funcional mejorada, responsable por el manejo de la señalización de la llamada tanto en la Red Inteligente, como en la Red IP.

  El CCF mejorado en el lado de la Red IP realiza las funciones de un Gatekeeper H.323, de un servidor SIP y las funciones de un Controlador de Gateway de Medio ("Media Gateway Controller" - MGC). Este último como su nombre lo indica es el encargado de controlar los Gateways de Medio ("Media Gateway" – MG) en una red IP.

  Esta entidad se encarga de pasar la información relacionada con el servicio hacia y desde el SCF.

  La Función de Control de Llamada podría ser vista como un Conmutador (switch) Lógico.

- **Función de Conmutación de Servicio (SSF)** (Service Switching Function): La SSF es una Entidad Funcional mejorada, encargada de interactuar con el SCF y con el CCF mejorado, trasladando el Protocolo de Control de Llamada en procedimientos y puntos impulsores (triggers) de eventos INAP, donde sea necesario.

  El SCF en combinación con el SSF mejorado y el CCF mejorado se encarga de controlar las llamadas de VoIP y de manipular la información de la llamada.

Adicionalmente a las Entidades Funcionales mencionadas, la recomendación Q.1244 explica ampliamente los siguientes temas, los cuales podrán ser estudiados detalladamente en un trabajo posterior a esta tesis:

- Interfaces Funcionales entre las diferentes entidades funcionales.
- Relaciones Funcionales y Clases de Control para CS-4 RI.
- Internetworking entre diferentes tipos de redes, tales como RI estructuradas y no estructuradas, redes públicas y privadas.
- Diferentes escenarios de implementación IN/IP (Soporte de sistemas SIP, sistemas H.323, servicios basados en PINT, servicios basados en SPIRITS, entre otros).
- Entidades Funcionales para soportar interacción CS-4 RI con características IMT-2000. (Ambiente Hogar Virtual – VHE “Virtual Home Environment”.)

## B.4 REDES CONVERGENTES (APIS ABIERTOS)

Hoy en día los servicios básicos de telecomunicaciones y las redes que los soportan (PSTN, celular, datos), comparten los mismos medios de transmisión en el nivel físico (p.e. Fibra Optica), pero en el nivel de red, cada una de ellas es totalmente diferente:

- La PSTN interconecta conmutadores de circuitos
- Las redes celulares interconectan centrales móviles
- Las redes de datos interconectan enrutadores y switches ATM.

Estas redes en el nivel de aplicación son administradas individualmente aún cuando pertenezcan al mismo proveedor de servicios. Cada tipo específico de red o transporte cuenta con servicios que frecuentemente tienen códigos de software diferentes, generando un incremento en los procesos requeridos para aprovisionamiento, facturación y administración de estos servicios.

Basados en el cambio hacia una arquitectura abierta, los desarrolladores de aplicaciones de telecomunicaciones están trabajando en la especificación de APIs (Application Programming Interfaces) abiertos que les permitan a los proveedores de servicios simplificar la creación, pruebas y soporte de servicios de valor agregado en las redes convergentes. Estos APIs permiten a la red ser aumentada o modificada rápidamente, para introducir nuevos servicios consistentes con el modelo de Internet.

Los APIs están diseñados para ocultar tanto como sea posible los detalles específicos de las infraestructuras, para ayudar a los desarrolladores de aplicaciones a concentrarse en la lógica del servicio y en los atributos de los servicios.

Los APIs de dominio público serán los habilitadores claves de la convergencia de redes, impulsando el desarrollo de servicios de valor agregado que se extienden sobre múltiples dominios (voz / datos, alámbrico / inalámbrico, público / privado).

Los APIs también proveerán una interfaz segura para los recursos de red, contribuyendo así a la apertura de las redes públicas.

En este campo, dos iniciativas de la industria que han ganado reconocimiento en el mercado y que son reconocidas en la evolución hacia las Redes de Próxima Generación, son: Parlay y JAIN.

### *B.4.1. PARLAY*

El grupo de trabajo de la Industria PARLAY fue formado en Abril de 1998 para especificar un API abierto para el control de los servicios de telecomunicaciones.

Los miembros originales fueron BT, Ulticom, Microsoft, Nortel Networks, y Siemens. En 1999 el grupo incluyó a AT&T, Cegetel, Cisco, Ericsson, IBM y Lucent. En el 2000 el grupo Parlay se incorporó a una organización sin ánimo de lucro y abrió sus actividades a membresías de compañías que desearan participar en la evolución del Parlay API.

Una excelente definición de este API es: "El API Parlay define un conjunto de interfaces independientes de la tecnología, que especifica métodos, eventos, parámetros y sus semánticas para permitir a creadores de aplicaciones externos (terceros) e internos (operadores de red tradicionales) el control sobre los recursos y capacidades del núcleo de la red". Dada por S. Beddus en "*Opening Up Networks with JAIN Parla*y. IEEE Communication Magazine, April 2000, pp. 136-143".

#### *B.4.1.1. Metas del Grupo Parlay*

El grupo Parlay trabaja en la especificación de un API de Control de Servicios Orientado a Objetos que sea independiente de las tecnologías de comunicaciones (PSTN, redes inalámbricas y redes IP), de la plataforma (independiente de lenguaje de programación, sistema operativo o hardware) y del vendedor.

El API está especificado en UML (*Universal Markup Language*) y está diseñado para soportar todas las principales tecnologías de middleware (DCOM, CORBA, Java Platform).

Las metas técnicas del grupo incluyen fomentar la Integración de la Telefonía y la Computación (CTI – *Computer-Telephony Integration*), permitiendo a los sistemas IT de

las empresas controlar, accesar y configurar servicios tradicionales de telefonía de RI, proporcionando una interfaz unificada de control de servicios para tipos de redes de heterogéneas (PSTN, Wireless y Voz sobre IP, VoIP) y la especificación de los servicios de marco de referencia de valor agregado tales como los mecanismos de facturación en línea.

Las metas de negocios incluyen la creación de un mercado para terceros proveedores de servicios, habilitando servicios que sean más personalizados para las necesidades individuales de las empresas, habilitando a pequeñas compañías de IT a desarrollar servicios de telecomunicaciones y permitiendo a los operadores de redes a vender acceso a sus infraestructuras de RI.

El API Parlay habilita a una nueva generación de servicios, controlados por terceros o por clientes, que están integrados en sistemas IT tales como e-mail, bases de datos de información de clientes, y muchos más, a utilizar directamente las capacidades de RI de los operadores de telecomunicaciones sin necesidad de desperdiciar el enrutamiento de la llamada a través de PBXs privados para luego ser redireccionados en la red del operador (*Fig.B.5*).

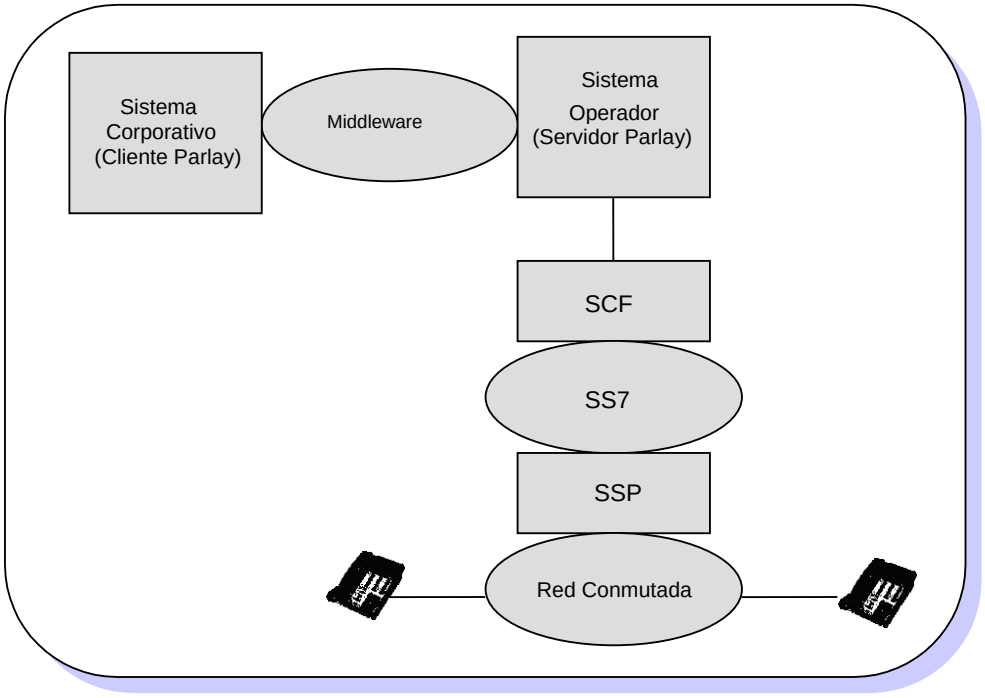



*Fig. B.5. La arquitectura Parlay.*

### *B.4.1.2. Elementos del API Parlay*

El API Parlay está dividido en dos porciones: Interfaces de Servicios e Interfaces de Framework. La porción de servicios provee un completo rango de capacidades de red. La porción de framework provee la infraestructura para soportar los servicios.

- *Interfaces de Servicios* – Ofrecen acceso a aplicaciones a un amplio rango de capacidades y de información de la red. Las Interfaces de Servicio son los bloques de construcción de tecnología vertical con los cuales se crean las aplicaciones y proveen acceso a los servicios de nivel de red necesarios para crear servicios superiores de nivel de usuario. Las funciones proporcionadas por las interfaces de servicio permiten acceso a capacidades de red tradicionales tales como:
  - Control de Llamada Genérico (Generic Call Control)
  - Control de Llamada INAP (INAP Call Control)
  - Administración de Llamada (Call Management)
  - Mensajería Genérica (Generic Messaging)
  - Interacción de Usuario (User Interaction)

- *Interfaces de Framework* – Las interfaces de framework son independientes de cualquier servicio, y proveen las capacidades de soporte necesarias para que las Interfaces de Servicio sean seguras, abiertas y administrables. Los servicios de framework son los medio a través de los cuales los proveedores de red pueden rastrear exactamente quien utiliza la red y cuanto utilizan la red. Las funciones proporcionadas a través de las interfaces de framework son:
  - Autenticación (Authentication)
  - Descubrimiento (Discovery)
  - Notificación de Eventos (Event Notification)
  - Administración de Integridad (Integrity management)
  - Operación, Administración y Mantenimiento (Operations, administration and maintenance – OA&M)

- *Interfaces de Recursos* – El grupo Parlay no especifica estas interfaces, pero son los medios a través de los cuales se interfasa un producto Parlay con los elementos de red. Estos adaptadores pueden ser proporcionados por el fabricante de equipos, construidos por terceros o incluidos con un producto Parlay. Sin embargo, pueden presentar problemas que afectarían la implementación del API Parlay, entre los que encontramos: disponibilidad, dificultad para su creación, demasiados costos.

#### *B.4.1.3. Participantes del API Parlay*

El API está compuesto por 4 actores principales, los dos primeros agrupados como clientes y los dos últimos agrupados como proveedores.

- Clientes: el operador corporativo (enterprise operator), la aplicación del cliente (client application). El operador corporativo tiene un dominio de red compuesto por sus aplicaciones de cliente.

- Proveedores: el proveedor de servicios (service provider) y el operador de framework (framework operator). El proveedor de servicios tiene un dominio de red compuesto por sus aplicaciones de servicios.

Existe una fuerte relación con los participantes de RI (*Tabla B.1.*):

| Participantes Parlay | Participantes RI |
|---|---|
| Operador Corporativo | Suscriptor del Servicio |
| Aplicación Cliente | Usuario del Servicio |
| Proveedor del Servicio | Proveedor del Servicio |
| Operador de framework | Operador de Red |

*Tabla B.1. Participantes Parlay - RI.*

#### *B.4.1.4. Arquitectura Parlay*

El Framework Parlay describe el flujo de información entre el proveedor del servicio (un servicio particular) y el dominio del operador corporativo (aplicación de un cliente particular).

Ya que Parlay es una especificación de un API, no está asociada con ninguna arquitectura física particular. Las aplicaciones pueden o no residir en el mismo elemento computacional donde reside el código Parlay. En una arquitectura lógica los diferentes componentes de un producto Parlay pueden estar separados, sin importar donde existirán en el momento de su operación.

Las aplicaciones existen fuera del dominio de la red e interactúan con la red a través del API Parlay. El API Parlay no especifica como se realiza la comunicación entre las aplicaciones y el API. Middlewares, tal como CORBA, pueden servir como el puente de comunicación entre el API y las interfaces de recursos.

El API Parlay correrá sobre una máquina llamada Gateway Parlay. Este gateway será conectado a aplicaciones a través de una red IP. Los adaptadores de recursos serán también probablemente conectados a través de una red IP. En algunos casos los equipos serán controlados indirectamente, posiblemente a través de un protocolo SS7.

Las aplicaciones se comunicarán con la red haciendo llamadas API a los gateways Parlay. Estas llamadas algunas veces resultarán en interacciones entre el gateway y un adaptador. Si el adaptador está relacionado al protocolo, puede introducir paquetes en la red SS7.

Como conclusión se puede decir que el API Parlay es una arquitectura que puede proveer independencia de red y portabilidad de aplicaciones. Esta iniciativa constituye un mejoramiento comparado con las RI actuales. Analizando los servicios de RI, estos son desarrollados de una manera céntrica en la red. Con una propuesta basada en API, las

capacidades de la red que son utilizadas para las aplicaciones son encapsuladas y se hacen visibles a estas aplicaciones. Esto mejora la integridad, rendimiento y seguridad de la red.

Sin embargo, esta iniciativa sigue siendo teórica. Es poco probable que haya una única tecnología de middleware dominante, por lo que Parlay puede ser implementado con cualquier tecnología. Sin embargo tendrá problemas de interoperabilidad si múltiples vendedores que reclamen conformidad con Parlay solo soportan uno (un subset) de los posibles mecanismos de implementación de middleware.

A pesar de que es muy prematuro garantizar su éxito, es seguro que ofrecerá a los proveedores de red y a terceros desarrolladores de aplicaciones, la propuesta de más alto nivel para la creación de servicios de valor agregado en redes convergentes.

### *B.4.2. JAIN – REDES INTEGRADAS*

Las Redes Integradas para APIs Java (Java APIs for Integrated Networks) nacieron en Junio de 1998, cuando Sun Microsystems y otras compañías en alianza con Sun, anunciaron "la primera solución de la industria basada en tecnología Java, para la construcción y desarrollo de los servicios de telecomunicaciones mediante la integración de las Redes Inteligentes y las tecnologías de Internet". Esta integración se conoce como REDES INTEGRADAS.

En la *Fig. B.6*. se puede observar la Iniciativa JAIN, la cual integra redes basadas en paquetes, redes inalámbricas y redes alámbricas (cableadas). La Iniciativa JAIN propone la estandarización en dos niveles diferentes. El nivel de red implica la convergencia de red, mientras el nivel de aplicación implica la portabilidad del servicio.

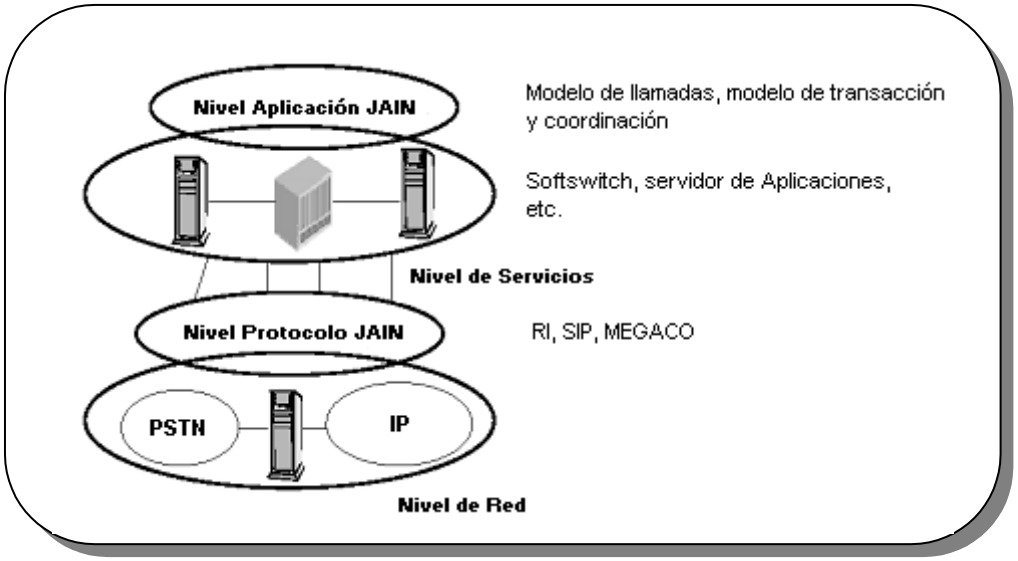



*Fig. B.6. Iniciativa JAIN.*

JAIN está compuesta por dos áreas de desarrollo. La primera, *Especificaciones API de Protocolo (Protocol API Specifications),* especifica la adaptación de protocolos especificos de red al modelo JAIN. La otra, *Especificaciones API de Aplicaciones (Application API Specifications)*, especifica los APIs requeridos para la creación de servicios dentro de una framework Java extendiéndose a través de todos los protocolos cubiertos por la Especificación de Protocolo API.

### *B.4.2.1. Especificaciones API del Nivel de Protocolo JAIN*

Esta área es manejada por el Grupo de Expertos en Protocolos (PEG – Protocol Expert Group). Este grupo estandariza las interfaces para redes IP y redes SS7. Su trabajo consiste en APIs para varios protocolos comunes, por ejemplo:

- TCAP, INAP, ISUP para el lado SS7
- SIP, H.248 (MEGACO) y H.323 para el lado IP

El API SS7 de JAIN permite que cualquier entidad JAIN acceda y se comunique con una entidad RI.

El API IP de JAIN permite el proveer servicios sobre una red IP equivalentemente a aquellos de una red de telefonía tradicional.

La evolución hacia redes NGN puede ser progresiva ya que las entidades de red preservan su software de protocolo nativo existente, mientras simultáneamente habilitan aplicaciones JAVA para proveer nuevos servicios. Así, las entidades que cumplan con JAIN podrán soportar y participar en el desarrollo de las redes NGN.

### *B.4.2.2. Especificaciones API del Nivel de Aplicaciones JAIN*

Esta área es manejada por el Grupo de Expertos de Aplicaciones (AEG – Application Expert Group). Este grupo define APIs de mayor nivel que los APIs de Protocolo:

- *API de Control de Llamada JAIN (JCC – Java Call Control)* y
- *API de Transacción y Coordinación JAIN (JCAT – Java Coordination and Transaction):* Estos dos APIs presentan un conjunto de rutinas de alto nivel para manipulación de las llamadas, independientemente de la tecnología y de la red.
- *API de Ejecución de la Lógica de Servicio JAIN (JSLEE - Java Service Logic Excecution Environment):* Define los servicios que se garantizan están disponibles en el SLEE (un SCP más general). Se encargará de administrar los servicios, los recursos que necesita y su interacción con la red. Es algo análogo a un Gateway Parlay.
- *API de Creación de Servicios JAIN (Service Creation):* Define los servicios que se garantizan están disponibles en el SCE. El SCE es un contenedor de componentes de software (beans) de Java, que permite a los creadores de servicios construir servicios utilizando un GUI para unir dinámicamente componentes de software.

- *Administración de conectividad JAIN:* Un API para manejar políticas y conexiones de red.
- *API de Acceso de Red Asegurado JAIN (Secure Network Access), también se conoce como API de Acceso de Proveedor de Servicios (SPA – Service Provider Access):* JAIN adoptará la especificación Parlay para proveer un medio seguro de accesar las capacidades de red.

La primera meta de este grupo es proporcionar un modelo sencillo de llamada a través de todos los protocolos soportados en el nivel de Protocolo, mencionados anteriormente.

### *B.4.2.3. El modelo de componentes JAIN*

La tecnología JAIN está basada en JavaBeans (pequeñas entidades de software Java). Estos componentes pueden ser adicionados, mejorados, ensamblados, compartidos, o redistribuidos en un sistema corriendo dinámicamente. Esto permite que los servicios y las características sean adicionadas, actualizadas y borradas en un ambiente real.

El modelo de componentes JAIN ha tomado como base al ambiente de Red Inteligente, con la ventaja de que las propiedades y características de JavaBeans en el sistema JAIN son mucho mejores que los SIBs estáticos utilizados para crear servicios en la RI tradicional. Por lo tanto, el sistema JAIN es una arquitectura completa y abierta que podría soportar reutilización de componentes.

## *B.4.3. ALIANZA PARLAY – JAIN*

JAIN y Parlay son soluciones complementarias en muchos aspectos, por lo que en Marzo 2000 unieron esfuerzos, obteniéndose las siguientes ventajas:

- La utilización de Java y JAIN para construir servicios y gateways Parlay.
- La adición de una jerarquía API compatible con Parlay en la especificación de JAIN. En algunas categorías, tales como seguridad, el API Parlay puede servir para proveer todas las funcionalidades JAIN, este es el caso de la adopción de Parlay en el API de Acceso de Red Asegurado JAIN o API de Acceso de Proveedor de Servicio (SPA) JAIN.

El API Parlay puede manejar los temas de seguridad para terceros proveedores de servicios. También se resalta que los servicios JAIN tienen un amplio rango de protocolos de comunicaciones disponibles para ellos. Sin embargo, la alianza no fue directa, debido a que las dos iniciativas utilizan mecanismos que la otra iniciativa no soporta, y no satisfacen los requerimientos de los mecanismos por obtener mayor rendimiento y soporte.

## B.5. REDES INTELIGENTES DISTRIBUIDAS

Como ya mencionamos anteriormente, a pesar de las grandes ventajas de las Redes Inteligentes, también cuentan con algunas limitaciones que hacen que sus implementaciones sean poco flexibles, centralizadas y con reducida escalabilidad y rendimiento.

- La naturaleza estática del stack del protocolo SS7 ha significado que la topología de la red, en términos de su flujo de RI, sea fija. La SS7 no ofrece las propiedades de un ambiente de procesamiento distribuido, por lo que las asociaciones entre entidades funcionales son configuradas estáticamente.
- Las arquitecturas de RI tradicionales son propensas a cuellos de botella en la red de señalización, debido a su arquitectura centralizada,

Nuevas tecnologías como CORBA (Common Object Request Broker) y MAT (Mobile Agent Technology) han creado un nuevo potencial para implementaciones de RI y han dado surgimiento al concepto de RI distribuidas.

Estas Redes Distribuidas, representan un paso en la evolución de las RI, introduciendo un alto nivel de programabilidad y flexibilidad en la ubicación del control del servicio, y en la administración y aprovisionamiento del servicio.

### *B.5.1. CORBA*

CORBA es una arquitectura de software, definida por el OMG (Object Management Group), que permite a los objetos de software interactuar recíprocamente con otros, en un ambiente de computación distribuido y abierto

Permite a los programadores enfocarse en la implementación de diferentes soluciones, (p.e. la implementación de un servicio sobre un servidor o de un cliente para el servicio), sin preocuparse por los problemas de comunicación e integración, los cuales son asumidos por el ORB (Object Request Broker) conocido comúnmente como Bus de Objetos, que es el corazón de la Arquitectura de Administración de Objetos (OMA – Object Management Architecture) del OMG.

Entre las principales ventajas de la adopción de CORBA para el desarrollo de aplicaciones a gran escala se encuentran:

- Orientación a objetos
- Independencia del lenguaje de programación de los objetos
- Independencia de la plataforma de implementación de los objetos
- Independencia de la ubicación de los objetos

- Reutilización de software
- Escalabilidad mejorada del sistema
- Ambiente distribuido, pero creando la ilusión de un espacio unificado

### *B.5.1.1. Modelo de Objetos OMG*

El modelo de objetos OMG estándar, está fundamentado en los principios orientados a objetos, y sigue el paradigma cliente/servidor. A continuación se describen algunos conceptos importantes para entender el modelo de objetos OMG y la arquitectura CORBA.

*Objetos CORBA* – Corresponden a todos los programas (software común) que son implementados en cualquier lenguaje de programación Orientado a Objetos soportado por CORBA, tales como Java, C++ y Smalltalk.

Un *Objeto Servidor* es una entidad encapsulada, identificable, que provee uno o más servicios que pueden ser solicitados por un *Objeto Cliente.*

*Referencia Objeto* – Cada objeto posee una única e invariable referencia objeto, la cual es asignada en el momento de su creación, permanece con él durante todo su ciclo de vida y sólo es desasignada en el momento de su eliminación. A través de estas referencias los clientes pueden hacer invocaciones.

*Interfaz* – Es una descripción de un conjunto de operaciones posibles que un Objeto Cliente puede requerir de un Objeto Servidor, y de otros aspectos del comportamiento del Objeto Servidor. Lo único que un objeto conocerá de otro objeto es su interfaz. Las Interfaces son especificadas en IDL.

*Operación* – Es una entidad identificable que denota un servicio que puede ser requerido. El OMG utiliza el nombre *Invocación de Método*, para describir la acción del ORB cuando hace una llamada de invocación al método que implementa (en la Implementación Objeto) una operación específica. Cada Operación tiene su propia Firma (Signature)

*IDL (Interface Definition Language)* – Lenguaje de Definición de Interfaces estandarizado por OMG, con el cual se definen las interfaces de todos los objetos existentes para que puedan interactuar con otros objetos. Esto significa que cada Objeto debe contar con una interfaz especificada en IDL. El lenguaje IDL ocultará detrás de la interfaz de un Objeto, los detalles de su implementación, tales como lenguaje y plataforma. Así por ejemplo, el Objeto Cliente invocará una operación remota en su propio lenguaje y el Objeto Servidor desarrollará el servicio en su propio lenguaje, y ninguno de ellos tiene que conocer el lenguaje de implementación del otro.

### *B.5.1.2. Arquitectura CORBA*

CORBA es una arquitectura basada en objetos, que permite la comunicación entre un Objeto Cliente y un Objeto Servidor (también llamado Objeto Implementación).
(Ver *Fig. B.7.*)

*ORB (Object Request Broker* – Agente de Petición de Objetos) – Es un bus de objetos, que se encarga de soportar todas las comunicaciones que se presentan entre los objetos en él implementados. Utilizando el ORB un Objeto Cliente puede invocar transparente una operación sobre un Objeto Servidor que puede estar en la misma máquina o a través de la red.

El ORB intercepta la petición y es responsable por encontrar un objeto que pueda implementar dicho requerimiento, entregándole los parámetros, invocando su operación y retornando los resultados. El cliente no tiene que preocuparse de donde se encuentra ubicado el objeto, su lenguaje de programación, su sistema operativo, si se encuentra activo o inactivo, o cualquier otro aspecto del sistema que no hace parte de una interfaz de objeto.

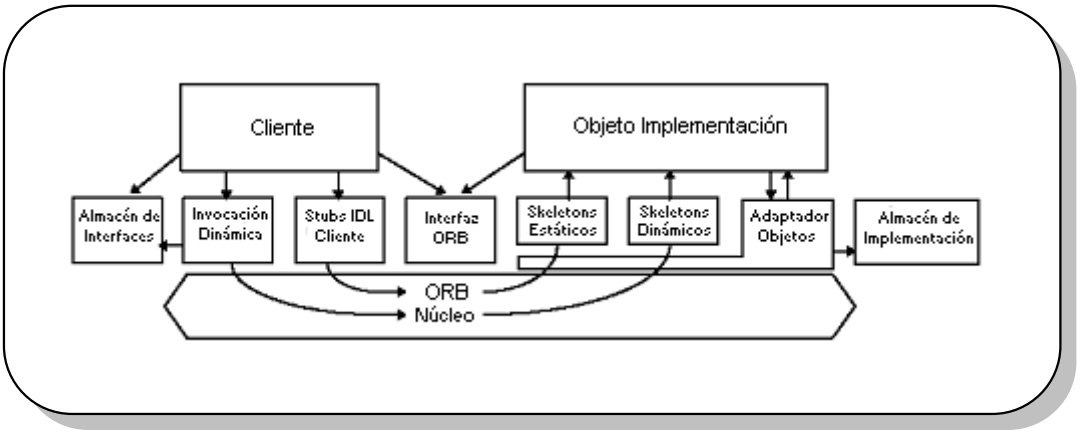



*Fig. B.7. Elementos de la Arquitectura CORBA.*

*Peticiones de un Objeto* – Un cliente puede hacer peticiones sobre un Objeto Servidor de dos diferentes maneras: Invocación Estática de una Interfaz (Stubs Cliente) e Invocación Dinámica (DII). La manera utilizada es transparente para los Objetos Servidores.

Todos los objetos cuentan con interfaces que han sido definidas usando el IDL de CORBA. Después de ser definidas, las interfaces se compilan utilizando un compilador IDL, el cual genera un código en el lenguaje de programación específico (por ejemplo Java). Este código incluye un Stub del Cliente (permite desarrollar programas cliente) y un código Skeleton para el Servidor (permite implementar objetos CORBA).

*Stubs Cliente* – Este método es utilizado cuando el cliente conoce de alguna manera la información que describe la operación que desea invocar en el Objeto Servidor. Se conoce como Invocación Estática. Desde el punto de vista del cliente, el Stub es un Proxy para el Objeto Servidor remoto. Es decir, el stub hace las funciones de servidor en el lado del cliente, siendo a este a quien el cliente en realidad realiza sus invocaciones (locales)

en su propio lenguaje de alto nivel (p.e. Java, C++) sin preocuparse por los detalles de la comunicación, protocolos, marshal, etc.

El stub contiene la representación de la interfaz IDL del objeto, necesaria para la comunicación con el ORB. El stub se encarga del proceso de marshal, por medio del cual divide las invocaciones en pequeños mensajes que puedan ser transportados por el ORB para hacerlas llegar al objeto adecuado.
De la misma manera, las respuestas a las invocaciones deben pasar primero por el stub para que puedan ser entendidas en el lenguaje específico en que está implementado el cliente.

*Interfaces de Invocación Dinámicas (DII - Dynamic Invocation Interfaces)* – Este método es utilizado cuando el cliente no conoce la definición de la interfaz del Objeto Servidor que quiere invocar. Se conoce como Invocación Dinámica.
En este caso el cliente utiliza interfaces estándar específicas ofrecidas por el ORB, llamadas Interfaces de Invocación Dinámicas, para descubrir el comportamiento del Objeto Servidor, buscando en el *Almacén de Interfaces*. Tan pronto el cliente encuentra que tipo de servicios puede ofrecer un objeto Servidor, invoca la operación deseada.

*Almacén de Interfaces* – Es un depósito del ORB, donde se guardan las definiciones de las interfaces de los objetos que están actuando sobre el ORB. Por medio del acceso a este almacén se pueden recuperar estas definiciones.

*Implementación de un Objeto* – Un Objeto Servidor puede alcanzar una implementación de dos diferentes maneras: Skeleton Estático y Skeleton Dinámica (DSI). La manera utilizada es transparente para los Objetos Clientes.

*Skeleton Estático* - Este método es utilizado cuando el Objeto Servidor conoce los tipos de los objetos que está implementando. Tiene la responsabilidad de revertir el proceso de marshal de los parámetros realizado en el cliente (agrupa las invocaciones enviadas por el ORB para entregarlas al objeto adecuado) y hacer una llamada al objeto Servidor específico.

El Skeleton espera por la ejecución de la operación en el Objeto Servidor y después envía los resultados de regreso al cliente. El Skeleton se encarga de representar al cliente en el lado del servidor, por lo que al servidor no le interesa ni la ubicación del cliente ni el lenguaje en el que está implementado, ya que toda su comunicación se realiza con el skeleton ubicado en el mismo espacio de memoria.

*Interfaces Skeleton Dinámicas (DSI – Dynamic Skeleton Interfaces)* – Este método es utilizado cuando el servidor no tiene conocimiento en el tiempo de compilación, de los tipos de objetos que está implementando. Se encarga de desarrollar los requerimientos desde el ORB hasta el Objeto Servidor.

*Almacén de Implementaciones* – Es el segundo depósito del ORB y contiene la ubicación de las implementaciones de los servidores, la relación con las interfaces que posee cada servidor, otras características de seguridad y datos de tipo administrativo. A través de este almacén se puede ubicar un servidor, y las implementaciones realizadas en el mismo.

*Adaptador de Objetos* **–** Interfaz que provee un entorno en tiempo de ejecución que permite al ORB interactuar con los servidores. Define operaciones adicionales requeridas por los Objetos Servidores que no son específicamente requeridos por los clientes. Entre sus servicios están:

- Registro de los objetos hechos en lenguajes específicos como Objetos CORBA, en el Almacén de Implementaciones.
- Asignación de referencias a los nuevos objetos creados
- Activación de los objetos implementación.
- Activación de los servidores que contienen objetos implementación, si al haber una petición estos no se encuentran activos.

### *B.5.1.3. Protocolo de Interoperabilidad entre ORBs*

La interoperabilidad entre ORBs está garantizada en CORBA 2.0, gracias al Protocolo General de Interoperabilidad entre ORBs (GIOP - General Inter-ORB Protocol), cuya implementación sobre TCP/IP se llama IIOP (Internet Inter-ORB Protocol).

Adicionales a estos protocolos CORBA soporta Protocolos de Ambiente Específico de Interoperabilidad entre ORBs (ESIOPs – Environment-Specific Inter-ORB Protocols), para plataformas heredadas, pero deben proveer un puente hacia el protocolo IIOP, ya que este último es considerado como normativo.

### *B.5.2. IN / CORBA INTERWORKING*

La Integración RI-CORBA se presenta como la alternativa más viable para la evolución de la Red Inteligente, ya que está basada en tecnologías existentes que tienen cierto grado de madurez lo que la hace técnicamente viable.

La introducción de una capa intermedia de software, permitirá realizar las funciones de Red Inteligente de forma distribuida. Los servidores de aplicación y de datos (SCF, SDF, SMF) contendrán objetos CORBA actuando como componentes de servicios reutilizables. Del mismo modo, aplicaciones de interacción con el usuario contenidas en los módulos de recursos especializados se construirán a partir de componentes CORBA.

Los objetos CORBA distribuidos en los diferentes módulos físicos interactúan a través del ORB, que recogerá el mensaje o la información de un Objeto Cliente y la enviará a un Objeto Servidor, a través de un protocolo de interoperabilidad genérico (GIOP) o específico (ESIOP). El protocolo IOP podría ser soportado por el SS7.

La interoperabilidad entre la nueva plataforma y los elementos y servicios de las Redes Inteligentes heredadas será ajustada por una compuerta CORBA/SS7 que se encargará de traducir mensajes CORBA a mensajes INAP.

En Septiembre de 1998 la “Fuerza de Trabajo del Dominio de Telecomunicaciones (Telecoms Domain Task Force) de la OMG produjo una especificación [OMG, “IN/CORBA interworking” OMG doc./dtc/99-12-02, Dec.1999] que se centraba en la interrelación de los sistemas basados en CORBA con los sistemas de señalización de telecomunicaciones, tales como RI y sistemas móviles (Ver *Fig. B.8*).

Este estándar resultó del trabajo conjunto de AT&T, GMD FOKUS, Nortel, IONA Technologies, y Teltec Ireland, en colaboración con Alcatel, Deutsche Telekom, Ericsson Telecommunications, Humboldt University, Object Oriented Conceptes Inc., y Telenor, y está actualmente en su etapa de implementación y revisión.

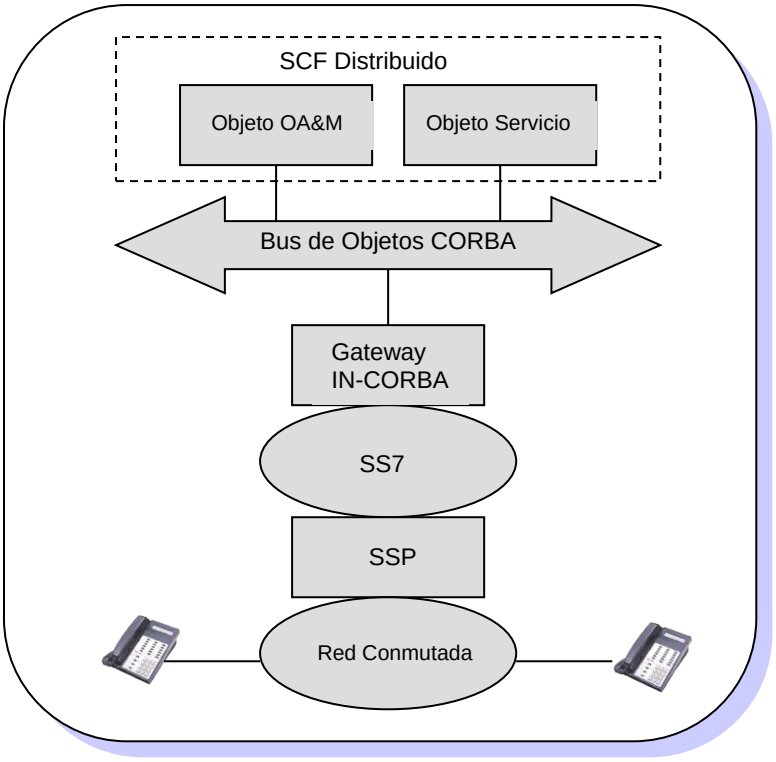



*Fig. B.8. IN / CORBA Interworking.*

La especificación cubre dos soluciones principales para la interoperabilidad de los sistemas tradicionales con los sistemas de RI:

- Interoperabilidad entre CORBA y SS7 - La motivación técnica primaria para la especificación IN/CORBA Interworking es proporcionar los mecanismos para la interrelación de las infraestructuras de servicios existentes, las cuales utilizan Capacidades de Transacción (TCs – Transaction Capabilities) para la comunicación, con objetos de servicio basados en CORBA, que utilizan un Protocolo de Intercambio de Requerimientos Entre Objetos (Inter-Object Request Broker Protocol – IOP) para la comunicación.

La especificación define un marco de referencia para el diseño de aplicaciones de usuario TC basadas en CORBA, tales como INAP, que pueden comunicarse a través de un gateway con usuarios TC heredados, tales como Puntos de Conmutación de Servicio (SSPs).

- Uso de SS7 como red de transporte para las aplicaciones CORBA - Una parte adicional de la especificación permite la interrelación entre islas de sistemas basados en CORBA utilizando la infraestructura existente de Señalización No. 7 (SS7) como una red de transporte para mensajes CORBA entre, por ejemplo, switches que exponen interfaces CORBA y objetos CORBA proporcionando lógica de servicio.

Las tecnologías middleware como CORBA se consideran cada vez más como la infraestructura apropiada para las redes de servicios futuras debido a las ventajas tecnológicas inherentes aplicadas por los ambientes distribuidos de procesamiento orientado a objetos.

En la misma presunción, las interfaces CORBA proporcionadas por la especificación IN/CORBA proporcionan las interfaces estandarizadas que permiten implementaciones más abiertas y distribuidas de servicios de RI. También el acercamiento común de CORBA para el aprovisionamiento de servicios y de la administración produce una red más integrada y una administración de servicios menos molesta.

IN/CORBA también facilita las facilidades crecientes de interconexión con recursos externos tales como Internet y las bases de datos privadas.

IN/CORBA ofrece la ventaja adicional de proporcionar una interfaz homogénea para cualquier implementación del stack del protocolo SS7. Esta independencia reduce los bloqueos de tecnología, permitiendo la creación del servicio independiente de las implementaciones propietarias del stack del protocolo SS7.

Ya que la especificación permite la implementación de tanto las RI basadas en CORBA como de los sistemas MAP, también puede proporcionar una base común para la convergencia de los sistemas fijos-móviles.

Aunque la especificación IN/CORBA muestra muchas posibilidades para el futuro de las RI, también cuenta con algunas desventajas asociadas. Para mantener la generalidad, la solución es totalmente de bajo nivel y no provee soporte específicamente para el desarrollo de los servicios de RI. CORBA aún tiene deficiencias cuando se espera que opere en un ambiente altamente tolerante a fallas y en tiempo real, lo cual se espera en los sistemas de telecomunicaciones.

De hecho, estos puntos no son tratados directamente por la especificación IN/CORBA Interworking.

### *B.5.3. TECNOLOGÍA DE AGENTES MOVILES*

La Tecnología de Agentes Móviles es una nueva tecnología que, retoma la vieja teoría de despachar una pieza de código para ser ejecutada remotamente. Sin embargo, la teoría ha sido mejorada, ya que los agentes móviles son capaces de reaccionar a estímulos externos y pueden exhibir comportamientos dinámicos, porque pueden por si mismos controlar su migración y la ejecución de los procesos.

En resumen, los agentes móviles son objetos de software que son capaces, mientras se están ejecutando en un nodo del computador, de detener su ejecución, transferirse ellos mismos a un computador remoto y reiniciar la ejecución en el nuevo sitio.

Los agentes móviles pueden ser asignados para desarrollar tareas en una manera completamente autónomos, lo que ha hecho énfasis en sus características de "inteligencia artificial".

Las plataformas de agentes móviles son los componentes necesarios en tiempo de ejecución para permitir a los agentes migrar, ejecutarse, encontrar a los otros y comunicarse.

Los agentes móviles están siendo estudiados junto con CORBA para la definición de un ambiente distribuido que pueda ser ofrecido a las más avanzadas plataformas de telecomunicaciones.

## B.6. REDES DE PROXIMA GENERACIÓN (NGN)

Las Redes de Próxima Generación (NGN – Next Generation Networks) son definidas como redes de telecomunicaciones abiertas, basadas en paquetes que emplean nuevas técnicas de señalización, administración, control y procesamiento distribuido para proveer todos los tipos de servicios, desde servicios básicos de telefonía de voz hasta avanzados servicios multimedia de banda ancha.

### *B.6.1. EVOLUCION DESDE LA PSTN HASTA LAS REDES NGN*

Cuando analizamos la evolución hacia las Redes de Próxima Generación, debemos partir de la existencia de dos redes de telecomunicaciones totalmente independientes.

La primera, corresponde a las Redes de Telefonía por Conmutación de Circuitos tradicionales, las cuales evolucionaron hacia las Redes Inteligentes obteniendo control e inteligencia sobre la red. A través de estas redes diseñadas y optimizadas para voz se realizaban inicialmente las transmisiones de datos (p.e. acceso Internet via módem y líneas dedicadas a 64Kbps), ya que la tecnología de conmutación de paquetes era aún inmadura y demasiado costosa.

La segunda red, más reciente, está conformada por las Redes de Datos por Conmutación de Paquetes, (paralelas e independientes a las Redes de Telefonía) diseñadas para la trasmisión de tráfico de datos de alta capacidad y que están basadas en tecnologías como ATM e IP.

Estas redes han tenido un rápido crecimiento, impulsado principalmente por el uso de Internet, por los nuevos desarrollos en conmutación de paquetes y por la disminución del costo del ancho de banda.

En la *Fig. B.9* se observa como en muy poco tiempo el tráfico de datos sobrepasará al tráfico de voz en las redes públicas en todo el mundo - lo cual ocurrió ya hace más de un año en Estados Unidos - y donde se espera que en el futuro el tráfico de voz represente solamente una pequeña fracción del tráfico de red total.

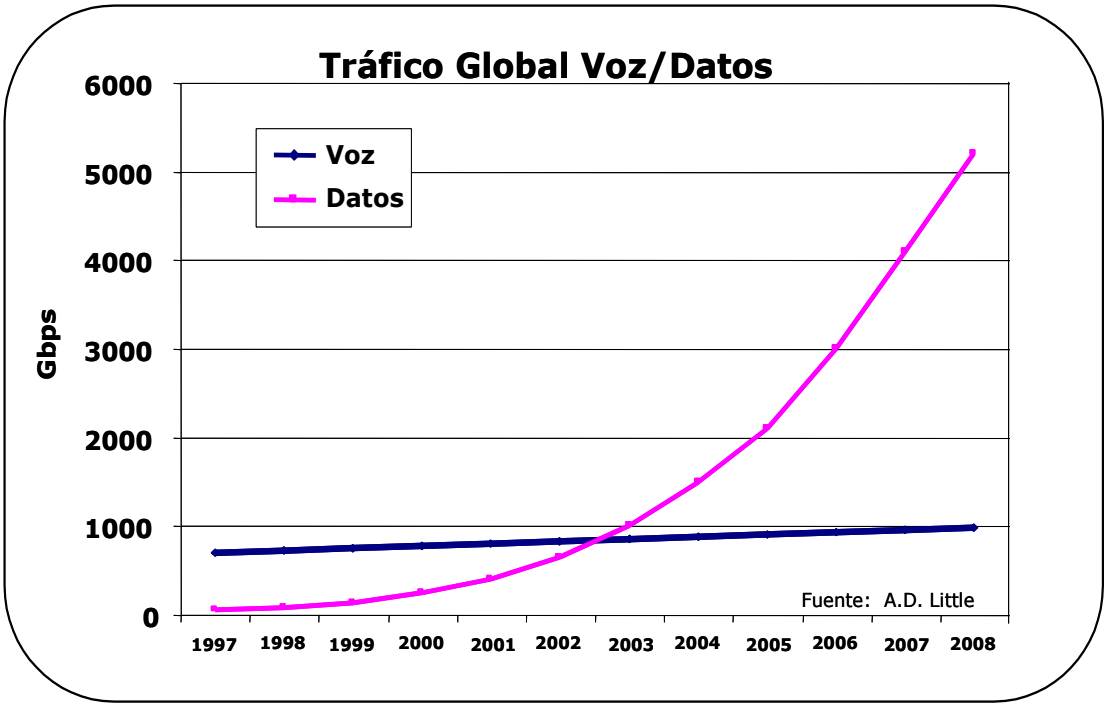



*Fig. B.9. Tráfico Global Voz y Datos.*

Todos los factores anteriormente mencionados, convierten a la infraestructura de redes de datos en un medio más propicio para la transmisión de voz, tanto técnica como comercialmente. Este hecho hizo que se cuestionara el papel de las Redes Inteligentes en la evolución de las redes.

Aunque en algún momento se cuestionó el papel de las RI en la evolución de las redes, en los últimos años ha habido un nuevo consenso entre los campos IP y de telecomunicaciones, de que las Redes Inteligentes aún tienen un importante papel para jugar, principalmente ofreciendo valor a los proveedores a través del desarrollo de un

rango más amplio de servicios para los usuarios, y en la mediación de la evolución de estos servicios entre los dos mundos.

El camino de migración hacia las Redes de Próxima Generación, no es tan simple como se muestra en teoría, por lo que los operadores pueden seguir diferentes caminos que de una u otra manera utilizan las Redes Inteligentes.

Como se puede ver en la *Fig. B.10.*, el primer paso hacia la convergencia de redes la dieron los proveedores de servicios de telecomunicaciones al transmitir comunicaciones de voz sobre redes dedicadas de datos (voz corporativa) y posteriormente TELEFONIA SOBRE INTERNET (tarjetas prepago), pero sin garantizar una buena calidad en la comunicación.

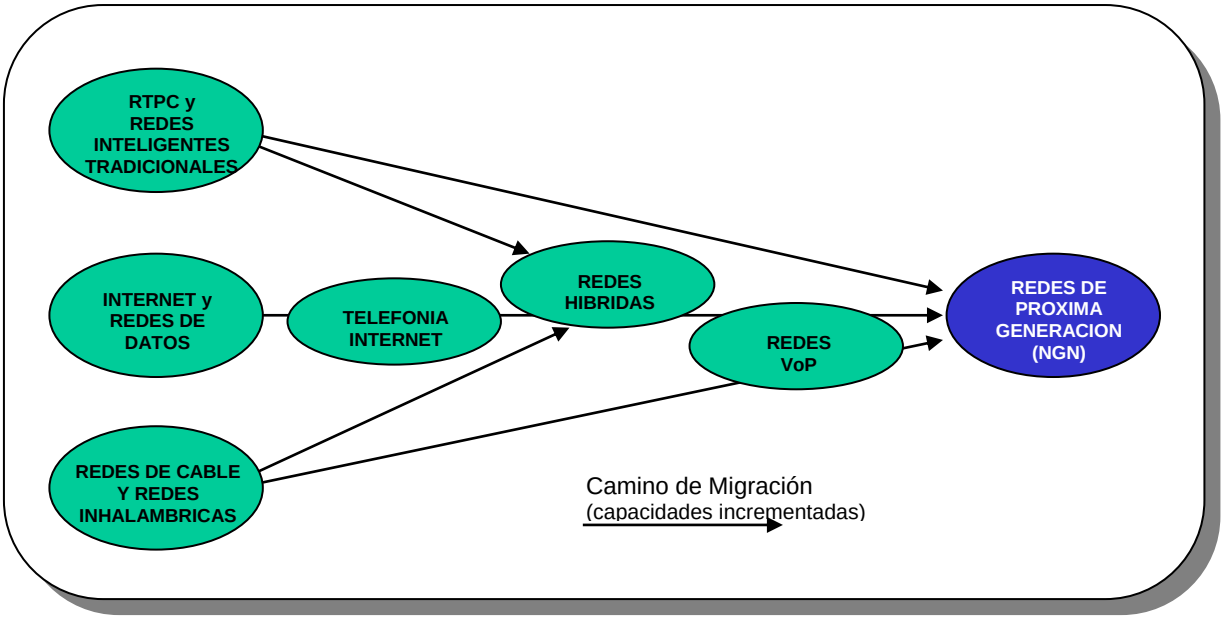



*Fig. B.10. Camino de migración hacia las redes NGN.*

El siguiente paso en el camino evolutivo hacia las Redes de Próxima Generación fue la creación de REDES HIBRIDAS, mediante el trabajo conjunto de Internet con las redes PSTN/RI, las cuales fueron explicadas en el numeral B.4 del presente capítulo. Los proveedores de servicios pueden ofrecer nuevos servicios híbridos que combinan la funcionalidad disponible en la PSTN, con Internet y con otras redes de paquetes.

La entrada al mercado de nuevos carriers que desean ofrecer servicios de telefonía y que inician sus operaciones desde cero (es decir, que no cuentan con una base instalada), ha llevado al surgimiento de las REDES DE VOZ SOBRE PAQUETES y ha obligado a los proveedores tradicionales (cuentan con una estructura de RTPC utilizando RI, tal como se puede observar en la *Fig. B.11.*) a incorporar estas nuevas tecnologías en sus redes para poder ser competitivos.

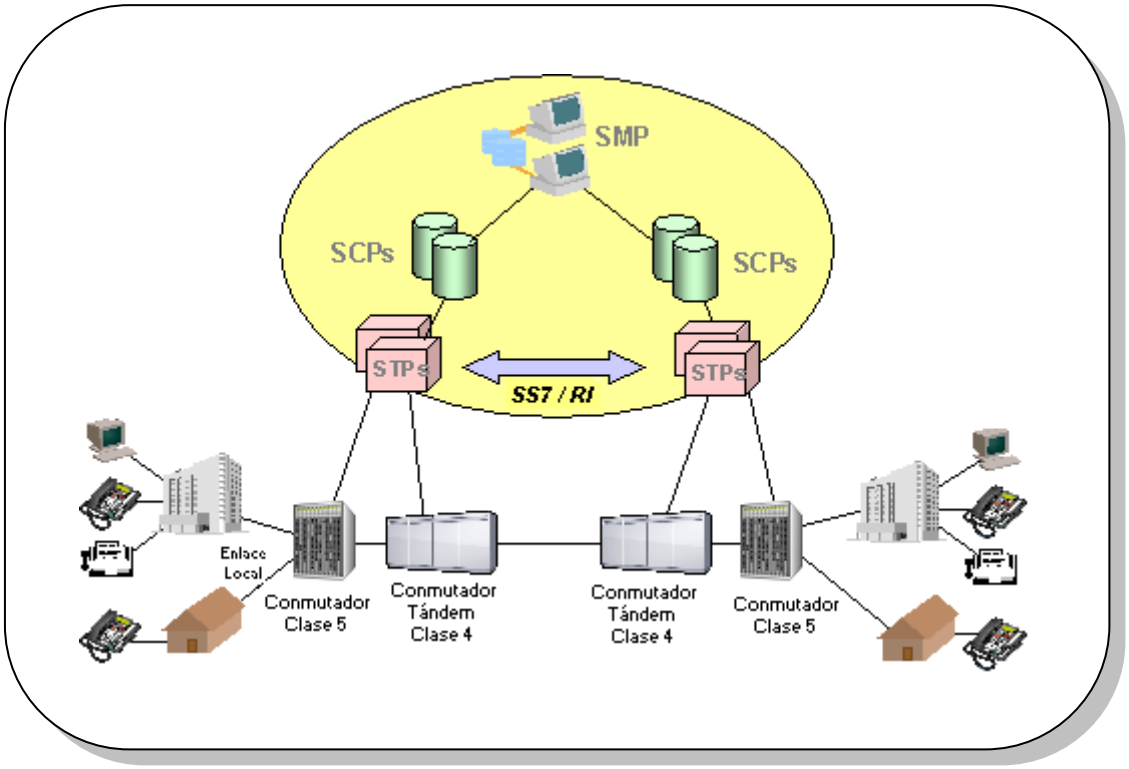



*Fig. B.11. Estructura de una Red PSTN / IN.*

Los elementos de la RI son el SMP, los SCPs, y los STPs (red de señalización SS7). Los SSPs (Puntos de Conmutación de Servicio) están representados por dos centrales de conmutación, una local (Clase 5) y una de tránsito (Clase 4). La conexión de los usuarios finales se realiza a través de líneas de cobre conectadas a la Central Telefónica.

La migración desde las redes PSTN/RI existentes hacia las Redes de Voz sobre Paquetes, se puede realizar en dos fases. La fase 1 corresponde a la Migración de Centrales de Tránsito y la fase 2 a la Migración de Centrales Locales.

La primera fase es totalmente transparente al usuario final (Ver *Fig. B.12*), ya que solamente las centrales de tránsito que conectan las centrales locales, son reemplazadas por Gateways de Troncales (Trunking Gateways).

Estos Gateways se encargan de recibir el tráfico conmutado de circuitos y de convertirlo a paquetes, para que puedan ser transportados sobre redes de datos IP – ATM hasta el sitio de destino de la llamada. En el destino otro Gateway se encarga de realizar la función inversa y de entregar la llamada sobre un circuito conmutado a la Central Local remota.

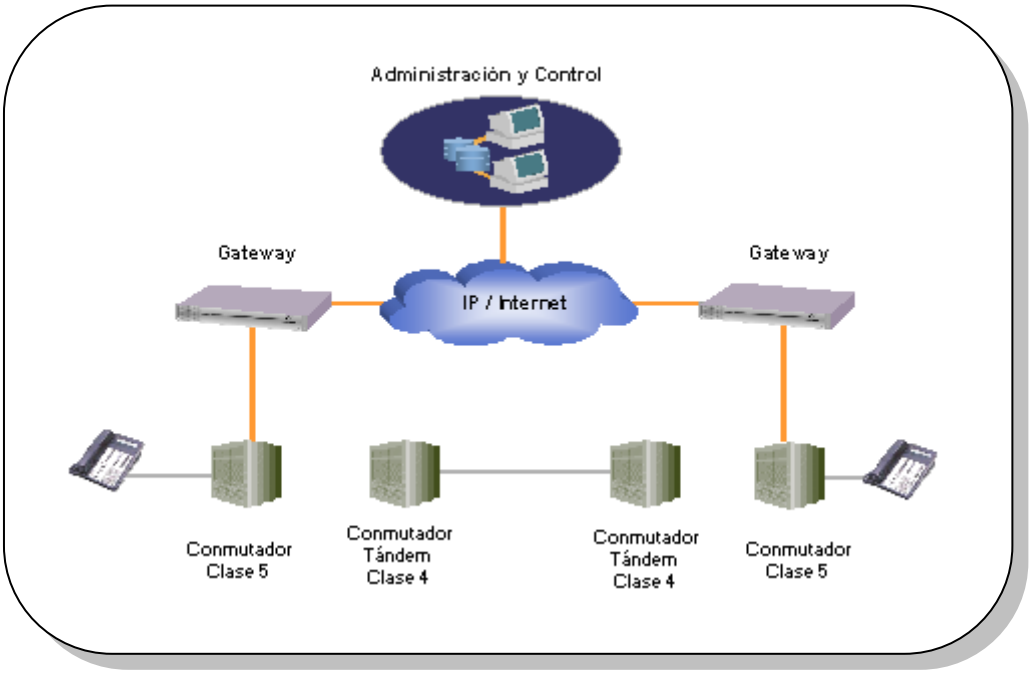



*Fig. B.12. Migración de Centrales de Tránsito.*

La conexión entre el Gateway y las Centrales locales se realiza mediante enlaces análogos o digitales E1/T1.

La segunda fase se encarga de llevar la convergencia desde el centro hasta el extremo de la red, es decir hasta el mismo usuario del servicio (Ver *Fig. B.13.*).

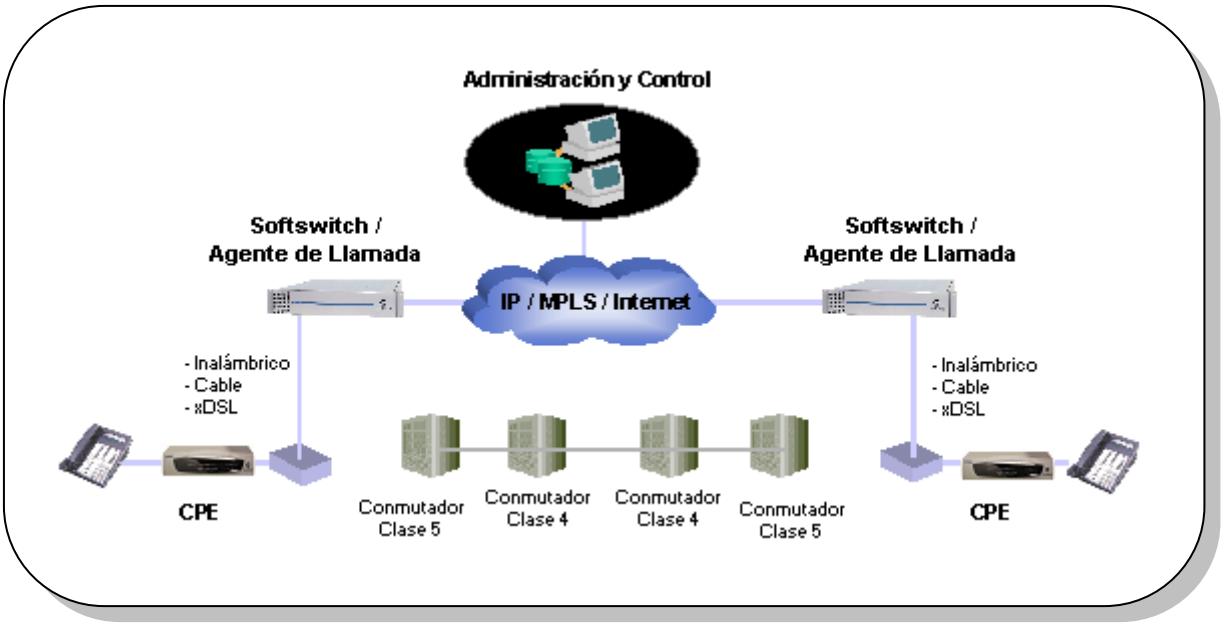



*Fig. B.13. Migración de Centrales Locales.*

Con este tipo de redes, el usuario utiliza un equipo CPE (Customer Premises Equipment - Equipo en las Premisas del Cliente) conectado a través de una Red de Banda Ancha (wireless, cable HFC, DSL, LMDS) con un backbone de paquetes, para establecer una llamada hasta otro usuario ubicado dentro de la red de datos o en la Red Telefónica Pública Conmutada.

El equipo CPE también llamado Gateway de Acceso conecta el cliente a la red backbone de paquetes bajo el control de un dispositivo conocido comúnmente como *Softswitch, Agente de Llamada (Call Agent) o Controlador de Gateways de Medio (Media Gateway Controller).*

El Agente de Llamada provee a la Red de Voz sobre Paquetes las funciones de Control de Llamada (CCF) y de Conmutación de Servicio (SSF) de la Red Inteligente para establecimiento de conexiones de llamada, administración de sesiones de llamada y peticiones de invocaciones de servicios.

Además de controlar varios Gateways de Acceso, el Agente de Llamada podría soportar capacidades limitadas de Control de Servicio (SCF) para procesar requerimientos de servicio y capacidades de acceso de RI en la RTPC para servicios pre-establecidos tales como Portabilidad de Número y Toll-Free.

Las capacidades de RI de un SCP PSTN, pueden ser accesadas usando el SS7/TCAP (Signaling System 7 / Transaction Capabilities Application Part) a través de un Gateway de Señalización. Otras arquitecturas pueden utilizar TCAP sobre IP y utilizar una red IP para comunicarse con un SCP.

Las redes de Voz sobre Paquetes son tan importantes actualmente en el mercado, que la ITU-T y la IETF se encuentran trabajando conjuntamente en la definición de las capacidades y los protocolos necesarios para soportar este tipo de redes.

Este corresponde al último paso antes de llegar a las Redes de Próxima Generación (NGN). Los carriers podrían decidir no modificar más su red y permanecer ofreciendo servicios híbridos o servicios de Voz sobre Paquetes; sin embargo, las redes NGN tienen un alcance más amplio ofreciendo las características de una arquitectura unificada e integrada, con procesamiento distribuido para las capacidades de control, administración y señalización y puede trabajar sobre múltiples tipos de redes de transporte.

### *B.6.2. SERVICIOS NGN*

Hasta ahora la mayoría de los proveedores, han estado enfocados en el mercadeo masivo de servicios de transporte de información entre usuarios, (p.e. llamadas de voz, con una conexión punto a punto por llamada) con algunas características de valor agregado. Sin embargo, este punto de vista de los servicios está cambiando rápidamente y los carriers están buscando desarrollar nuevos servicios avanzados, que les permitan seguir siendo competitivos, así como expandir sus capacidades para entrar en nuevos mercados

En el futuro los proveedores de servicios tendrán la flexibilidad para enfocarse en micro-mercadeo (lo opuesto al mercadeo masivo). Las decisiones sobre los servicios serán consideradas con base en paquetes: precio, servicios requeridos, mercadeo y conveniencia.

La meta principal será habilitar a los usuarios para conseguir el contenido de la información que ellos quieren, sobre cualquier facilidad, en cualquier medio y formato, en cualquier momento, en cualquier lugar, y en cualquier volumen.

Las redes NGN le permitirán a los carriers reducir costos eliminando las ineficiencias de las soluciones actuales propietarias, no reutilizables y con servicios específicos y disminuir el tiempo de entrada al mercado y los costos del ciclo de vida de lanzar nuevos servicios.

Los servicios tradicionales relacionados con servicios básicos de acceso / transporte / enrutamiento / conmutación, servicios básicos de control de sesión, de recursos y de conectividad y algunos servicios de valor agregado, seguirán existiendo en las redes de los carriers, al mismo tiempo que las redes NGN habilitarán un conjunto mucho más amplio de tipos de servicios.

A continuación se presenta una clasificación de los servicios NGN y algunos ejemplos de los mismos, sin embargo, no es la única clasificación que se ha hecho de los mismos.

### *B.6.2.1. Servicios de Comunicaciones Interactivas*

Estos servicios constituyen la evolución de la telefonía de voz de hoy en comunicaciones multimedia de próxima generación entre múltiples participantes. Esta categoría incluye servicios que involucran múltiples participantes que interactúan en tiempo real y que utilizan múltiples tipos de tráfico (voz, video y datos).

Debido a sus requerimientos de control dinámico y rendimiento en tiempo real, se puede considerar que será el conjunto de servicios más complejos que las redes NGN ofrecerán a sus clientes.

Los servicios de comunicaciones también incluyen servicios que no son en tiempo real y que involucran múltiples participantes y múltiples tipos de tráfico. Esto representa la evolución de la mensajería de hoy (e-mail y voz mail) en un conjunto unificado de servicios multimedia de almacenar y enviar (store and forward) con elaboradas capacidades de conversión de tráfico, control y adaptabilidad de terminal.

Algunos ejemplos de estos servicios son:

- Conferencia Multimedia Multipunto – Múltiples partes interactúan utilizando voz, datos y/o video. Los clientes pueden conversar con otros mientras despliegan información visual.

- Mensajería Unificada – Soporta la entrega de correo de voz, correo de fax, correo electrónico y páginas a través de interfaces comunes. A través de tales interfaces, los usuarios podrán acceder, así como ser notificados, de varios tipos de mensajes, independiente de los medios de acceso (es decir, teléfono móvil o fijo, computador, o dispositivo de datos inalámbricos).

### *B.6.2.2. Servicios de Datos / Información*

Estos servicios pueden ser considerados como la evolución de los servicios de datos y de Internet de hoy: navegación, búsqueda de información, directorios en línea, desarrollo de información programada, e-commerce, publicidad y otros servicios que generalmente no están basados en la red.

También incluyen un amplio conjunto de servicios de control y acceso remoto (p.e. telemetria, monitoreo, seguridad, y otros servicios orientados a datos), servicios de Procesamiento y Almacenamiento de información (p.e. Aprovisionamiento y Administración de Unidades de Almacenamiento de Información para Mensajería, Servidores de Archivos, Servidores de Terminales, Plataformas de OS, etc)

Adicionalmente incluyen Servicios de Middleware (p.e. Transacciones, Licenciamiento, Agenciamiento, etc.), y Servicios de Interworking para interacciones con otros tipos de aplicaciones, servicios, redes, protocolos o formatos (p.e. Traslación EDI (Electronic Data Interexchange)).

Algunos ejemplos de estos servicios son:

- Servicios de Datos – Establecimiento en tiempo real de conectividad de datos entre puntos remotos, incluyendo varias características de valor agregado (p.e. ancho de banda por demanda, conexión confiable y flexible de SVCs, y control de admisión de llamada y administración del ancho de banda.

- Computación Colaborativa – Recursos de computador, documentos, aplicaciones y herramientas de grupos de trabajo (groupware) pueden ser compartidas para esfuerzos de trabajo interactivo.

- Computación de Red Pública – Empresas y usuarios finales utilizan servicios de computación basados en una red pública. Por ejemplo, el proveedor podría proveer capacidades de almacenamiento y procesamiento genéricos (p.e. hosting de páginas Web; almacenamiento, mantenimiento y backup de archivos de datos; y acceso aplicaciones de computación.

- Agenciamiento (Brokering) de Información – Servicios que habilitan a los usuarios a ser enlazados con proveedores a través de publicidad, descubrimiento y entrega de información. Por ejemplo, los usuarios podrían recibir información basados en criterios pre-establecidos o basados en preferencias personales y patrones de comportamiento.

- E-commerce – Permite a empresas y usuarios comprar bienes y servicios electrónicamente sobre la red. Esto podría incluir procesamiento de transacciones, verificación de información de pagos, manejo de seguridad, y comercialización de bienes y servicios.
  Los servicios de los clientes incluyen "Home Banking" (un banco en el hogar) y "Home Shopping" (compras en el hogar). También se incluyen Aplicaciones de Negocios a Negocios (Business to Business) tales como administración de la cadena de abastecimiento (supply-chain) y conocimiento de las aplicaciones de administración.

- Redes Privadas Virtuales (VPN) – Servicios VPN de datos se expanden más allá de los servicios VPN de voz tradicionales y proveen adicionales características de seguridad y conectividad de red que permiten a los clientes utilizar una red IP compartida como un grupo cerrado de usuarios.

#### *B.6.2.3. Servicios de Educación / Entretenimiento*

La tercera clase de servicios que un carrier deberá ofrecer con las redes NGN se relaciona con el desarrollo de contenido (content delivery). Estos servicios pueden ser ofrecidos por demanda, casi por demanda, sobre una base broadcast o multicast o sobre una base de desarrollo diferido para usar posteriormente.

Los servicios por demanda y/o multicast (video por demanda, música de alta calidad por demanda, etc.) involucran interesantes retos técnicos desde el punto de vista de la escalabilidad.

Algunos ejemplos de estos servicios son:

- Aprendizaje a Distancia – Los usuarios pueden tomar cursos interactivos desde locaciones remotas. Estos cursos pueden ser ofrecidos en un entrenamiento basado en computador o en un ambiente de clase virtual.

- Juegos Interactivos – Los usuarios finales pueden encontrar juegos de video en línea y establecer sesiones interactivas de juego.

- Realidad Virtual Distribuida – Se refiere a representaciones de eventos, personas, lugares, experiencias, etc, del mundo real generados tecnológicamente, en los cuales los participantes entran y los proveedores de las experiencias virtuales se encuentran físicamente distribuidos.

#### *B.6.2.4. Servicios de Administración / Auxiliares*

Esta última clasificación incluye los Servicios de Administración para mantener, operar y administrar los servicios y redes de comunicaciones / computación. Esta clase incluye servicios tales como suscripción, aprovisionamiento de clientes, administración de red de clientes y administración de servicios de clientes.

El principal método de acceso a estos servicios probablemente será a través de una interfaz Web. Muchos servicios en esta categoría son típicamente necesitados como soporte de otros servicios de usuario final, y por esto se consideran auxiliares por naturaleza.

Otros servicios en esta clase incluyen administración de configuración, administración y monitoreo de rendimiento, administración de cuentas y facturación, administración de seguridad de servicios, ejecución de políticas y servicios similares. Ofreciendo versiones amigables y eficientes de estos servicios, en conjunto con los servicios primarios, vendrá a ser un fuerte diferenciador de servicios en las redes NGN.

Algunos ejemplos de estos servicios son:

- Administrador del Hogar – Con la aparición de la conectividad en el hogar y los aparatos inteligentes, estos servicios podrían monitorear y controlar los sistemas de seguridad, los sistemas de energía, los sistemas de entretenimiento y otros aparatos del hogar.

- Servicios de Centro de Llamadas (Call Center) – Un suscriptor puede colocar una llamada a un agente de Centro de Llamadas realizando la petición desde una página Web. La llamada puede ser enrutada al agente adecuado, quien puede estar localizado en cualquier lugar, inclusive en su casa (Centros de Llamadas Virtuales).

### *B.6.3. RELACION NGN CON REDES INTELIGENTES*

La arquitectura de red NGN puede ser descompuesta en Entidades Funcionales, tal como ocurre en las Redes Inteligentes (Ver *Fig. B.14.*).

Para cada elemento del nivel de Control de Servicios en la arquitectura NGN (el softswitch es descompuesto en funciones) hay una correspondiente entidad funcional en la arquitectura de RI:

- La *Función de Soporte/Control* (Service Control/Support Function) es responsable por proporcionar las capacidades de valor agregado a las sesiones de los servicios (por ejemplo, características suplementarias). Esta función corresponde a la SCF de RI.

- La *Función de Fábrica de Servicios* (Service Factory Function) es responsable por el manejo de componentes dinámicamente para soportar sesiones de servicios y corresponde a la SCF y SDF de RI (por ejemplo, almacén de datos para lógica del servicio).

- La *Función de Administración de Sesión* (Session Management) es responsable por el manejo de las sesiones de acceso, servicio y comunicación, correspondientes al SSF de RI.

- La *Función de Administración de Conectividad* (Connectivity Management) es responsable por las conexiones a través de las redes de paquetes y de los gateways de interconexión. Esta capacidad corresponde al CCF de RI.

- La *Función de Administración de Interrelación* (Interworking Management) es responsable por el manejo de la interrelación con la arquitectura de servicios PSTN existente (via ISUP y TCAP). Esto incluye manejo de activadores (triggers) de RI (petición de servicios) y control de los dispositivos gateways de bajo nivel. Esta capacidad tiene elementos de la SSF y CCF de RI.

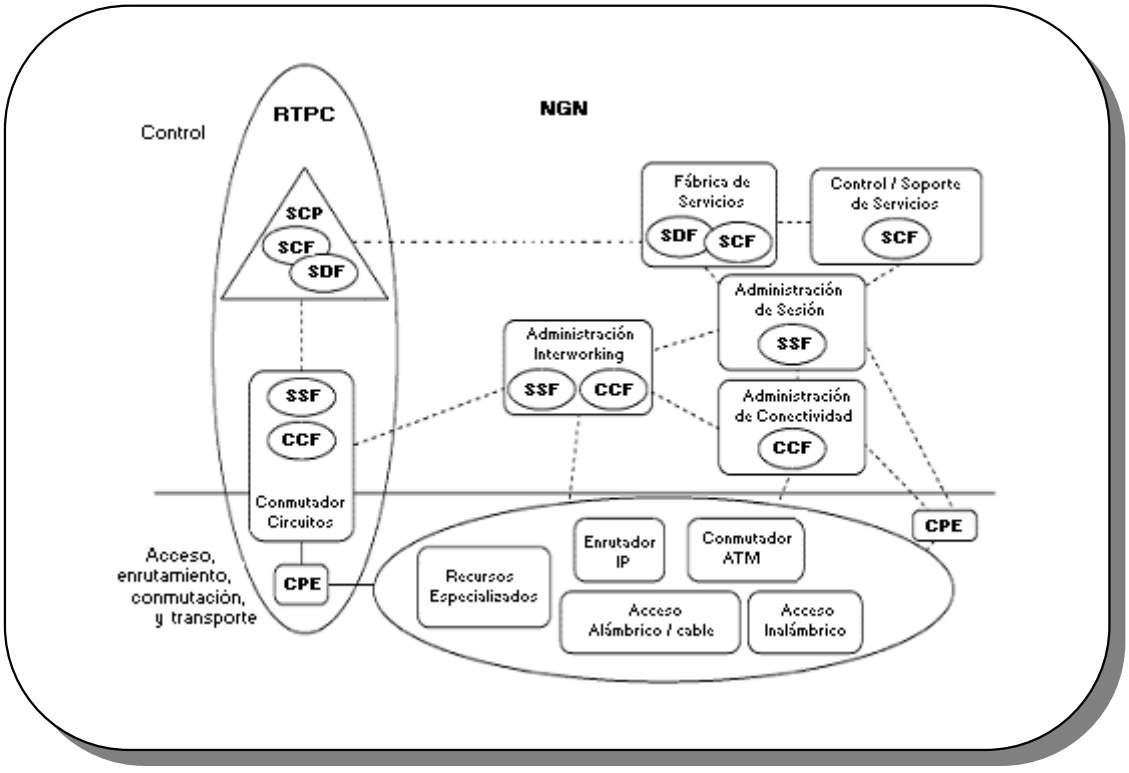



*Fig. B.14. Entidades Funcionales de las Redes NGN*

En el nivel más alto de la arquitectura NGN se encuentran las funciones de Administración de Servicio (SMF), Agente de Administración de Servicio (SMAF) y Ambiente de Creación de Servicios (SCEF), cada uno de los cuales realiza funciones similares o corresponde a elementos de red en la RI.

Muchas de las funciones encontradas en el SCP y SSP han sido descompuestas. Esta separación de funcionalidad en elementos discretos en el nivel de control de servicios aprovecha la ventaja de la Computación de Objetos Distribuidos soportando un Ambiente de Procesamiento Distribuido (DPE – Distributed Processing Environment) independiente de la plataforma, con capacidades y servicios middleware.

## B.7. VOZ SOBRE INTERNET

Hasta hace algunos años, la transmisión de Voz sobre Internet era solamente una posibilidad, hoy en día, es una realidad. Esto ha obligado a realizar detallados estudios económicos y regulatorios en todo el mundo, en especial para determinar como manejar la gigantesca diferencia de costos entre la transmisión de Voz sobre Internet y la transmisión de Voz sobre las Redes Telefónicas Públicas Conmutadas.

IP fue diseñado para transmitir archivos de datos que pueden tolerar retardos, pérdida de paquetes y retransmisiones. La voz, en cambio, es sensitiva al retardo, por lo que siempre se había transmitido a través de redes públicas de circuitos conmutados.

Sin embargo, los desarrollos tecnológicos hardware y software de los equipos de comunicaciones, nos permiten estar hoy en día, a las puertas de la próxima generación de empresas de telecomunicaciones globales, que brindarán transmisión de voz / fax y datos sobre Internet.

Las características claves que debe tener una red de datos para transportar bien la voz, son: bajo retardo, desarrollo predecible de la información de voz, recursos de prioritización del tráfico de voz por encima de los datos, y una alta eficiencia para transportar el tráfico de voz extra. La eficiencia solo se relaciona indirectamente con el transporte de voz, sin embargo, sin una alta eficiencia de la tecnología, se deberá adicionar ancho de banda extra para su transporte, incrementando los costos y reduciendo al mínimo los ahorros que se pueden alcanzar.

Voz sobre IP (VoIP) es una tecnología que permite a los sistemas y enlaces que conectan las redes de computadores, actuar como una alternativa a las líneas de teléfonos – desarrollando voz en tiempo real tanto para teléfonos como para PCs estándares.

Voz sobre IP permite a los usuarios realizar llamadas de voz y fax entre los puntos de su compañía (en el caso de redes de datos corporativas, Intranets) o entre puntos de la Red Telefónica Pública Conmutada (las redes de Voz sobre Paquetes se explicarán en el capítulo 5) sobre redes de datos IP (e Internet), o sobre redes ATM, mejorando la integración de los servicios de voz con servicios de datos y video y generando ahorros entre el 70% y el 80% en consumo telefónico nacional e internacional.

La tecnología de VoIP trabaja creando una red paralela (overlay) de voz/fax encima de cualquier conexión IP existente. El tráfico de voz o fax es encapsulado en un paquete IP y enviado sobre la red IP.

### *B.7.1. TENDENCIAS VOIP*

Según el reporte “IP Telephony Services: Market Forecast and Analysis, 1999 – 2005” publicado por IDC en 2000: *“Los ingresos del servicio de Telefonía IP están proyectados para alcanzar $1.0 billón de dólares en 2000 (Ver Tabla 10*). El ingreso está proyecto*

*para incrementarse en un CAGR de 127% para exceder $61 billones de dólares en 2005".* (*Ver *Tabla B.2.*)

**Table 10**
**Worldwide Retail and Wholesale IP Telephony Services Revenue, 2000–2005 ($M)**

| | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2000–2005 CAGR (%) |
|---|---|---|---|---|---|---|---|
| Retail | | | | | | | |
| Paid consumer/small business | 330 | 908 | 2,723 | 7,657 | 20,419 | 51,047 | 174 |
| Corporate | 2 | 71 | 549 | 1,553 | 4,098 | 6,989 | 396 |
| Wholesale | 683 | 916 | 1,192 | 1,733 | 3,162 | 3,266 | 37 |
| Total | 1,015 | 1,895 | 4,464 | 10,943 | 27,678 | 61,301 | 127 |

*Tabla B.2. Proyección de Ingresos de Telefonía IP. 2000-2005.*

Este incremento se debe principalmente a dos factores:

- Técnicas de VoIP están siendo adoptadas rápidamente por los ISPs. Desde que los ISPs ya provean acceso de datos sobre la infraestructura existente, VoIP les permitirá obtener mayores ganancias ofreciendo también voz/fax.
- VoIP es clave para la Integración Telefonía – Computación (CTI – Computer Telephony Integration). Varios estándares son ampliamente aceptados hoy en día por el mercado, ellos son: H.323 es el más ampliamente aceptado por los vendedores, SIP, MGCP/MEGACO. VoIP permitirá a los sistemas ordinarios de teléfonos, teléfonos de PC y CTI co-existir. Se presentará una fuerte demanda de Gateways de Voz sobre Internet y aplicaciones tales como Telefonía, por lo que los centros de llamadas (Call Centers) serán capaces de atender llamadas de teléfonos normales o llamadas de redes IP, sin cambiar equipos o reentrenarse.

### *B.7.2. REDES INTELIGENTES - VOIP*

Varios factores favorecen la utilización de las tecnologías de Redes Inteligentes para soportar VoIP Los rápidos desarrollos que se están dando en VoIP, han acelerado la aparición de una nueva generación de carriers de telecomunicaciones globales, y han propiciado alianzas entre proveedores de productos y servicios.

Varios factores favorecen la utilización de las tecnologías de Redes Inteligentes para soportar VoIP:

- Ya que las conexiones migran desde conmutación de circuitos a conmutación de paquetes, la RI es un poderoso medio para soportar ambos tipos de transporte, apalancando infraestructuras existentes y reutilizando servicios de red existentes.

- Existe una extensa base de servicios de voz basados en RI, tales como Número 800/Freephone y Redes Privadas Virtuales (VPNs), que ofrecen un valor considerable a los usuarios finales y que generan miles de billones de dólares en ingresos a los carriers en todo el mundo.

- Las implementaciones de RI separan la lógica del servicio de la administración de la conexión, y este es un modelo de distribución que es muy compatible con las redes VoIP.

La convergencia crea oportunidades adicionales para que las RI adicionen valor a los servicios de datos:

- Utilizando las conexiones de datos basadas en Internet par controlar servicios de voz, permitiendo a los usuarios mayor control sobre sus servicios a través de mejores interfaces de usuarios.

- Extendiendo los servicios de RI a datos y video. Las plataformas de RI proveen capacidades de ejecución de servicio y administración de datos necesarios para las redes conmutadas de paquetes y las redes conmutadas de servicios.

Actualmente, la tecnología está disponible para transportar llamadas de voz sobre una red de datos como Internet y obviamente sobre la tradicional Red Telefónica Pública Conmutada (RTPC).

La tecnología para transportar tráfico de voz sobre la RTPC tradicional está basado en estándares de “circuitos conmutados” y la tecnología para transportar información sobre la Red IP está basada en estándares de “paquetes conmutados”. Actualmente se están presentando diferentes tendencias para unificar las redes de conmutación por circuitos y de conmutación por paquetes, de tal forma que los abonados puedan tener acceso a ambas y completar una llamada telefónica a cualquier destino. Este tema se explicará extensamente en el capítulo 5.

Además, ninguno de los servicios de Red Inteligente, tales como Portabilidad de Número Local (LNP - Local Number Portability), VPN, o los servicios de voz mejorados como Identificación de abonado llamante (caller-ID), correo de voz, sistemas de menú de voz, son ofrecidos a través de las Redes de Telefonía sobre Internet.

# ANEXO C – VPN IP

Este documento presenta algunas consideraciones básicas de las redes VPN IP, los componentes hardware necesarios para implementar una red VPN IP, explicando en detalle el funcionamiento de los cortafuegos *(firewall),* que corresponden a uno de los principales elementos utilizados para garantizar la seguridad de una red.

Se describen los principales factores que se deben cumplir al realizar una transmisión de datos sobre redes públicas, haciendo énfasis especialmente en las técnicas de "creación de túneles" (*tunnelling*). Adicionalmente se hace un análisis detallado de los dos principales protocolos para creación de túneles, los cuales son IPSec y MPLS y finalmente se presenta una comparación entre ellos.

## C.1. CONSIDERACIONES BASICAS DE LAS REDES VPN IP

Una VPN es una red corporativa desarrollada sobre una infraestructura pública empleando las mismas políticas de seguridad, administración y rendimiento de procesamiento aplicadas en una red privada.

Las VPNs son una infraestructura alterna a las redes WAN existentes y satisfacen los mismos requerimientos de las redes WAN, tales como soporte para múltiples protocolos, alta confiabilidad, y escalabilidad, pero lo hacen de una manera más rentable y con mayor flexibilidad.

Una VPN puede utilizar cualquiera de las tecnologías de transporte disponibles hoy: Internet público, redes IP de proveedores de servicios, así como redes Frame Relay y ATM de proveedores de servicios. La tecnología del transporte se mantiene transparente a los clientes, ya que ellos utilizan simplemente una interfaz de acceso IP para tener acceso a la plataforma VPN en su borde, sin importar la plataforma desde la cual el proveedor de servicio ha elegido entregar el servicio.

Las VPNs se dividen en tres categorías principales: acceso remoto, intranets y extranets. Las VPNs de acceso remoto conectan a los usuarios teleconmutados, usuarios móviles, o inclusive oficinas remotas más pequeñas con mínimo tráfico, con la red WAN de la empresa y con sus recursos computacionales. Una VPN Intranet conecta las localizaciones fijas y oficinas remotas creando una red WAN corporativa. Una VPN Extranet permite el acceso a los recursos computacionales de la empresa a sus socios de negocios, tales como proveedores o clientes.

Las VPNs ofrecen a los clientes muchas ventajas sobre las redes tradicionales, entre ellas se incluyen:

- *Costos más bajos que en las redes privadas:* Comparado con las redes privadas y redes dedicadas arrendadas, se reducen los costos por ancho de banda de transporte, equipos de backbone y operaciones. Los costos de conectividad de LAN a LAN típicamente se reducen entre un 20 y un 40 por ciento para las redes de líneas dedicadas o privadas domésticas y entre un 60 y un 80 por ciento para las redes de acceso remoto.

- *Mayor escalabilidad y flexibilidad:* Las VPNs son más flexibles y escalables que las redes WAN clásicas, permitiendo a las empresas ampliar su conectividad rápida y rentablemente, facilitando la conexión o desconexión de oficinas remotas, localizaciones internacionales, usuarios teleconmutados, usuarios móviles, y socios de negocios externos.

- *Cargas administrativas reducidas comparadas con la operación de una infraestructura de red privada propia:* Las empresas pueden contratar algunas o todo las funciones WAN a un proveedor de servicios, permitiendo a las empresas centrarse en los objetivos de su negocio base, en vez de manejar una red WAN o una red de acceso remoto.

- *Simplifica las topologías de la red:* Utilizando un backbone IP se eliminan los circuitos virtuales permanentes estáticos (PVCs) asociados con protocolos orientados a conexión como Frame Relay y ATM, por lo que se puede crear una topología completamente enmallada de la red mientras se disminuye la complejidad y el costo de la red.

De igual manera los proveedores de servicios obtienen grandes beneficios, entre los cuales se incluyen:

- *Nuevos mercados:* Extensión del mercado gracias a la inclusión de empresa pequeñas y a la capacidad de participar en el espacio de negocios a negocios B2B (business to business).

- *Nuevos servicios:* Ofrecimiento de soluciones administradas de valor agregado, más allá de los servicios básicos, tales como acceso a Internet, administración y soporte de soluciones de negocios Intranet y extranet.

- *Retención del cliente:* Una posición más estratégica para el proveedor de servicios con sus clientes en comparación con un simple servicio de transporte /conectividad. Proporcionando un camino de migración permitiendo a las empresas crecer y liberarse de la tecnología según sea requerido.

- *Diferenciación:* La viabilidad competitiva a largo plazo requiere ofrecer los servicios VPN IP dentro del portafolio de productos.

- *Posicionamiento futuro:* Punto de entrada para las necesidades futuras de outsourcing de la empresa, tales como servidores y aplicaciones. Ofrece las bases para un conjunto altamente rentable y expandible de soluciones de seguridad.

## C.2. COMPONENTES HARDWARE PARA LAS VPNs IP

Para implementar los diferentes tipos de VPNs, se requieren diferentes dispositivos de hardware. Muchos de estos dispositivos son comunes a las redes estándar, pero algunos tienen responsabilidades adicionales cuando se aplican a las VPNs. Los principales dispositivos hardware empleados por las VPNs son los siguientes:

**Servidor VPN.** Normalmente es un componente hardware, aunque también lo puede ser software, que puede actuar como un gateway en una red o en un único computador. Debe estar siempre conectado y esperando a que clientes VPN se conecten a él. El software para el Servidor VPN es bastante común. Sistemas como **Windows 2000 Server** permiten alojar un Servidor VPN. El precio a finales del año 2001 para el hardware de los Servidores VPN oscilaba entre los *$170* y los *$300* dólares. (Ver *Fig. C.1.*)

**Cliente VPN.** En la mayoría de los casos es un componente software, aunque puede ser también un componente hardware. Un cliente realiza una llamada al servidor y se conecta. Entonces la computadora cliente podrá comunicarse con el Servidor VPN, ya que ellos se encuentran en la misma red virtual. El software para un cliente VPN es bastante común. Cuando se carga en la computadora este software permite crear un túnel seguro VPN a través de Internet para poder comunicarse con el Servidor VPN. (Ver *Fig.C.1.*)

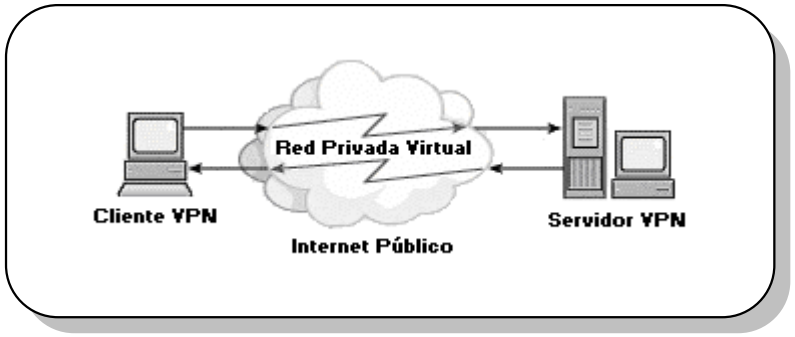



*Fig. C.1. Servidor y Cliente VPN.*

**Firewalls.** Proveen servicios críticos tales como creación de túneles (tunnelling), criptografía y filtrado de contenido y de rutas, con el fin de proteger la red de usuarios no permitidos.

**Enrutadores.** Puede adicionarse la funcionalidad VPN a enrutadores existentes, pero esto podría tener un impacto negativo en el rendimiento, particularmente en los puntos críticos de la red. Las VPNs MPLS manejan este problema haciendo que solamente los Enrutadores de Borde (PE – Perimeter Routers) tengan la capacidad VPN, así los Enrutadores de Núcleo (Core Routers) no necesitan mantener múltiples tablas de enrutamiento las cuales introducen demasiado encabezado en los enrutadores PE.

**Conmutadores (switches).** Algunos switches ofrecen facilidades para una mejor separación de tráfico, permitiendo a una red física ser particionada en un número de V-LANs. Sobre un switch normal, todos los puertos son parte de la misma red, mientras un

switch V-LAN puede tratar puertos diferentes como partes de diferentes redes si se desea.

**Servidores de Túneles.** Este servicio puede ser proporcionado por un enrutador VPN o por un firewall, permitiendo la creación de túneles. Asignando esta responsabilidad adicional a un componente de red existente puede tener un serio impacto en el rendimiento.

**Tarjetas de Encripción (Cryptocards).** Hardware especializado de criptografía que es instalado en estaciones de trabajo (o computadores) soportando el algoritmo de encripción Triple-DES proporcionado por IPSec, sin afectar el rendimiento del equipo. Este hardware es proporcionado en forma de una tarjeta de expansión, la cual puede estar separada o integrada con la NIC. Algunos firewalls también ofrecen soporte de hardware para varios algoritmos de encripción.

### *C.2.1. CORTAFUEGOS (FIREWALLS)*

Los Cortafuegos son una buena protección para las redes privadas desde Internet. Permiten la restricción en el número de puertos abiertos, el tipo de paquetes que pasan a través de ellos y los tipos de protocolos aceptados. Los cortafuegos pueden también ser utilizados para terminar sesiones VPN.

Los cortafuegos están presentes para proteger los recursos corporativos de ataques, a diferencia de la autenticación y la encripción VPN que generalmente son utilizadas para proteger la información corporativa mientras se encuentra fuera de la empresa.

Es indudable la importancia de los Cortafuegos para la implantación de medidas de seguridad en las conexiones de la red corporativa con Internet. Actualmente constituyen uno de los principales componentes para la definición e implantación de la política de seguridad en la empresa, no solamente para el control de accesos entre la red Corporativa e Internet sino como parte de soluciones más amplias de seguridad integral en Intranets y para la creación de Redes Virtuales Privadas (VPN) incluso con servicios de cifrado de la información.

No todos los Cortafuegos son iguales, ni todas las empresas tienen los mismos requerimientos de seguridad. La selección de la tecnología utilizada por el Cortafuegos y la arquitectura del mismo son aspectos primordiales en el proceso de decisión para implantar un Cortafuegos.

Existen básicamente las siguientes tecnologías que definen la arquitectura de los cortafuegos:

- Filtrado de paquetes (Packet Filter).
- Pasarela de Aplicación (Aplication Gateway - Proxy).
- Inspección de Estados (Stateful Inspection).

### *C.2.1.1. Filtrado de paquetes*

Los cortafuegos de filtrado de paquetes examinan varios campos específicos en el encabezado del paquete para determinar el acceso.
Como filtro de paquetes, dispone de una potente ayuda para la definición de las reglas apropiadas basadas en la interfase de red, dirección y tipo de datos. Para cada regla que se define, pueden configurarse atributos como "autorizar respuestas" o "forzar puerto" o bien permitir, denegar o auditar un determinado paquete. Puede inspeccionar y trabajar sin problemas con protocolos del tipo sin conexión (connectionless) como ICMP (Internet Control Message Protocol) y UDP (User Datagram Protocol).

### *C.2.1.2. Funcionamiento como Pasarela de Aplicación (Proxy)*

Como filtro a nivel de aplicación (proxy), el cortafuegos puede configurarse para la práctica totalidad de las aplicaciones existentes para Internet.

Existe un proxy específico para cada aplicación y proporciona el aislamiento necesario entre las dos redes, estableciendo sesiones separadas. Todas las aplicaciones proxy proporcionan funcionalidad de pasarela de circuitos y algunas de ellas proporcionan autentificación y funcionalidad de verificación de contenido.

Los proxies a nivel de circuito (Circuit Gateway Proxies) proporcionan una conexión entre las redes pública y privada, asegurando que solamente atraviesan el cortafuegos las solicitudes adecuadamente formateadas.

Los proxies de autentificación (Authenticating Proxies) requieren a los usuarios autentificarse en el cortafuegos antes de que se permitan conexiones a través del cortafuegos.

Los proxies de verificación de contenido (Content Enforcement Proxies) examinan el contenido de las conexiones y controlan las acciones o la información que atraviesa el cortafuegos.

El filtrado proxy trabaja en el nivel de aplicación (Nivel 7) de la torre OSI, lo que significa que el cortafuegos examina el paquete completo para cada paquete que pasa. Este tipo examina información específica dentro de un paquete para deteminar el acceso, tal información es personalizada por cada aplicación.

*Los cortafuegos proxy* operan en los niveles superiors de la torre OSI, y por lo tanto requieren procesamiento extra comparado con los cortafuegos de filtrado de paquetes y de inspección de estado que operan principalmente en los niveles 3 y 4.

### *C.2.1.3. Funcionamiento como Inspección de Estados*

Las decisiones de seguridad realizadas en una máquina con un sistema operativo seguro, son inherentemente inseguras. Parte de la potente solución de seguridad aportada es la

utilización de la tecnología de "Reglas de Estados Dinámicas" (una implementación de la tecnología de Inspección de Estados).

El Cortafuegos monitorea cada conexión para asegurar que todo el tráfico de red desde el cliente o el servidor, cumple con la política de seguridad de la red y con su protocolo correspondiente. Esta tecnología trabaja con todo el tráfico IP incluidos UDP y ICMP.

Cada conexión tiene una única regla de estado dinámica, que permite al cortafuegos monitorear el estado de cada conexión individual y por lo tanto implantar la política de seguridad específica para dicha conexión.

Cualquier paquete recibido por el cortafuegos que no cumple con la política definida, se descarta proporcionando la correspondiente alarma.

Los cortafuegos de inspección de estados inspeccionan principalmente los niveles 3 y 4 y dinámicamente abren el acceso a tráfico autorizado. Ellos mantienen en el caché un rastreo de cada conexión autorizada y apagan el acceso cuando la conexión se completa.

## C.3 SEGURIDAD EN REDES PRIVADAS VIRTUALES

Como se mencionó en la sección 4.3.2. del trabajo de grado, los principales factores que deben ser ofrecidos cuando se transmiten datos sobre redes públicas son:

- Privacidad (encripción).
- Integridad (suma de comprobación - *checksum*).
- Autenticación.
- No Repudiación (firmas digitales).

Adicionalmente a los factores que garantizan la seguridad de los datos, se deben tener en cuenta otros factores tales como administración de acceso y la seguridad en la transmisión (túneles) de la información.

A continuación se presenta una breve descripción de cada una de las principales herramientas para garantizar la seguridad en una VPN.

### *C.3.1 ENCRIPCIÓN*

Algoritmos criptográficos son esenciales para lograr comunicaciones seguras sobre redes públicas. Sin embargo puede tener implicaciones para la operación de la VPN entre ellas el costo (en especial utilizando hardware especializado), efectos negativos sobre el rendimiento y molestias en el análisis de protocolos, monitoreo de fallas, filtrado de contenido y otras utilidades de la administración de la red.

Hay un número de diferentes algoritmos de encripción disponibles, muchos de los cuales soportan varios niveles de seguridad. Los esquemas de encripción más ampliamente

utilizados son: Estándar de Encripción de Datos (DES - Data Encryption Standard) y Triple DES (3-DES). DES ha sido un estándar de facto en las comunicaciones de datos por bastantes años, utilizando claves desde 56 bits, sin embargo, el incremento en las capacidades de procesamiento de los computadores ha hecho que hoy en día solamente las claves de mayor longitud soportadas por DES sean consideradas seguras, tales como claves de 128 bits. Triple DES utiliza claves de 112 o 168 bits.

Otros algoritmos, tales como IDEA (International Data Encryption Algorithm), CAST, RC5 y Blowfish también son utilizados. IDEA utiliza una clave de 128-bits y ha demostrado hasta ahora ser altamente resistente al criptoanálisis. El tamaño de la clave de CAST varia desde 40 hasta 128-bits y su característica clave es que la función de redondeo difiere de redondeo a redondeo, adicionando esto a su fortaleza criptoanalítica. Las operaciones matemáticas de Blowfish son similares a DES, pero el tamaño de su clave es variable hasta 448 bits, pero no es conveniente para aplicaciones en la cual la clave secreta cambia frecuentemente.

### *C.3.1.1. Generación de Claves*

Ya que los algoritmos de encripción son conocidos, la fortaleza de la encripción depende de la generación de las claves y la administración de las mismas. Es mejor utilizar claves generadas aleatoriamente puesto que esto hace imposible predicciones pasadas y futuras de claves. Las claves generadas por hardware, por ejemplo utilizando diodos de ruido, son más seguras que las claves generadas por algoritmos, ya que invirtiendo suficiente tiempo y dinero, es posible descubrir estas claves.

Otra decisión para considerar es la longitud de la clave. Entre más larga es la clave, más difícil es descubrirla. De acuerdo con la asociación “RSA Security Inc.” claves con longitudes menores de 56 bits son consideradas inseguras.

### *C.3.1.2. Intercambio de Claves*

El algoritmo Diffie-Hellman es considerado como el estándar establecido para el intercambio de claves. Pero para proporcionar encripción / desencripción así como firmas digitales, debe ser utilizado el algoritmo de encripción de claves públicas RSA.

La encripción / desencripción en este caso, se refiere al remitente encriptando el mensaje con la clave pública del receptor. Las firmas digitales, se refieren al remitente “firmando” un mensaje con su clave privada.

Una VPN es más segura entre más frecuentemente ocurra el intercambio automático de claves. El intercambio manual de claves es considerado inseguro ya que los usuarios pueden no recordar realizar el intercambio de claves.

### *C.3.2. INTEGRIDAD – CHECKSUM*

Una suma de comprobación (checksum) es una serie de bits de longitud fija, cuyo valor se deriva de un bloque de datos dado. Los checksums son frecuentemente adicionados a un bloque de datos antes de su transmisión, de modo que el receptor pueda verificar que los datos fueron recibidos en las condiciones exactas en las cuales fueron enviados.

Los checksums simples son sencillamente una cuenta del número de bits en una unidad de transmisión, la cual es insuficiente para los propósitos de seguridad ya que no proporciona ningún medio de verificar la integridad de los datos recibidos, sólo que el tamaño sea correcto.

Para esto se introducen las funciones hash, las cuales tienen mayores requerimientos computacionales que una cuenta simple, pero permiten la verificación de que la transmisión fue recibida satisfactoriamente, libre de errores de transmisión o de ataques deliberados en el camino.

Los requerimientos básicos para una función hash criptográfica son:

- La entrada puede ser de cualquier longitud pero la salida es siempre de una longitud fija.
- La función hash es una algoritmo unidireccional.
- La función hash es razonablemente libre de colisiones.

El valor hash, también conocido como resumen del mensaje, representa el mensaje o documento más largo de los cuales fue derivado. Un resumen del mensaje actúa como una forma de “huella digital” del documento original, y puede ser hecho público sin revelar el contenido del documento correspondiente.

El papel principal de una función hash criptográfica en VPN está en la provisión de chequeos de integridad del mensaje y en las firmas digitales.

### *C.3.3. AUTENTICACIÓN*

La autenticación de usuarios VPN generalmente se realiza confirmando el conocimiento de un secreto compartido. Hay varios niveles de autenticación aplicados a las VPNs en la industria.

#### *C.3.2.1. Contraseñas (Passwords)*

Utilizar únicamente contraseñas puede ser la forma más débil de autenticación. Aunque las contraseñas no son costosas de desarrollar, pueden ser robadas o adivinadas. Una contraseña alfa-numérica puede ser verificada por un servidor de autenticación trabajando con RADIUS o un servicio equivalente.

### *C.3.2.2. Certificados Digitales*

Esta forma de autenticación ha llegado a ser más común con el crecimiento de transacciones basadas en Internet. Los certificados digitales trabajan identificando a los usuarios que tienen acceso a las credenciales digitales como los dueños legítimos. Estos certificados pueden ser utilizados solos, o con contraseñas.

### *C.3.2.3. Autenticación de Dos-Factores*

Esta implementación de autenticación es más segura que las contraseñas y los certificados digitales. Requiere que los usuarios presenten dos formas de identificación. Esto podría ser comparado a utilizar un cajero automático de un banco, donde los usuarios tienen que conocer el PIN y poseer el dispositivo de autenticación (por ejemplo, la tarjeta inteligente). Combinando los certificados digitales con autenticación de dos-factores incrementa mucho más el grado de seguridad.

### *C.3.2.4. Tarjetas Inteligentes con Certificados Digitales*

Esta es una de las formas más seguras de autenticación. En primer lugar, la tarjeta inteligente es protegida con autenticación de dos-factores. En segundo lugar, pares de claves también pueden ser generadas y almacenadas en la tarjeta. La clave privada no deja la tarjeta, así usuarios no autorizados no pueden copiar la clave.

### *C.3.2.5. Tarjetas Inteligentes con Certificados y Biométrica*

Utilizando la biométrica con las tarjetas inteligentes y los certificados digitales asegura el nivel más fuerte de autentificación disponible. Esto se debe al hecho de que la biométrica se refiere a características que son únicas a un usuario particular. Medidas tales como la huella dactilar y la exploración retiniana son actualmente disponibles.

### *C.3.4. ADMINISTRACIÓN DE ACCESO*

Una vez que un usuario ha ganado acceso a la red, puede representar una amenaza para la seguridad de la empresa, ya que podría tener acceso ilimitado a casi todos los recursos en la VPN llegando a conocer las vulnerabilidades del sistema y donde se encuentra información sensible. A pesar de los riesgos implicados de proteger una VPN y sus recursos contra usuarios que han logrado acceso, se le asigna una prioridad relativamente baja, si no es ignorada completamente.

Usando herramientas de administración del acceso, como Kerberos, una empresa puede garantizar que los usuarios tienen acceso solamente a los recursos para los cuales explícitamente se les ha asignado derechos de acceso.

Generalmente, el proceso de administrar y restringir el acceso a los recursos de la VPN implica mantener una Lista de Control de Acceso (ACL - Access Control List) para cada uno de los recursos para los cuales el uso se restringe a los usuarios o a grupos específicos de usuarios. Cuando un usuario intenta tener acceso a un recurso dado, la herramienta de administración de acceso consulta la ACL para ese recurso, y concederá posteriormente el acceso solamente si el usuario aparece en la lista.

### *C.3.5. INFRAESTRUCTURA DE CLAVES PUBLICAS (PKI)*

Una infraestructura de claves públicas abarca una gama de tecnologías que juntas proporcionan intercambio de datos seguros y privados sobre una red pública insegura tal como Internet. Un PKI provee seguridad utilizando criptografía de claves públicas, la cual provee no solamente encripción, sino también los servicios de autenticación y no repudiación. También permite a los certificados digitales identificar individuos u organizaciones. Los servicios de directorio almacenan y, cuando es necesario, revocan certificados.

Las capacidades de PKI son importantes para las operaciones de las VPNs, puesto que el intercambio de certificados digitales es el método más eficiente y escalable para realizar la distribución de claves seguras compartidas sobre redes no confiables. Este mecanismo puede ser utilizado para proporcionar una fuerte autenticación de usuario de la cual carece el protocolo IPSec.

#### *C.3.5.1. Implementación de un PKI*

Un cliente VPN puede implementar su propio PKI o puede contratarlo con otra organización. Esta decisión depende principalmente del presupuesto y de los requerimientos de seguridad para la VPN. Si el cliente implementa su propio PKI obtiene control, pero se requiere una muy alta inversión, tanto inicialmente en software y hardware, como posteriormente para el mantenimiento y soporte.

La Autoridad de Certificación (CA – Certification Authority) es responsable de producir los siguientes documentos, los cuales son cruciales para la operación exitosa del correspondiente PKI:

- Política de Certificados (CP – Certificate Policy). Un CP es un documento formal que especifica los requisitos para emitir certificados. El CP también especifica los requisitos que la CA está obligada a cumplir, para propósitos de seguridad y de responsabilidad.
- Declaración Práctica de Certificados (CPS – Certificate Practice Statement). El operador de la CA debe escribir una CPS, la cual define el método de operación de la CA para cumplir los requisitos delineados en el CP

### *C.3.5.2. Certificados Digitales*

Un certificado digital actúa como una identificación electrónica para establecer las credenciales de una parte comunicándose. Contiene la información sobre el tenedor del certificado, un número de serie, una fecha de vencimiento y la clave pública del tenedor del certificado. Esta información es verificada por la firma digital (véase la sección 2,9,3) de la CA que emitió el certificado.

Los certificados Digitales en sí mismos no proporcionan autentificación, pues es una cuestión trivial para un atacante obtener el certificado digital de un tercero y pasarlo como el suyo propio. Sin embargo, esta posibilidad no representa una amenaza práctica de seguridad; incluso si un certificado robado se acepta equivocadamente, la secuencia de datos será encriptada con la clave pública almacenada en el certificado. El atacante no tiene ningún medio de descifrar este tráfico una vez recibido, pues él no posee la llave privada correspondiente.

Los certificados Digital se pueden emplear para autenticar puntos finales de IPSec, donde los dos puntos finales que desean negociar un túnel seguro se identifican a través del intercambio de certificados digitales.

### *C.3.5.3. Firmas Digitales*

Una firma digital actúa como una huella digital electrónica; no puede ser imitada por terceros, pues se genera usando la clave privada de la entidad que identifica. Como tal, puede autenticar confiablemente el remitente, pues se asume que solamente el remitente verdadero posee la clave privada dada. Puede también ser utilizada para verificar que el mensaje o el documento que ha sido transmitido no ha sido alterado mientras estab en tránsito.

## *C.3.5. CREACIÓN DE TUNELES (TUNNELLING)*

Una comunicación segura a través de una red con un backbone no confiable es esencial para la operación exitosa de una VPN. Para lograr esta comunicación segura se utiliza una técnica de “creación de túneles” (tunnelling) en la cual los túneles seguros transportan tráfico VPN encriptado a través del backbone. El contenido de los paquetes que son transportados entre los sitios de la VPN no puede ser vistos por terceros.

La técnica de “creación de túneles” (tunnelling) en sí misma no proporciona seguridad, pero puede ofrecer la encapsulación de modo que la red objetivo pueda utilizar su propia estructura de direccionamiento. Para garantizar la seguridad para una VPN usando creación de túneles, es necesario desarrollar filtros de ingreso para prevenir paquetes externos con el formato de GRE de ser inyectados en la VPN.

### *C.3.5.1. Técnicas de Creación de Túneles*

Dos tipos principales de técnicas de “creación de túneles” (tunnelling) empleadas por las VPNs son:

- *Tunnelling Extremo a Extremo*, también conocidos como tunnelling “modelo de transporte”. Los dispositivos VPN en cada extremo de la conexión son responsables de la creación del túnel y de la encripción de los datos transferidos entre los dos sitios, así que el túnel puede extenderse a través de dispositivos de borde, tales como cortafuegos, hasta las computadoras que envían y que reciben el tráfico. El protocolo SSL/TLS es un ejemplo de un protocolo que emplea "creación de túneles" extremo a extremo. El alcance de un túnel extremo a extremo se muestra en la *Fig. C.2.*

  Esta solución es extremadamente segura, porque los datos nunca aparecen en la red en forma de texto transparente. Sin embargo, la ejecución de la encripción en el host extremo aumenta la complejidad del proceso de hacer cumplir las políticas de seguridad; los gateways de la red, que serían normalmente responsables de hacer cumplir las políticas de seguridad, se utilizan solamente para el envío (forwarding) de los paquetes a su destino en este escenario, y como tal ellos no poseen ningún conocimiento del contenido o del propósito del tráfico. Esto es particularmente problemático para los programas de filtrado instalados en el gateway.

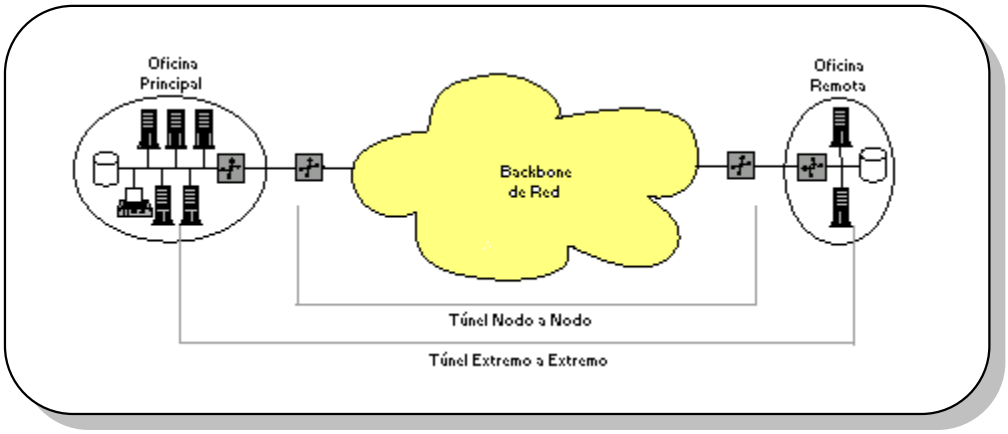



*Fig. C.2. Técnicas de “creación de túneles”.*

- *Tunnelling Nodo a Nodo.* Como se muestra en la figura 2,1, la creación y terminación de un túnel de nodo-a-nodo ocurre en los dispositivos gateway que abarcan el borde de las redes satélites, que son típicamente cortafuegos. Bajo este modelo, el transporte dentro de las LANs permanece sin cambio, pues se asume que el tráfico interno es inaccesible fuera de la LAN. Una vez que el tráfico alcance al gateway, es encriptado y enviado vía un túnel establecido dinámicamente al dispositivo equivalente en la LAN de recepción, donde los datos se descifran para recuperar su formato original, y se transmiten sobre la LAN al recipiente previsto.

Esto tiene una ventaja adicional de seguridad, en que un atacante operando un analizador de red en un cierto punto en la red entre los dos servidores del túnel vería los paquetes IP con la direcciones de fuente y destino que corresponden a esos dos servidores - la fuente y el destino verdaderas se ocultan en la carga útil encriptada de estos paquetes. Puesto que se oculta esta información, el atacante no tendría ninguna indicación en cuanto a cual tráfico se está dirigiendo hacia o desde una máquina particular, y así que no sabría qué tráfico vale la pena descifrar.

Esto también elimina la necesidad de la Conversión de Dirección de Red (NAT) para convertir las direcciones entre espacios públicos y privados, y mover la responsabilidad de realizar la encripción a un servidor central, así que el trabajo intensivo de encripción no necesita ser realizado por las estaciones de trabajo. Esto es especialmente importante al usar encripción costosa tal como 3-DES, que requiere soporte de hardware de encripción para funcionar sin limitar el ancho de banda efectivo.

Hay dos desventajas principales asociadas con la creación de túneles de nodo-a-nodo:

1. Es*calabilidad pobre.* El número de túneles requeridos para una VPN se incrementa geométricamente a medida que el número de nodos VPN aumenta, lo que tiene serias implicaciones en el rendimiento para VPNs grandes.

2. *Enrutamiento sub-optimo.* Puesto que los túneles representan solamente los puntos finales y no el camino tomado para alcanzar el otro extremo del túnel, los caminos tomados a través de la red compartida pueden no ser óptimos, creando problemas de rendimiento.

### *C.3.5.2. Requerimientos para Protocolos de Creación de Túneles*

Se presenta un número de características deseables para los mecanismos de creación de túneles. Algunas de estas características son:

- *Multiplexación.* En los casos donde múltiples túneles VPN son requeridos entre los puntos finales comunes, es deseable que un túnel común sea compartido para reducir el estado de latencia y la carga de procesamiento asociada al establecimiento del túnel. Se requiere por lo tanto que exista un campo de multiplexación de modo que los paquetes que pertenecen a diversos túneles puedan ser distinguidos.

- *Protocolo de Señalización.* El establecimiento del túnel puede ser logrado en una de dos maneras: vía una operación de administración, o vía un protocolo de señalización que soporta el establecimiento dinámico de túneles. El uso de un protocolo de señalización es esencial para muchos escenarios de desarrollo, puesto que la otra alternativa puede imponer una carga excesiva de administración. Un protocolo de señalización también simplificaría grandemente el proceso de configuración requerido si una VPN atravieza múltiples dominios administrativos.

- *Seguridad de datos.* Un protocolo de creación de túneles VPN debe proporcionar soporte para los diferentes requerimientos de seguridad, incluyendo la encripción y la autentificación. Si los túneles se establecen dinámicamente, generalmente es necesario autenticar a la parte que solicita que el túnel sea creado.

- *Transporte multi-protocolo.* Muchas VPNs transmitirán tráfico multi-protocolo entre los sitios, por lo que el protocolo de creación de túneles que facilita el transporte de este tráfico debe ser capaz de realizar transporte multi-protocolo.

- *Secuenciamiento de tramas.* La capacidad para ordenar los paquetes en un flujo de datos puede ser requerida para soportar la operación eficiente de protocolos o aplicaciones VPN particulares. Tal proceso requiere que el mecanismo de creación de túneles soporte un campo de secuenciamiento.

- *Mantenimiento del túnel.* Es necesario que los puntos extremos del túnel VPN supervisen los túneles establecidos previamente para asegurarse de que la conectividad no se ha perdido. Esto puede ser logrado periódicamente realizando comprobación en banda (in-band), o con el uso de algún mecanismo fuera de banda (out-of-band) para detectar la pérdida de conectividad.

- *Flujo y control de la congestión.* Estas características son necesarias para proporcionar un rendimiento aceptable sobre las redes donde ocurren niveles substanciales de pérdida de paquetes.

- *QoS / administración del tráfico.* Los clientes VPN pueden requerir un comportamiento específico de la red, tal como tasas de pérdidas, ancho de banda o latencia garantizadas. El desarrollo de tales garantías será generalmente responsabilidad de los nodos VPN y de las redes de backbone.

### *C.3.5.3. Protocolos de Creación de Túneles*

Existen varios protocolos de creación de túneles VPN, los cuales son usados para transportar paquetes a través de una red IP, con el método de transporte independiente del direccionamiento de los paquetes encapsulados. Estos protocolos son:

| | | |
|---|---|---|
| • L2F (CISCO) | Layer 2 Forwarding | (RFC 2341) |
| • L2TP | Layer 2 Tunneling Protocol | (RFC 2661) |
| • PPTP | Point-to-Point Tunneling Protocol | (RFC 2637) |
| • GRE | Generic Routing Encapsulation | (RFC 1701) |
| • IP/IP | IP over IP | (RFC 2003) |
| • IPsec | IP Security | (RFC 2475) |

Los protocolos más utilizados actualmente son: PPTP, L2TP y IPSec. Estos protocolos fueron explicados brevemente en el trabajo de grado. IPSec se considera el protocolo más completo para la implementación de VPNs ya que fue diseñado y desarrollado con todas las capacidades de seguridad necesarias para la transmisión de datos sobre redes públicas. (Ver Sección C.4)

Adicionalmente es muy importante mencionar una nueva tecnología que está surgiendo, conocida como MPLS (Multiprotocol Label Switching), cuyo objetivo principal es crear redes flexibles y escalables, brindando grandes beneficios a las redes basadas en IP, entre los cuales se destacan la Ingeniería de Tráfico, la diferenciación de servicios en diferentes clases (CoS) y el establecimiento de redes privadas virtuales (VPNs) sobre una topología "inteligente" muy superior en prestaciones a las soluciones tradicionales de túneles y de circuitos virtuales. (Ver Sección C.5)

Mientras IPSec se concentra en proteger el nivel de red (nivel 3) diseñando mecanismos criptográficos de seguridad que puedan soportar combinaciones de autenticación, integridad, control de acceso y confidencialidad, MPLS se enfoca en integrar las funcionalidades del nivel de red (nivel 3) y del nivel de enlace (nivel 2), desplazando la problemática de la creación de túneles del equipo del cliente a la red del proveedor de servicio, además de proveer otras funcionalidades adicionales.

En la *Tabla C.1.* se presentan las características que cumplen cada uno de los principales protocolos para la creación de túneles. En la tabla se puede observar, que ningún protocolo proporciona actualmente todas las facilidades requeridas.

| **Característica** | **Protocolos de Creación de Túneles** | | | |
|---|---|---|---|---|
| | L2TP | PPTP | IPSec | MPLS |
| Multiplexación | ✓ | ≈ | ✓ | × |
| Señalización | ✓ | ✓ | ✓ | ≈ |
| Seguridad de Datos | × | × | ✓ | ≈ |
| Transporte Multi-protocolo | ✓ | ✓ | ≈ | ✓ |
| Secuenciamiento de Trama | ✓ | ✓ | ≈ | × |
| Mantenimiento de Túnel | ✓ | ≈ | ≈ | ≈ |
| QoS / Administración de Tráfico | × | × | × | ✓ |

✓ Soportado × No soportado ≈ Soportado a través de extensiones

*Tabla C.1. Capacidades de los protocolos de creación de túneles.*

## C.4. PROTOCOLO IPSEC

IPSec es un grupo de protocolos de nivel de red, el cual provee seguridad criptográfica tanto para redes IPv4 como para redes IPv6. IPSec proporciona un conjunto de servicios de seguridad incluyendo control de acceso, integridad no orientada a la conexión, autenticación de origen de datos, rechazo o reenvío de paquetes, confidencialidad y negociación de compresión IP.

IPSec provee seguridad a nivel de red y requiere que solo dos puntos extremos soporten el estándar IPSec. Todos los demás dispositivos de red entre los puntos extremos solo retransmiten el tráfico como paquetes IP. IPSec puede ser empleado para proteger uno o más caminos entre:

- Pares de Host.
- Host y Gateway de seguridad.
- Pares de Gateway de seguridad.

Las características de seguridad de IPSec son proporcionadas a través de dos nuevos protocolos de seguridad: “Encabezado de Autenticación” (AH, "Authentication Header") y “Carga Útil de Seguridad Encapsulada” (ESP, "Encapsulating Security Payload") y un protocolo de administración de claves: “Intercambio de Claves Internet” (IKE, “Internet Key Exchange”).

### *C.4.1. PROTOCOLOS DE SEGURIDAD*

#### *C.4.1.1. Carga Util de Seguridad Encapsulada (ESP)*

ESP puede 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 (éstas dos van siempre juntas). La confidencialidad (encripción) se puede usar con o sin autenticación y/o integridad. Del mismo modo, puede usar la autenticación y/o la integridad con o sin la confidencialidad.

ESP maneja encripción de IP al nivel de paquete utilizando encripción simétrica de claves. ESP está diseñado para usar cualquier número de algoritmos de encripción, el más común de los cuales es DES (Encripción Estándar de Datos). ESP está diseñado para cambiar con el Internet en el tiempo, así el desarrollo de estándares de Internet continuará siendo soportado por ESP.

En la *Fig. C.3.*, se puede observar lo siguiente:

- El encabezado ESP es insertado entre el encabezado IP y el resto del paquete.
- Los campos SPI y Número de Secuencia proveen las mismas funciones que en AH.
- La porción “TCP”, “Data”, y “ESP Trailer” son todos encriptados.
- ESP provee autenticación de la misma manera que AH lo hace.

La cabecera ESP no considera los campos de la cabecera IP que van delante, y por lo tanto no garantiza nada excepto la Carga útil. Los distintos tipos de ESP aplicables deben seguir conformidad con el RFC 2406.

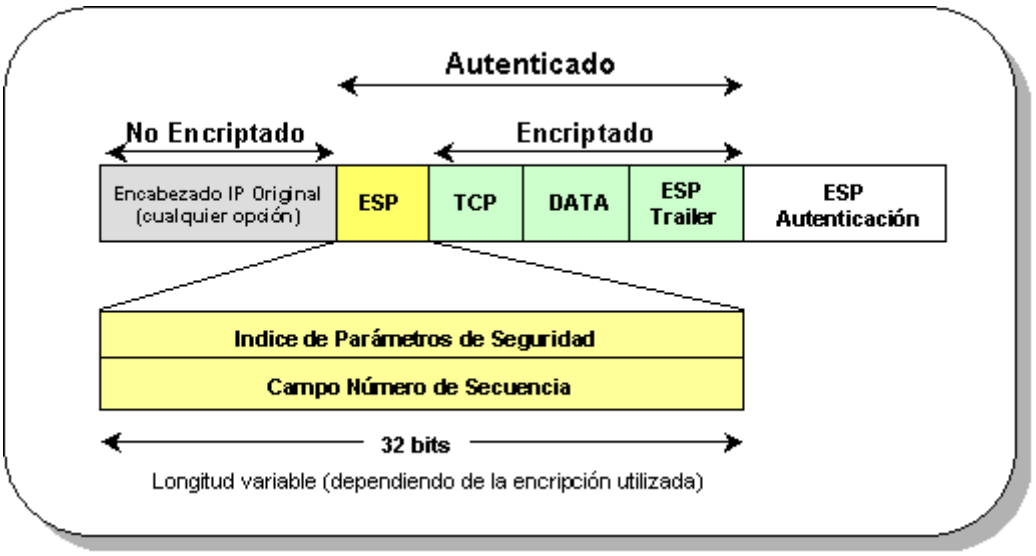



*Fig. C.3. Paquete ESP de IPSec.*

### *C.4.1.2. Encabezado de Autenticación (AH)*

AH provee autenticación, integridad, y protección a la réplica (pero no confidencialidad). Su principal diferencia con ESP es que AH provee autenticación para partes de la cabecera IP del paquete (como las direcciones de origen o destino), así como para datos de protocolos de nivel superior. Sin embargo, algunos campos del encabezado IP pueden cambiar en el camino y así el valor de estos campos una vez recibidos puede no ser predecible para el remitente. Por consiguiente, estos campos no permiten la protección AH.

AH no encripta la porción de datos del paquete. En la *Fig. C.4.* el campo SPI (Indice de Parámetros de Seguridad) es un número de 32 bits que indica cuales protocolos de seguridad están siendo utilizados. Los algoritmos y claves son incluidos en este campo. El Número de Secuencia indica cuantos paquetes han sido enviados y provee protección anti réplicas.

AH puede ser aplicado solo, en combinación con ESP, o anidado en el modo túnel de IPSec (ver sección C.4.2.). ESP puede ser utilizado para proveer los mismos servicios de seguridad, la diferencia primaria esta en el grado de cobertura, ESP no protege ningún campo del encabezado IP a menos que estos campos sean encapsulados por ESP en el modo túnel.

Hay varios RFCs diferentes que ofrecen una elección de algoritmos para AH, sin embargo todos deben seguir los lineamientos especificados en el RFC 2402.

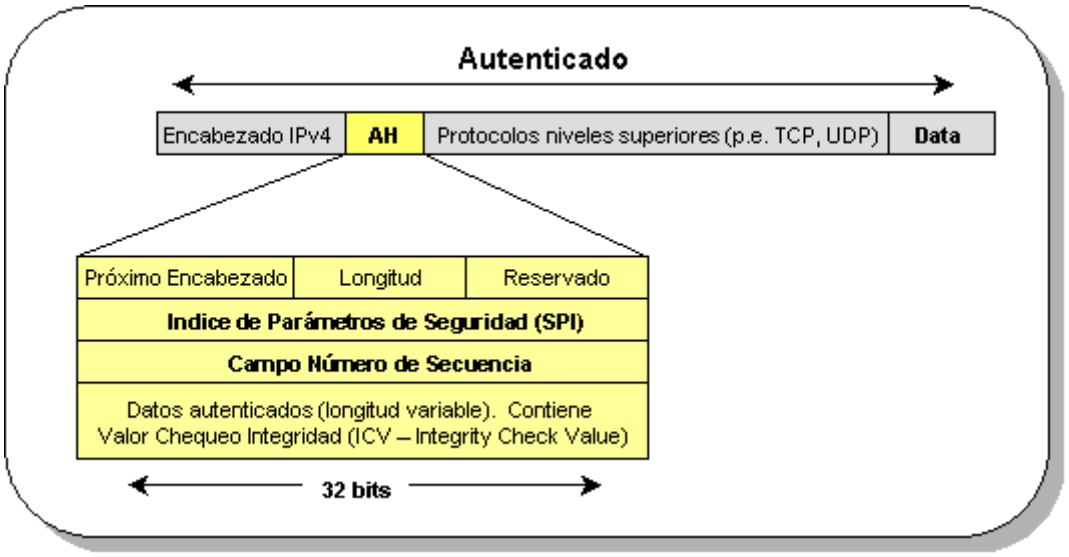



*Fig. C.4. Paquete AH de IPSec.*

### *C.4.2. ASOCIACIONES DE SEGURIDAD IPSEC*

Los enlaces seguros de IPSec se definen en términos de "Asociaciones de Seguridad" (**SA** – Security Association). Una SA es un acuerdo entre dos partes sobre el método que ellas emplearán para soportar comunicaciones seguras. Este acuerdo se logra después de una etapa de negociación que discierne las características comunes soportadas por las implementaciones potencialmente diferentes en cada extremo.

Los servicios de seguridad son ofrecidos a una SA IPSec a través del uso de AH o ESP, pero no de ambos. Por lo tanto, si las dos protecciones AH y ESP son aplicadas a una corriente de tráfico, entonces dos o más SAs deben ser creadas para permitir la protección deseada. Las SAs son unidireccionales, por lo tanto en una comunicación bidireccional entre dos host o gateways de seguridad, se requieren dos SAs, una en cada dirección.

Hay dos tipos de Asociaciones de Seguridad definidas por IPSec: modo transporte y modo túnel. Un host debe soportar ambos modos, un gateway de seguridad sólo debe soportar modo túnel.

El modo **Transporte**: Una SA modo transporte es un acuerdo entre dos hosts. El modo transporte solamente encripta hasta la carga útil del paquete IP. En el caso de ESP, un SA modo trasporte provee servicios de seguridad sólo para protocolos de nivel superior, no para el encabezado IP o para encabezados de extensiones que precedan al encabezado ESP. En el caso de AH, la protección también se extiende a porciones específicas de cualquier encabezado IP y cualquier encabezado de extensiones. (Ver Fig.C.5.)

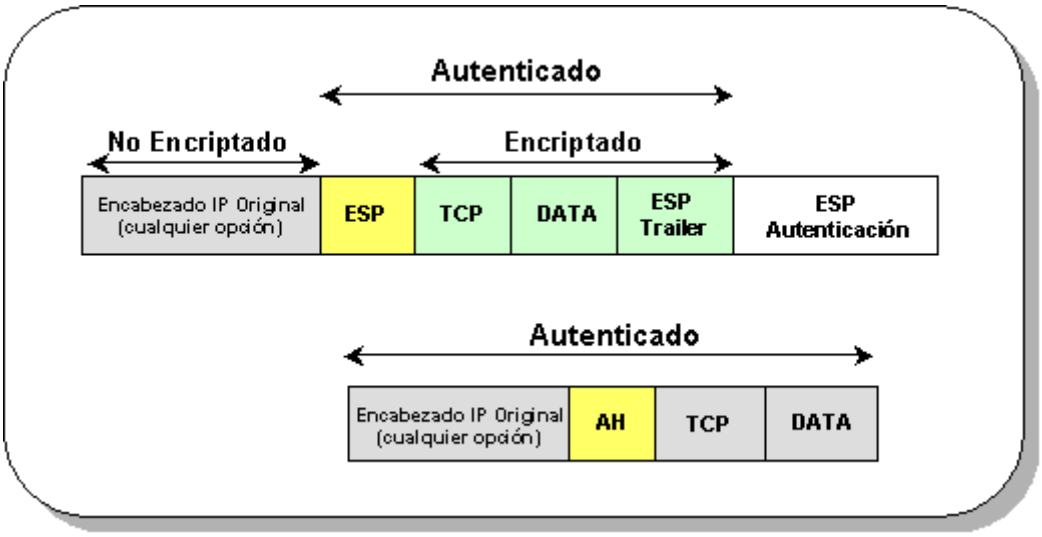



*Fig. C.5. Modo transporte de los paquetes ESP y AH de IPSec.*

El modo **Túnel**. Una SA modo túnel es esencialmente una asociación de seguridad modo transporte que es aplicada a un túnel IP. Este modo es requerido siempre que una asociación de seguridad termine en un gateway de seguridad para evitar la fragmentación y nuevo ensamble de los paquetes IPSec, y en situaciones donde existen múltiples caminos al mismo destino, detrás de gateways de seguridad. Dos hosts pueden establecer opcionalmente una SA modo túnel si se requiere una seguridad creciente. (Ver Fig. C.6.)

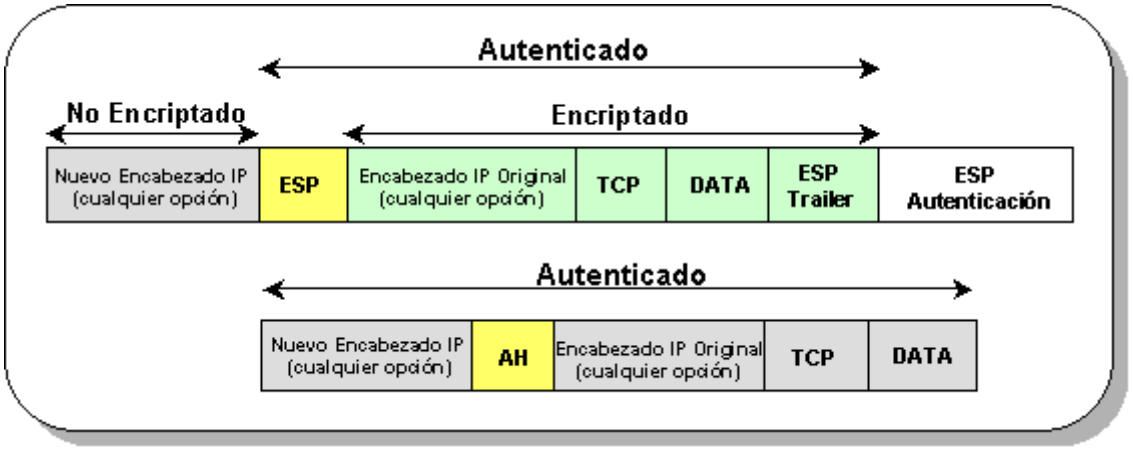



*Fig. C.6. Modo túnel de los paquetes ESP y AH de IPSec.*

En modo túnel el paquete IP entero es encriptado y no sólo la parte de datos como en el modo transporte. Después de que los campos AH y ESP son incluidos con el paquete IP, el nuevo paquete es tratado como la carga útil de un nuevo paquete de salida IP, con un nuevo encabezado. Ya que el modo túnel no modifica el contenido del paquete original, puede ser implementado utilizando hardware o software localizado en un punto intermedio

entre el sistema fuente y el sistema destino. Esto significa que tanto el sistema final como un sistema intermedio pueden implementar el modo túnel.

Los paquetes en el modo túnel cuentan con dos encabezados IP, uno externo que especifica los datos para llegar al destino del túnel, y otro interno que especifica el destino final para el paquete.

Si AH es empleado en modo túnel, porciones del encabezado IP exterior son protegidas, así como todo el paquete IP encapsulado. Si se emplea ESP, la protección es permitida solo al paquete entunelado, no al encabezado exterior.

### *C.4.3. PROTOCOLO DE ADMINISTRACION DE CLAVES (IKE)*

El protocolo IKE (Internet Key Exchange) es un sofisticado sistema de administración e intercambio de claves, que está incluido en el conjunto de protocolos IPSec para proporcionar servicios de distribución segura de claves entre socios que desean comunicarse sobre una red no muy confiable.

IKE es un protocolo híbrido compuesto de características de los protocolos: ISAKMP (Internet Security Association and Key Management Protocol). Oakley y SKEME (Secure key Exchange Mechanism)

IKE es un protocolo basado en UDP para negociar Asociaciones de Seguridad y proveer intercambio autenticado de claves para sus clientes. IKE crea un túnel seguro y autenticado, entre dos entidades (IKE SA) y entonces negocia las asociaciones de seguridad para IPSec.

Hay tres modos de operación para IKE:

- Modo Principal. Utilizado cuando dos entidades hablan por primera vez y tienen que negociar una SA con el fin de hablar de manera segura.
- Modo Agresivo. Es una versión abreviada del modo principal, con las mismas funciones.
- Modo Rápido. Es utilizado cuando el modo principal o el modo agresivo ya han establecido una SA, pero servicios de seguridad necesitan ser negociados o hay la necesidad por nuevo material de claves. Debido a que un canal seguro ya está establecido antes de utilizar el modo rápido, este modo es seguro sin todo el encabezado utilizado por los modos principal y modo agresivo.

Hay varios métodos de autenticación de IKE. Con claves precompartidas, cada host (o gateway de seguridad) está en posesión del mismo secreto precompartido. IKE autentica las diversas entidades usando un hash de la llave. La otra entidad entonces descifra el hash para ver si las llaves coinciden.

En criptografía de claves públicas, cada entidad genera un número aleatorio y lo encripta en la clave pública de la otra parte. La autentificación ocurre cuando la otra entidad

puede computar y enviar un hash de este número aleatorio de regreso a la primera entidad.

Con firmas digitales, cada dispositivo firma digitalmente un sistema de datos y lo envía a la otra parte. Este método es similar a la criptografía de claves públicas pero adiciona no repudiación.

Tanto las firmas digitales como la criptografía de claves públicas requieren el uso de certificados digitales para validar el mapeo de claves públicas / privadas. IKE permite al certificado ser alcanzado independientemente o haciendo que los dos dispositivos intercambien los certificados explícitamente como parte de IKE.

## C.5. MPLS – MULTIPROTOCOL LABEL SWITCHING

La convergencia hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución de superponer IP sobre ATM, llevaron a que a finales de los 90s (1997-98) varios fabricantes desarrollaran técnicas para realizar la integración de los niveles 2 (conmutación) y 3 (enrutamiento) de forma efectiva. Dichas técnicas se conocieron como "conmutación IP" (IP switching) o "conmutación multinivel" (multilayer switching).

Las principales tecnologías privadas de conmutación multinivel implementadas fueron:

- IP Switching de Ipsilon Networks
- Tag Switching de Cisco
- Aggregate Route-Base IP Switching (ARIS) de IBM
- IP Navigator de Cascade/Ascend/Lucent
- Cell Switching Router (CSR) de Toshiba

El problema que presentaban tales soluciones era la falta de interoperatividad entre los productos privados de los diferentes fabricantes, ya que usaban diferentes tecnologías para combinar la conmutación de nivel 2 con el enrutamiento IP de nivel 3. Además de esto, la mayoría de esas soluciones necesitaban ATM como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas (Frame Relay, PPP, SONET/SDH y LANs).

Por lo anterior, el IETF estableció en 1997 un grupo de trabajo cuyo objetivo era la definición de un estándar unificado e interoperativo, que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de enlace. De este grupo de trabajo surgió el actual estándar MPLS del IETF.

MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel (o conmutación IP). La idea básica es separar el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de enrutamiento estándar IP, logrando un acercamiento de los niveles 2 y 3 y grandes beneficios en cuanto a rendimiento y flexibilidad de esta arquitectura.

MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP (típicamente limitadas a encaminar por dirección de destino). Además de poder hacer ingeniería de tráfico IP, MPLS permite mantener clases de servicio y soporta con gran eficacia la creación de VPNs. Por todo ello, MPLS se presenta como la gran promesa y esperanza para poder mantener el ritmo actual de crecimiento de Internet.

### *C.5.1. DESCRIPCIÓN FUNCIONAL DE MPLS*

La arquitectura de MPLS (al igual que todas las soluciones de conmutación multinivel) esta basada en los siguientes conceptos:

- La separación entre los componentes funcionales de envío (forwarding) y de control (routing).
- El intercambio de etiquetas para el envío de datos

En la *Fig. C.7.* se representa la separación funcional de esos dos componentes, uno de control y otro de envío.

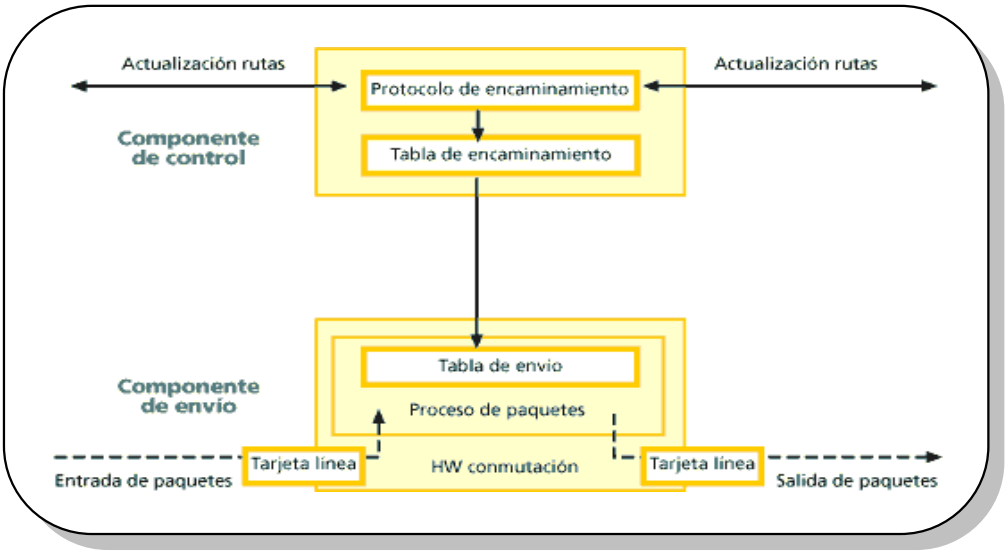



*Fig. C.7. Separación funcional de enrutamiento y envío.*

El componente de control utiliza los protocolos estándar de enrutamiento para el intercambio de información con los otros enrutadores, para la construcción y el mantenimiento de las tablas de enrutamiento.

El mecanismo de envío asigna una etiqueta corta de longitud fija a cada paquete indicando a los nodos de conmutación a lo largo de la trayectoria del paquete como procesar y enviar los datos.

Cada paquete es analizado en una base salto por salto. Así, al llegar los paquetes a un salto, el componente de envío examina la información de la cabecera del paquete, busca en la tabla de etiquetas de envío (mantenida por el componente de control) la entrada correspondiente, toma la decisión de enrutamiento y dirige el paquete desde la interfaz de entrada a la de salida a través del correspondiente hardware de conmutación.

Al separar el componente de control (enrutamiento) del componente de envío, cada uno de ellos se puede implementar y modificar independientemente. El único requisito es que el componente de enrutamiento mantenga la comunicación con el de envío mediante la tabla de envío de paquetes y actualice la información.

El mecanismo de envío se implementa mediante el intercambio de etiquetas, por lo tanto lo que se envía por la interfaz física de salida son paquetes "etiquetados".

La etiqueta que marca cada paquete, es un campo de unos pocos bits, de longitud fija, que se añade a la cabecera del mismo y que identifica una "clase equivalente de envío" (Forwarding Equivalence Class, FEC). Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes. Realmente, una etiqueta es similar a un identificador de conexión (como el VPI/VCI de ATM o el DLCI de Frame Relay). Tiene solamente significado local y, por consiguiente, no modifica la información de la cabecera de los paquetes; tan sólo los encapsula, asignando el tráfico a los correspondientes FEC.

El algoritmo de intercambio de etiquetas permite la creación de Caminos Conmutados de Etiquetas (LSP – Label-Switched Paths), funcionalmente equivalentes a los PVCs de ATM y Frame Relay.

Los LSPs se establecen para un solo sentido del tráfico en cada punto de entrada a la red (simplex); el tráfico dúplex requiere dos LSPs, uno en cada sentido. Un LSP es orientado a conexión porque el camino es creado sin importar si algún tráfico es requerido para fluir a lo largo del camino.

Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un “conmutador de etiquetas” (LSR – Label-Switching Router) a otro, a través del dominio MPLS. Un LSR puede ser cualquier enrutador o conmutador que implementa los procedimientos de distribución de etiquetas y puede enviar paquetes basados en las etiquetas.

En la *Fig. C.8.* se puede ver la funcionalidad del MPLS. Los protocolos de señalización y enrutamiento para la distribución de etiquetas entre los nodos son diferentes a los definidos para ATM. MPLS utiliza el protocolo RSVP o un nuevo estándar de señalización definido por el IETF conocido como “Protocolo de Distribución de Etiquetas” (LDP – Label Distribution Protocol).

Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. Los LSRs intermedios se conocen como LSRs interiores del dominio MPLS.

Cada entrada de la tabla de envío contiene un par de etiquetas entrada / salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta.

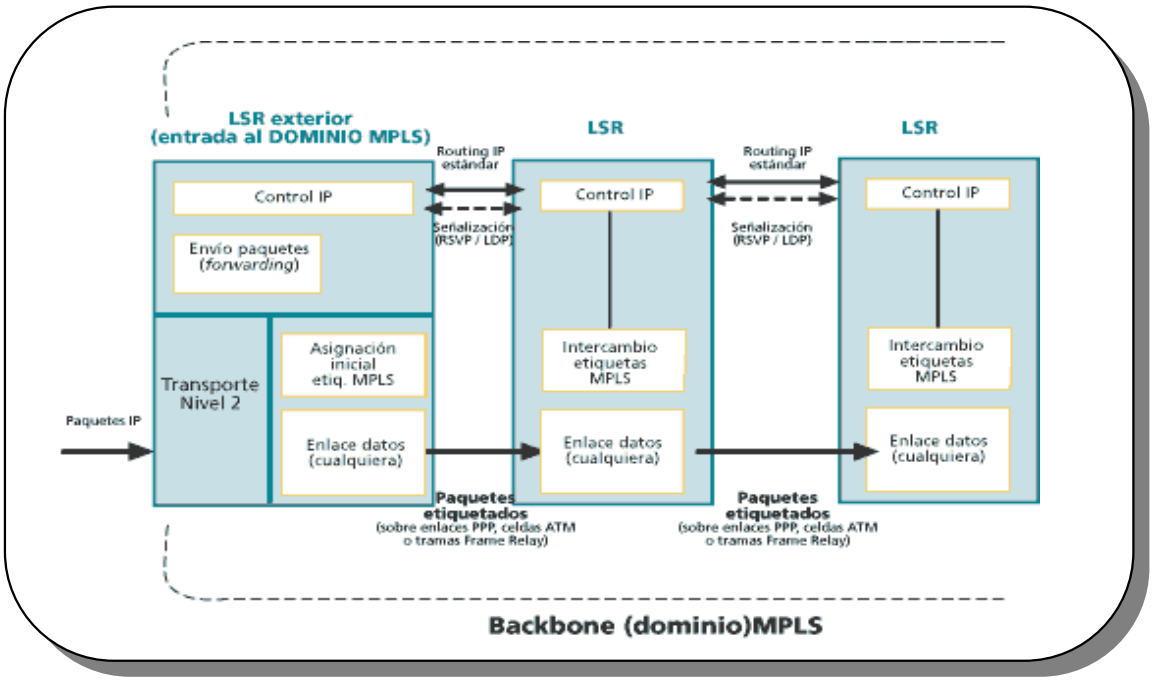



*Fig. C.8. Esquema funcional de MPLS.*

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la siguiente figura el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de enrutamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP. (Ver *Fig. C.9*.)

Dentro del dominio MPLS los LSR ignoran el encabezado IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas la quita y envía el paquete utilizando enrutamiento convencional.

MPLS fue creado para funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Si el protocolo de transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay) se

utilizan esos campos nativos para las etiquetas. Si la tecnología de nivel 2 utilizada no soporta un campo para etiquetas (p.e. enlaces PPP y LAN), se emplea una cabecera genérica MPLS de 4 octetos,que contiene un campo específico para la etiqueta y que se inserta entre la cabecera de nivel 2 y la del paquete de nivel 3.

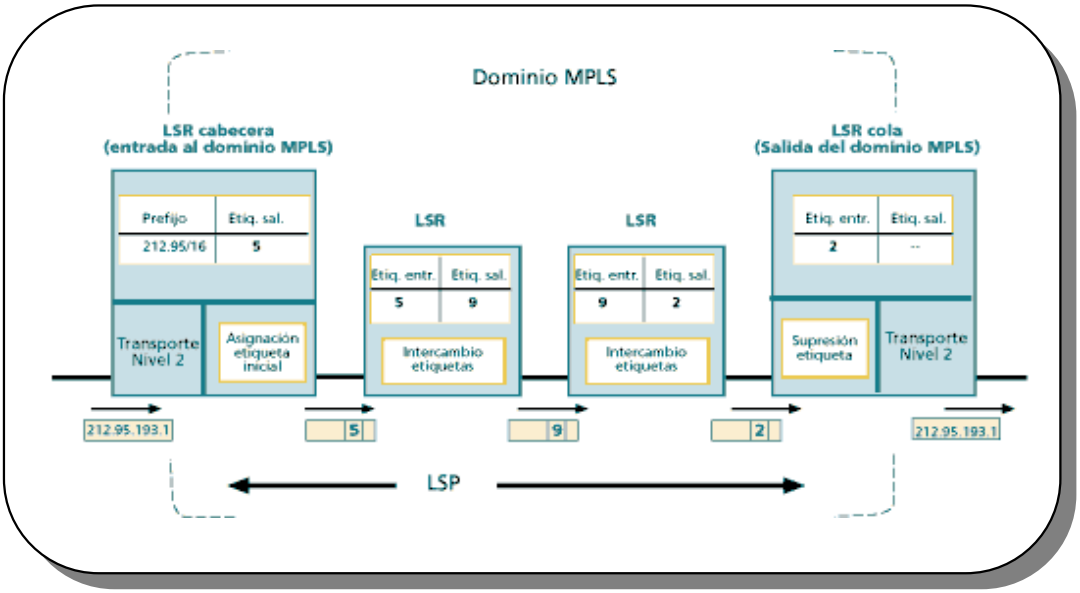



*Fig. C.9. Ejemplo de envío de un paquete por un LSP.*

En la *Fig. C.10* se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS), 1 bit de stack para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

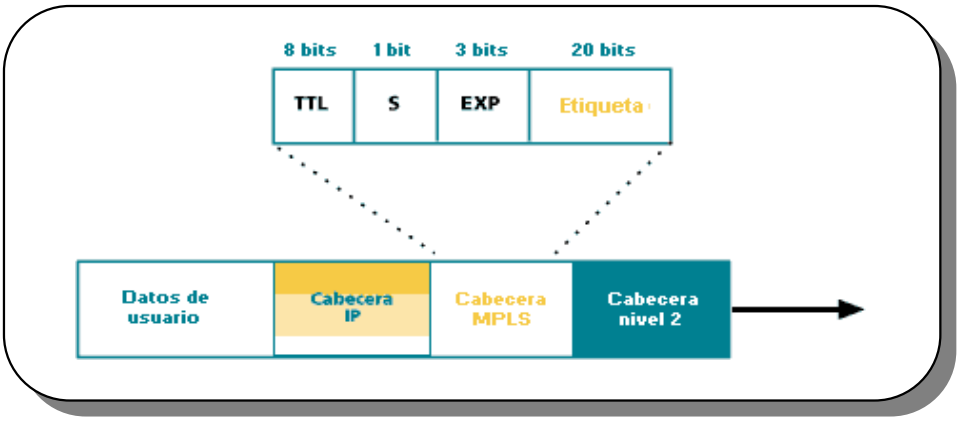



*Fig. C.10. Cabecera genérica MPLS*

### *C.5.2. FUNCIONAMIENTO GLOBAL MPLS*

El esquema global de funcionamiento de MPLS se presenta en la *Fig. C.11*. En la figura se pueden observar las diversas funciones realizadas en cada uno de los elementos que integran la red MPLS.

En el borde de la nube MPLS se tiene una red convencional de enrutadores IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de enrutadores a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología enmallada (directamente o por PVCs ATM). La unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de enrutadores).

La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Esto permite mejorar el rendimiento de las redes y soportar nuevas aplicaciones de usuario, tal como el servicio de Redes Privadas Virtuales.

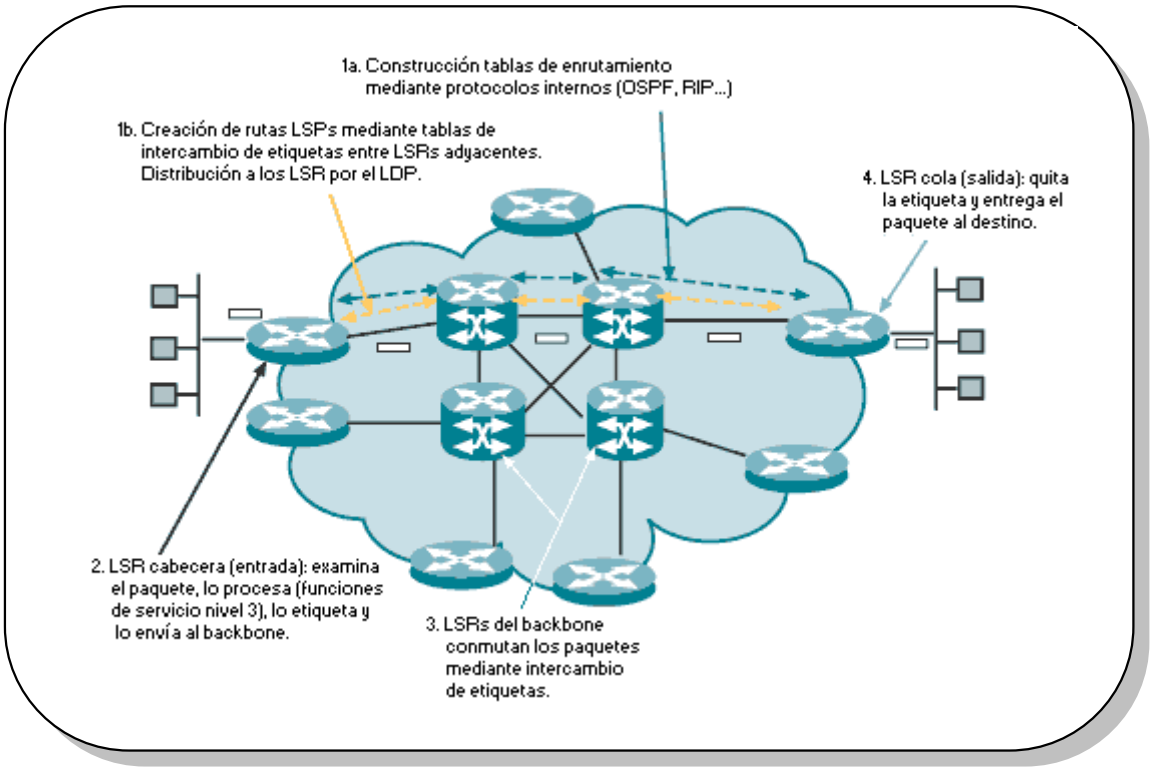



*Fig. C.11. Funcionamiento global MPLS.*

### *C.5.2. REDES PRIVADAS VIRTUALES MPLS*

La ventaja principal de las redes VPN MPLS es que son sin conexión. Las soluciones actuales de VPN requieren un enlace orientado a conexión punto a punto en la red. Creando una VPN sin conexión, no se necesitan túneles ni encripción para la privacidad de la red, eliminando así una significativa complejidad. La escalabilidad es crítica, porque los clientes quieren utilizar servicios privados en sus intranets y extranets.

Las VPNs basadas en MPLS utilizan la arquitectura sin conexión de nivel 3 y el modelo de conexión de pares (peer model) para apalancar una solución VPN altamente escalable. El modelo de pares requiere que un sitio de cliente tenga solamente un par con una ruta del extremo del proveedor en comparación con todos los otros CPEs o rutas del extremo del cliente que son miembros de la VPN.

La arquitectura sin conexión permite la creación de VPNs en el nivel 3, eliminando la necesidad de túneles. Ya que las VPNs MPLS son sin conexión, no se requieren topologías o mapas de conexiones punto a punto específicas. Se pueden adicionar sitios a las intranets y extranets fácilmente y formar grupos de usuario cerrados. Las VPNs MPLS VPNs pueden ser construidas sobre múltiples arquitecturas de redes, incluyendo IP, ATM, Frame Relay y redes híbridas.

### *C.5.3. BENEFICIOS DE LAS REDES VPN MPLS*

Las VPNs MPLS, las cuales son creadas en el nivel 3, son sin conexión, y por consiguiente más escalables y fáciles para construir y administrar que las VPNs convencionales. Adicionalmente, se pueden adicionar servicios, tales como hosting de datos y aplicaciones, comercio de red, y servicios de telefonía para VPN MPLS.

- Rápido desarrollo de servicios IP de valor agregado adicionales.
- Privacidad y seguridad iguales a las VPNs de nivel 2.
- Integración transparente con intranets de los clientes.
- Clase de Servicio IP.

## C.6. COMPARACIÓN VPNs IP vs. VPNs MPLS

Las VPNs IP están basadas en un modelo topológico superpuesto sobre la topología física existente, a partir de túneles extremo a extremo (o circuitos virtuales) entre cada par de enrutadores de cliente en cada VPN. Debido a esto se presentan desventajas tales como poca flexibilidad en la provisión y gestión del servicio, problemas de crecimiento al añadir nuevos túneles y la gestión de QoS es posible en cierta medida pero no se puede mantener extremo a extremo a lo largo de la red ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre las distintas locaciones de una VPN, se utilizan conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS.

Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo.

En los túneles se utiliza el enrutamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de enrutamiento IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas de Calidad de Servicio (QoS) basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer Clases de Servicio (CoS) y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

En la *Fig. C.12.* se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean dentro de la red, a base de LSPs, y no de extremo a extremo a través de la red.

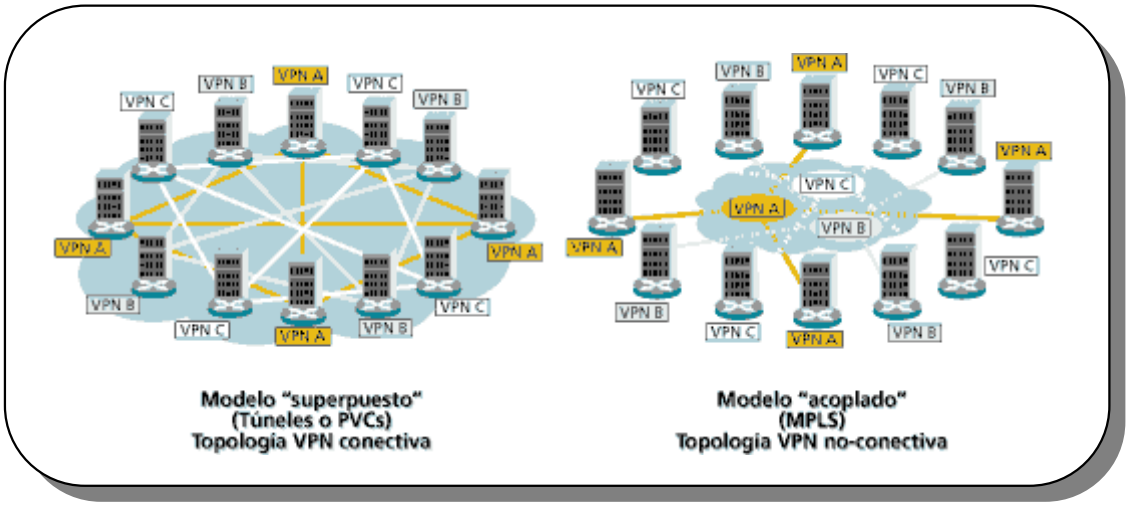



*Fig. C.12. Modelo superpuesto (túneles/PVCs) vs. Modelo acoplado (MPLS).*

Como resumen, las ventajas que MPLS ofrece para IP VPNs son:

- Proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs)
- Evita la complejidad de los túneles y PVCs
- La provisión de servicio es sencilla: una nueva conexión afecta a un solo enrutador.
- Tiene mayores opciones de crecimiento modular.
- Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.
- Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación...), lo que es necesario para un servicio completo VPN.

# ANEXO D - EJEMPLOS VPN

En el presente anexo se exponen las soluciones de Redes Privadas Virtuales sobre Redes Inteligentes implementadas por algunos de los operadores de telecomunicaciones más importantes de la Latinoamérica y del mundo.

## D.1. MÉXICO – TELMEX

La siguiente información fue tomada de la página Web de Telmex: www.telmex.com.mx y de la página Web de la "Comisión Federal de Telecomunicaciones" (COFETEL) de México (http://www.cft.gob.mx/html/4_tar/telmex/indice.html) y se transcribe literalmente.

### *D.1.1. DESCRIPCIÓN DEL SERVICIO*

Le permite la creación de una red corporativa de voz entre sus instalaciones, facilitándole la comunicación, sin requerir inversión en infraestructura, proporcionándole la máxima cobertura en telecomunicaciones a la medida de sus necesidades, con la mejor relación costo-beneficio y tarifas preferenciales. A través de Lada VpNet la empresa delega la administración de sus telecomunicaciones a Telmex - Lada, reduciendo gastos de operación innecesarios.

### *D.1.2. TIPO DE LLAMADAS*

- *On Net - On Net (En Red a En Red).* Llamadas originadas en un sitio de su Red Lada VpNet y con destino en otro sitio de la misma red por medio de su plan de marcación privado.

- *On Net - Off Net (En Red a Fuera de Red).* Llamadas originadas en un sitio de su Red Lada VpNet y con destino en un sitio no perteneciente a su red por medio de la marcación pública.

- *Off Net - On Net (De Fuera de Red a En Red).* Llamadas realizadas por medio de la Tarjeta Lada VpNet con su plan de marcación privado, desde la red pública conmutada a un sitio de su Red Lada VpNet.

- *Off Net - Off Net (De Fuera de Red a Fuera de Red).* Llamadas realizadas por medio de la Tarjeta Lada VpNet con marcación pública desde la red pública conmutada a un sitio no perteneciente a su red.

### *D.1.3. BENEFICIOS*

- No requiere inversión en infraestructura, Lada VpNet le proporciona la infraestructura necesaria para su red, por lo que no incurre en gastos de instalación.
- Facilita la comunicación y expansión de sus oficinas a través de su plan de marcación privado, que le brinda comunicación fácil y rápida.
- Máxima cobertura en telecomunicaciones: nacional, internacional y mundial.
- Optimización de recursos y costos de operación; por medio de las tarifas preferenciales en larga distancia, que Lada le ofrece de acuerdo a su consumo mensual en minutos.
- Usted recibirá el detalle de sus consumos en la factura de Cuenta Maestra, así como podrá crear centros de distribución de costos de acuerdo a sus necesidades y aplicaciones administrativas, a través de la identificación de consumos mediante el uso de Siana.

### *D.1.4. ESQUEMA TARIFARIO DEL SERVICIO VPNET*

Los siguientes precios y definiciones que aparecen a continuación fueron tomados la página Web de la “Comisión Federal de Telecomunicaciones” (COFETEL) de México (http://www.cft.gob.mx/html/4_tar/telmex/SECC5.html).

**Libro tarifario de Telmex**
**Sección No. 5** Tarifas para la RED LADA VpNet (RLVPN)
(vigente a partir del 08 de junio de 2002) **(Folio 2839)**

#### *D.1.4.1. Tipos de tráfico*

| En Red - En Red (ON-ON) | En Red - Fuera de Red (ON-OFF) | Fuera de Red - En Red (OFF-ON) | Fuera de Red - Fuera de Red (OFF-OFF) |
|---|---|---|---|
| Tráfico que se genera con un Plan Privado de Marcación, desde Sitios del Cliente definidos en la Red VpNet del Cliente y que termina en Sitios del Cliente definidos en la Red VpNet del Cliente. | Tráfico que se genera desde los Sitios del Cliente definidos en la Red VpNet del Cliente y que termina en la Red Pública Telefónica, con dos modalidades: Desde sitios dedicados (On - Off dedicado) y desde Sitios Conmutados (On - Off conmutado) . | Tráfico que se genera desde la Red Pública Telefónica a través de la Tarjeta LADA VpNet del Cliente, usando el Plan Privado de Marcación, y que termina en Sitios del Cliente definido en la red VpNet del Cliente. | Tráfico que se genera desde la Red Pública Telefónica a través de la Tarjeta LADA VpNet del Cliente y que termina en Sitios de la Red Pública Telefónica. |

***D.1.4.2. Tarifas por cobertura del servicio, características adicionales, plan o paquete del servicio***

1. Costo por acceso al servicio:

   Este se aplica por evento cuando el servicio es solicitado por primera vez y se establece a nivel de la red del Cliente y se factura bajo el siguiente concepto.

   Gastos de acceso al servicio: $240,000.00

1.1. Este pago le permite al Cliente obtener las siguientes características sin costo adicional:

   a) Tráfico tomando en cuenta:
      i. Tráfico telefónico de voz interno del contratante.
      ii. Tráfico telefónico de voz externo del contratante.
   b) Plan de marcación.
   c) Servicios de operadora.
   d) Control de llamadas estándar.
   e) Anulación de control de llamadas estándar.
   f) Facturación detallada.

2. Tarifas por consumo por minuto o fracción:

   a) Tarifas Base

| Minutos mensuales | Tráfico | On - On | On - Off Dedicado | On - Off Conmutado | Off - On | Off - Off |
|---|---|---|---|---|---|---|
| Tarifas Base | Nacional | $0.90 | $1.00 | $1.00 | $ 1.57 | $1.73 |
| | Zonas Fronterizas USA. | $1.32 | $1.45 | $1.45 | $ 1.96 | $2.16 |
| | Resto USA. | $3.30 | $3.60 | $3.60 | $ 4.73 | $5.20 |

   b) Tarifas LADA VpNet

| Minutos mensuales | Tráfico | On - On | On - Off Dedicado | On - Off Conmutado | Off - On | Off - Off |
|---|---|---|---|---|---|---|
| 40,000 - 249,999 | Nacional | $0.84 | $0.92 | $1.00 | $ 1.57 | $ 1.73 |
| | Zonas Fronterizas USA. | $1.27 | $1.40 | $1.40 | $ 1.96 | $ 2.16 |
| | Resto USA. | $3.10 | $3.40 | $3.40 | $ 4.73 | $ 5.20 |
| 250,000 - Adelante | Nacional | $0.82 | $0.85 | $1.00 | $ 1.57 | $ 1.73 |
| | Zonas Fronterizas USA. | $1.23 | $1.35 | $1.35 | $ 1.96 | $ 2.16 |
| | Resto USA. | $3.00 | $3.30 | $3.30 | $ 4.73 | $ 5.20 |
| Todos los rangos y Tarifas Base | Canadá | $4.50 | $4.50 | $4.50 | $ 7.21 | $ 7.21 |
| | Centro América | $3.60 | $3.60 | $3.60 | $ 5.77 | $ 5.77 |
| | Sudamérica y Caribe | $8.00 | $8.00 | $8.00 | $12.97 | $12.97 |
| | Europa, Africa y Mediterráneo | $7.20 | $7.20 | $7.20 | $11.53 | $11.53 |
| | Resto del mundo e Israel | $9.00 | $9.00 | $9.00 | $14.42 | $14.42 |

Tarifas para el tráfico Off Net - Off Net y Off Net - On Net, (Tarjeta LADA VpNet) con origen en E.U.A. y Canadá, para cualquier rango de facturación:

| Tipos de Tráfico | Por Minuto |
|---|---|
| De E.U.A. a México | $ 5.20 |
| De E.U.A. a E.U.A. | $ 5.20 |
| De E.U.A. a Canadá | $ 5.20 |
| De Canadá a México | $ 7.25 |
| De Canadá a Canadá | $ 7.25 |
| De Canadá a E.U.A. | $ 7.25 |
| De E.U.A. y Canadá a Centro América | $21.00 |
| De E.U.A. y Canadá a Sudamérica y el Caribe | $21.00 |
| De E.U.A. y Canadá a Europa, Africa y Cuenca del Mediterráneo | $21.00 |
| De E.U.A. y Canadá a Resto del Mundo | $21.00 |

Nota: Las tarifas no contemplan el Impuesto al Valor Agregado (IVA).

3. Tarifas para características y funciones adicionales:

3.1 Rentas mensuales

| Función | Tarifa |
|---|---|
| a) Control de llamada especial y código de autorización (por línea) | $ 50.00 |
| b) Línea rápida (Hot Line) (por terminación) | $ 50.00 |
| c) Servicio Digital (Sígueme) | $ 50.00 |
| d) Ruta seleccionada en Red Virtual Nacional. | $ 50.00 |
| e) Ruta seleccionada en Red Virtual Internacional. | $180.00 |
| f) Enrutamiento por selección de Ruta Primaria | $ 50.00 |
| g) Enrutamiento Alternativo | $ 50.00 |

Nota: Ninguna de las funciones anteriores tendrá "Cargos por Instalación".
Las tarifas no contemplan el Impuesto al Valor Agregado (IVA)

### *D.1.4.3. Cobertura de Comericalización*

El Servicio de Red LADA VpNet se ofrece a todos los Clientes comerciales de todo el país, siempre y cuando cumplan con las condiciones especificadas en el presente documento y en el contrato de servicio.

### *D.1.4.4. Reglas de Aplicación*

1. Todos los Clientes recibirán la tarifa de acuerdo al consumo del mes anterior en su primer mes y posteriormente se posicionará en el rango corresponde, de acuerdo a su consumo en minutos del mes anterior.

2. De acuerdo al tipo de tráfico que curse el Cliente y al consumo en minutos a través de LADA, el Cliente se situará en un rango de tarifa, la cual es dinámica de manera que el Cliente puede disminuir su tarifa si aumenta su tráfico y viceversa.

3. El Cliente no podrá recibir una sola tarifa para todo su tráfico nacional, debido que las tarifas del inciso B) 2. se aplican en función al tipo de llamada, según las definiciones del tipo de tráfico del inciso A) 1.

4. Para ser Cliente del Servicio Red LADA VpNet se requiere la firma de un contrato.

5. El Servicio de Red LADA VpNet se activará a través de la Red Pública Conmutada de Telmex.

6. En caso de que en uno o seis meses consecutivos el Cliente no cumpla con el consumo mínimo mensual de 40,000 minutos, Telmex aplicará automáticamente las tarifas base para LADA VpNet.

7. En caso de que en seis meses consecutivos el Cliente no cumpla con el consumo mínimo mensual de 40,000 minutos, Telmex aplicará automáticamente la mejor tarifa de larga distancia para tráfico público conmutado de acuerdo a su consumo mensual.

### *D.1.4.5. Descuentos*

1. Se aplica el descuento del 100% en los gastos de acceso al servicio LADA VpNet. Aplicable hasta el 31 de Diciembre del 2001.

2. "Promociones y Descuentos LADA VpNet"

   Estas Promociones tendrá vigencia indefinida, Telmex notificará con 3 meses de anticipación la terminación de las mismas y ofrece a los Clientes VpNet lo siguiente:

   a) Para los Servicios Tarjeta Telefónica Telcard, Servicios por operadoras 020, 090, Servicios Semiautomáticos y 001 - 880, 881 y 882 se les aplicarán los siguientes descuentos de acuerdo al 100% de su consumo mensual de Minutos en Larga Distancia:

| Consumo Mensual en Minutos: | Descuento LADA VpNet |
|---|---|
| Menores a 40,000 | 30% |
| 40,000 a 100,000 | 33% |
| 100,001 en adelante | 38% |

### *D.1.4.6. Políticas de Comercialización*

1. Para acceder a los beneficios y tarifas de la Red LADA VpNet, el Cliente debe consumir actualmente 40,000 minutos mensuales de Larga Distancia y deberá firmar el contrato de Red LADA VpNet con duración de hasta por 3 años. Posteriormente el Cliente deberá facturar en la Red LADA VpNet un consumo mínimo mensual de 40,000 minutos.

2. La configuración de la Red LADA VpNet, se ofrece a los Clientes comerciales para satisfacer sus necesidades de comunicación interna, por lo que queda prohibido su uso para propósitos de reventa o cualquier otro uso no permitido por la Ley, la normatividad vigente en materia de telecomunicaciones y resoluciones emitidas por "COFETEL".

3. La prestación de este servicio, así como sus términos y condiciones únicamente se aplicarán al Cliente que se encuentre al corriente de sus pagos, conforme al contrato vigente y al código de prácticas comerciales de Telmex.

4. Las tarifas del servicio aquí presentadas, son excluyentes de cualquier otro plan o promoción que ofrezca actualmente o en el futuro Telmex, en sus servicios de larga distancia.

5. Asociado a la Red LADA VpNet, los Clientes podrán obtener el servicio de Tarjeta LADA VpNet.

6. TELMEX configurará la Red LADA VpNet de cada Cliente a fin de acondicionarla de manera que sea funcional a las necesidades particulares de cada Cliente, acorde a sus necesidades de comunicaciones privadas y únicamente para ser usada en el entorno de la RLVPN.

7. Los servicios y/o enlaces dedicados que no formen parte de la RLVPN se cobrarán a las tarifas vigentes debidamente autorizadas por "COFETEL".

8. El tráfico de larga distancia que se realice a través de enlaces dedicados que formen parte de la RLVPN no causa cargo por servicio medido.

9. Para que el Cliente tenga acceso al tráfico On Net - On Net Internacional, el Cliente se compromete a mantener un consumo mínimo mensual de 1,000 minutos de larga distancia internacional o su equivalente en un año.

10. Si el Cliente desea terminar anticipadamente el contrato, el Cliente deberá informar a Telmex con 90 días naturales de anticipación sin que esto implique sanción alguna por parte de Telmex.

11. Los cargos de los servicios locales utilizados para establecer y accesar la Red LADA VpNet, serán los vigentes registrados ante "COFETEL".

12. Las tarifas correspondientes a la Red LADA VpNet podrán sufrir incrementos o decrementos durante la vigencia del contrato, acorde a las condiciones del mercado.

## D.2. MÉXICO – ALESTRA

La siguiente información fue tomada de la página Web de Alestra: www.alestra.com.mx y de la página Web de la “Comisión Federal de Telecomunicaciones” (COFETEL) de México (http://www.cft.gob.mx/html/4_tar/alestra/alestra017d.html).

**Libro tarifario de Alestra**
**Capítulo 4.** Otros servicios
(Vigencia al 30 de julio de 1998) **Folio 497**

### *D.2.1. DEFINICIONES IMPORTANTES*

- *Acceso Remoto:* Tipo de acceso que permite a los usuarios realizar llamadas desde ubicaciones fuera de red y completar llamadas tanto dentro como fuera de su red a través de una Tarjeta Telefónica AT&T Aria-VNS.
- *AT&T Aria-VNS:* Servicio de Red Privada Virtual de Alestra.
- *AT&T Aria-GVNS:* Servicio de interconexión entre redes privadas virtuales internacionales.
- *Interconexión a SDN/SDDN*: Funcionalidad que permite interconectar a Clientes del Servicio AT&T Aria-VNS en México a la Red Privada Virtual SDN y/o SDDN del mismo Cliente en EUA.
- *Llamada AT&T Aria-VNS Acceso Remoto*: Este tipo de llamada se lleva a cabo cuando ésta se origina en una localidad no perteneciente a la red privada virtual del cliente a través de la *Tarjeta Telefónica AT&T Aria-VNS*.
- *Llamada AT&T Aria-VNS en Red*: Este tipo de llamada se lleva a cabo cuando el número marcado está registrado en la base de datos del servicio AT&T ARIA-VNS, y forma parte de la Red Privada Virtual del Cliente.
- *Llamada AT&T Aria-VNS Forzada en Red*: Este tipo de llamada se lleva a cabo cuando un usuario marca un número público para llamar a una localidad que forma parte de la Red Privada Virtual del Cliente, sin embargo la llamada es terminada utilizando un número específico de ruteo. Para efectos de Tarificación se considera como una llamada en Red.
- *Llamada AT&T Aria-VNS Virtual en Red:* Este tipo de llamada se lleva a cabo cuando el número marcado está registrado en la base de datos del servicio AT&T ARIA-VNS, y forma parte de la Red Privada Virtual del Cliente, sin embargo esta llamada es terminada usando un número público de ruteo. Para efectos de Tarificación, se considera como una llamada en Red.
- *Llamada AT&T Aria-VNS Fuera de Red:* Este tipo de llamada se lleva a cabo cuando el número marcado no está registrado en la base de datos del servicio AT&T Aria-VNS, por lo que no forma parte de la Red Privada Virtual del Cliente.
- *SDN (Software Defined Network):* Servicio de Red Privada Virtual de AT&T en EUA para transmisión de voz.
- *SDDN (Software Defined Data Network):* Servicio de Red Privada Virtual de AT&T en EUA para transmisión de datos.
- *Tarjeta Telefónica AT&T Aria-VNS:* Tarjeta Telefónica Postpagada de Alestra utilizada para los Servicios de Red Privada Virtual de Alestra.

### *D.2.2. DESCRIPCIÓN DEL SERVICIO AT&T ARIA-VNS*

El servicio consiste en una red privada virtual (VNS, por sus siglas en ingles) configurada mediante programas de "Software" dentro de la Red Inteligente de Alestra (sistemas, procesadores de información y bases de datos para cada Cliente), que permite a las empresas integrar y utilizar la misma en concordancia con sus líneas privadas dedicadas o sus enlaces conmutados. (Ver *Fig. D.1.*)

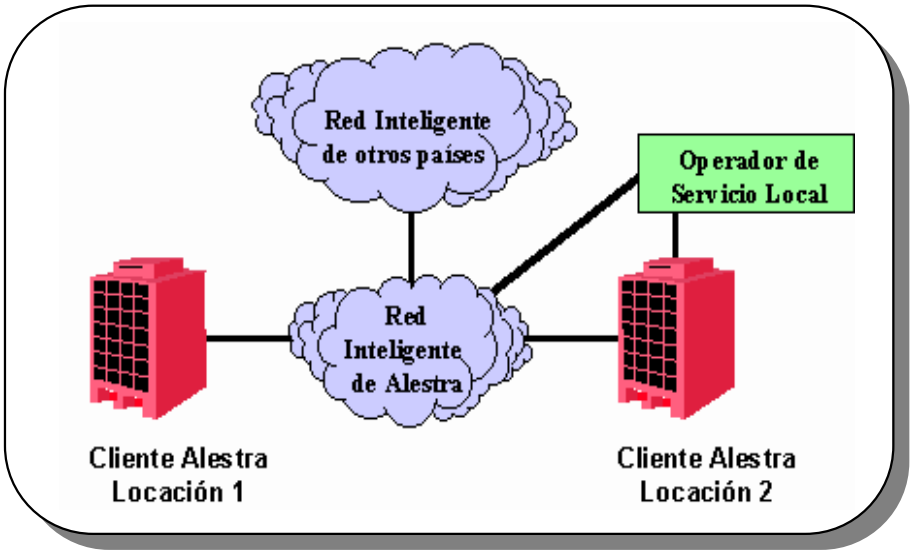



*Fig. D.1. Servicio AT&T Aria-VNS.*

### *D.2.3. DESCRIPCIÓN DEL SERVICIO DE INTERCONEXIÓN ENTRE REDES PRIVADAS VIRTUALES INTERNACIONALES*

Este servicio ofrece la capacidad de unir en una sola red global, la red privada virtual en México de un cliente con su red privada virtual en el extranjero. De tal manera, que un cliente de ***AT&T Aria-VNS*** en México que también cuente con una red privada virtual en otro país, podrá unir sus redes privadas virtuales y será capaz de realizar llamadas "GVNS - En Red" .

Las llamadas GVNS - En Red son aquellas que tienen como origen y destino localidades que forman parte de la red ***AT&T Aria-VNS*** en México y de la red privada virtual del cliente en algún otro país. Todas aquellas llamadas que no cumplan totalmente con este esquema, no serán consideradas llamadas ***AT&T Aria-GVNS.***

El servicio de ***AT&T Aria-GVNS*** únicamente se puede ofrecer a aquellos clientes de ***AT&T Aria-VNS*** en México que cuenten con un servicio de red privada virtual internacional con alguna compañía que haya celebrado un convenio bilateral de interconexión con Alestra para originar y terminar llamadas GVNS - En Red.

### *D.2.4. REGLAS DE APLICACION DEL SERVICIO AT&T ARIA-VNS*

Las reglas de aplicación del servicio *AT&T Aria-GVNS* pueden ser consultadas en la página Web de COFETEL de México:
http://www.cft.gob.mx/html/4_tar/alestra/alestra19d.html.

#### *D.2.4.1. Tiempo*

- En la oferta de Alestra para el servicio *AT&T Aria-VNS* todas las llamadas serán medidas en intervalos de minutos completos; esto es, las fracciones se redondearán al minuto inmediato superior. En la determinación del redondeo de centavos M.N. para las llamadas de Red Privada Virtual se utilizará el mismo procedimiento que en todas las tarifas de Alestra donde se siguen los lineamientos legales en la materia. La unidad mínima para el cálculo de tiempo es un minuto.

- El tiempo real de cálculo para la duración de la llamada se registra cuando se inicia la conexión con el destino y termina cuando se desconecta.

#### *D.2.4.2. Distancia.*

- Para efectos de tarificación de llamadas con origen y destino dentro de la República Mexicana existe una tarifa única, esto es, la tarificación no dependerá de la distancia entre los puntos.

- Para efectos de tarificación de llamadas con origen dentro de la República Mexicana hacia E.U.A., Canadá o Resto del Mundo, la tarificación dependerá de la región destino de la llamada.

#### *D.2.4.3. Tarificación.*

Los cargos de *AT&T Aria-VNS* son determinados en base a factores de configuración de llamadas (en red, fuera de red, virtual en red, forzada en red), tipo de acceso y egreso, destino, duración de llamadas, funcionalidad y tipo de contratación en diversos Planes de descuento disponibles.

1. A menos que se especifique lo contrario la unidad de tarificación será un centavo de peso mexicano. Cualquier cantidad menor se redondeará a la unidad inmediata superior.

2. El servicio de *AT&T Aria-VNS* es sensitivo a diversos factores en la determinación de sus precios por consumo. La estructura de tarifas está integrada por tres tipos de elementos.

    - Cargos por Uso: Por llamada según tarifa *AT&T Aria-VNS* correspondiente / Por uso de funcionalidad.
    - Cargos Mensuales: Por funcionalidad.

- Cargos por Evento: Por contratación / Por evento de instalación de funcionalidad / Por evento por demanda.

3. Planes y Paquetes Tarifarios: Para efectos de contratación del Servicio *AT&T Aria-VNS* será indispensable que el Cliente seleccione al menos uno de los Planes ofrecidos para este servicio. La contratación de cualquier Plan incluye:

   - Posibilidad de realizar diferentes tipos de llamadas (en red, forzada en red, virtual en red, fuera de red).
   - Planes de marcación.
   - Reportes generales en papel o medio magnético.
   - Facturación detallada.

   Aunado a esto, el Cliente puede elegir el tipo de funcionalidad que se adecue a sus necesidades, misma que incurre en cargos de instalación y mensuales independientes.

4. Cargos por Funcionalidad

| Funcionalidad | Cargo por Evento/Instalación | Cargo Mensual |
|---|---|---|
| Códigos de Autorización:<br>Bloque de 20 Códigos<br>Bloque de 50 Códigos | | |
| | $750.00 | $280.00 |
| | $1,500.00 | $560.00 |
| Códigos de Cuenta | $750.00 | $1,400.00 |
| Enrutamiento Alterno en egreso ocupado* | $380.00 | -- -- |
| Enrutamiento Flexible (Por activación, incluye desactivación) | $50.00 | -- -- |
| Filtración Básica:<br>Por grupo de Estación Básico<br>Por grupo de Filtración | | |
| | $500.00 | $300.00 |
| | $260.00 | $150.00 |
| Filtración Programada:<br>Por grupo de Estación programada<br>Por grupo de Filtración | | |
| | $550.00 | $350.00 |
| | $260.00 | $150.00 |
| Grupo cerrado de Usuarios (Por grupo) | $760.00 | $450.00 |
| Interfaz a Red Privada* | $500.00 | -- -- |
| Interconexión a SDDN**<br>Franja Fronteriza***<br>Resto de México | | |
| | $15,000.00 | $60,000.00 |
| | $15,000.00 | $129,000.00 |
| Localidad Compartida* | $700.00 | -- -- |
| Localidad Virtual* | $380.00 | -- -- |

### *D.2.5. ESQUEMA TARIFARIO DEL SERVICIO AT&T ARIA-VNS*

La estructura tarifaria del servicio *AT&T Aria-GVNS* puede ser consultada en la página Web de COFETEL de México http://www.cft.gob.mx/html/4_tar/alestra/alestra19d.html.

La tarificación de llamadas del servicio *AT&T Aria-VNS* se lleva a cabo de acuerdo con el tipo de llamada realizada: En red, fuera de red y la forma de acceso / egreso. Para la tarificación del Servicio de Red Privada Virtual se ofrecen las siguientes tarifas base. Las tarifas que se ofrecen son por minuto para los diferentes destinos.

| Destino | Tipo de Llamada | | Tarifa |
|---|---|---|---|
| | En Red | Fuera de Red | |
| Nacional | A1 | | 1.07 |
| | B1,B3 | B2 | 1.19 |
| | C1 | C2 | 1.45 |
| EUA Banda 1 y 2 | F1 | F2 | 4.70 |
| | G1 | G2 | 4.91 |
| EUA Ciudades Fronterizas | F1 | F2 | 1.93 |
| | G1 | G2 | 2.04 |
| Canadá | J1 | J2 | 6.53 |
| | K1 | K2 | 6.84 |
| Centroamérica | J1 | J2 | 5.19 |
| | K1 | K2 | 5.43 |
| Sudamérica, Caribe, Puerto Rico y Alaska | J1 | J2 | 11.70 |
| | K1 | K2 | 12.28 |
| Europa, Africa y Cuenca del Mediterráneo | J1 | J2 | 10.50 |
| | K1 | K2 | 10.92 |
| Resto del Mundo | J1 | J2 | 13.17 |
| | K1 | K2 | 13.74 |

1. Descripción de tarifas para llamadas *AT&T Aria-VNS* Nacionales.

   Tarifa A1. Llamada AT&T Aria-VNS tipo A (En red). Aplica para llamadas entre localidades en red con acceso y egreso dedicado a la red ALESTRA.

   Tarifa B1. Llamada AT&T Aria-VNS Tipo B (En red). Aplica para llamadas entre una localidad en red con acceso dedicado y una localidad en red con egreso conmutado.

Tarifa B3. Llamada AT&T Aria-VNS Tipo B (En red). Aplica para llamadas entre una localidad en red con acceso conmutado y una localidad en red con egreso dedicado.

Tarifa B2. Llamada AT&T Aria-VNS Tipo B (Fuera de red). Aplica para llamadas entre una localidad en red con acceso dedicado y una localidad fuera de red con egreso conmutado.

Tarifa C1. Llamada AT&T Aria-VNS Tipo C (En red). Aplica para llamadas entre dos localidades en red con acceso y egreso conmutado.

Tarifa C2. Llamada AT&T Aria-VNS Tipo C (Fuera de red). Aplica para llamadas entre una localidad en red con acceso conmutado y una localidad fuera de red con egreso conmutado.

2. Descripción de tarifas para llamadas AT&T Aria-VNS desde México hacia E.U.A.

   Tarifa F1. Llamadas AT&T Aria-VNS Tipo F (En red). Aplica para llamadas entre una localidad en red con acceso dedicado a una localidad virtual en red en EUA.

   Tarifa F2. Llamadas AT&T Aria-VNS Tipo F (fuera de red). Aplica para llamadas entre una localidad en red con acceso dedicado a una localidad fuera de red en EUA.

   Tarifa G1. Llamadas AT&T Aria-VNS Tipo G (En red). Aplica para llamadas entre una localidad en red con acceso conmutado a una localidad virtual en red en EUA.

   Tarifa G2. Llamadas AT&T Aria-VNS Tipo G (Fuera de red). Aplica para llamadas entre una localidad en red con acceso conmutado a una localidad fuera de red en EUA.

3. Descripción de tarifas para llamadas AT&T Aria-VNS desde México hacia el resto del mundo (ROW).

   Tarifa J1. Llamadas AT&T Aria-VNS Tipo J (En red). Aplica para llamadas entre una localidad en red con acceso dedicado a una localidad virtual en red internacional.

   Tarifa J2. Llamadas AT&T Aria-VNS Tipo J (Fuera de red). Aplica para llamada entre una localidad en red con acceso dedicado a una localidad fuera de red Internacional.

   Tarifa K1. Llamadas AT&T Aria-VNS Tipo K (En red). Aplica para llamadas entre una localidad en red con acceso conmutado a una localidad virtual en red internacional.

   Tarifa K2. Llamadas AT&T Aria-VNS Tipo K (Fuera de red). Aplica para llamadas entre una localidad en red con acceso conmutado a una localidad fuera de red internacional.

4. Descripción de tarifas para llamadas AT&T Aria-VNS Acceso Remoto.

| Orígen | Destino | Tarifa |
|---|---|---|
| México | Nacional | 1.73 |
| Estados Unidos Continental | México | 9.00 |
| México | EUA Banda 1 y 2 | 5.20 |
| México | EUA Ciudades Fronterizas | 2.16 |
| México | Canadá | 7.21 |
| México | Centroamérica | 5.77 |
| México | Sudamérica, el Caribe, Puerto Rico y Alaska | 12.97 |
| México | Europa, Africa y Cuenca del Mediterráneo | 11.53 |
| México | Resto del Mundo | 14.42 |

- Llamada *AT&T Aria-VNS* Acceso Remoto Nacional: Este tipo aplica para llamadas que se originan en México a través de la *Tarjeta Telefónica AT&T Aria-VNS* hacia cualquier lugar del territorio nacional.

- Llamada *AT&T Aria-VNS* Acceso Remoto a EUA: Este tipo aplica para llamadas que se originan en México través de la *Tarjeta Telefónica AT&T Aria-VNS* hacia EUA.

- Llamada *AT&T Aria-VNS* Acceso Remoto Internacional: Este tipo aplica para llamadas que se originan en México a través de la *Tarjeta Telefónica AT&T Aria-VNS* hacia el resto del mundo.

- Llamada *AT&T Aria-VNS* Acceso Remoto desde EUA hacia Destino Nacional: Este tipo aplica para llamadas que se originan desde cualquier localidad en EUA a través de la *Tarjeta Telefónica AT&T Aria-VNS* hacia un Destino en México.

5. Descripción de bandas geográficas AT&T Aria-VNS desde México hacia Estados Unidos.

| Bandas en México | Distancia entre el origen de la llamada en México y el Punto de interconexión fronterizo (PCT) |
|---|---|
| 1 | 0.1 - 550 Km |
| 2 | más de 550.1 Km |

Nota: Banda 1 - Desde México Centro Norte. Banda 2 - Desde México Centro Sur.

## D.3. BRASIL – EMBRATEL

La siguiente información fue tomada de la página web de Embratel: http://www.embratel.com.br.

### *D.3.1. DESCRIPCIÓN DEL SERVICIO*

El servicio de Red Privada Virtual de voz de Embratel "VipNet", conocido también como Voice VPN (Virtual Private Network) atiende oficinas no sólo en el Brasil sino también en el exterior.

El VipNet, como servicio de telefonía avanzada de larga distancia evolucionó a la par con la demanda de tráfico de las llamadas nacionales e internacionales, además de facilitar las comunicaciones corporativas. El nuevo VipNet en la RI conecta el PABX de las empresas clientes con la red 100% digital de Embratel, permitiendo formar una Voice VPN que soporta el tráfico de telefonía corporativo, con calidad, desempeño y economía. Con este servicio, la comunicación corporativa es más simple y eficiente.

El VipNet ofrece a los clientes una gran variedad de beneficios:

- Costos de instalación y operación de redes reducidos.
- Disponibilidad y confiabilidad de una red privada.
- Rápida instalación.
- Interconexión de sus unidades de negocios remotos y usuarios en tránsito a la red.
- Flexibilidad para extender las facilidades de telefonía a cada localidad del cliente.
- Reconfiguración de su capacidad de transmisión conforme la dinámica de la empresa.
- Llamadas nacionales e internacionales con costo reducido.
- Acceso de teléfonos celulares a la red (extensiones virtuales).
- La posibilidad de comercializarse junto con el servicio Digidial, que atiende bajo requerimiento a los clientes que necesitan de aplicaciones tales como videoconferencia, educación a distancia y telemedicina.

El cliente VipNet cuenta con un plan de numeración especial de siete dígitos para realizar las llamadas corporativas. Esta facilidad simplifica el discado entre las unidades de negocios del cliente.

VipNet ofrece una facturación flexible, que puede centralizarse en una única localidad, o descentralizarse en cada punto de la red, conforme opción del cliente. El cliente VipNet también contará con un conjunto de informes vía Internet, que le permitirán dar seguimiento al tráfico telefónico de su empresa y sus respectivos costos.

Compartiendo los recursos disponibles de la moderna red de telecomunicaciones de Embratel, el VipNet ofrece un servicio de alta calidad, desempeño y bajo costo, ideal para las empresas nacionales y multinacionales con intereses de tráfico corporativo y de negocios, tanto en el Brasil como en el exterior.

En la siguiente tabla se presentan los países y los operadores con los cuales Embratel tiene acuerdos comerciales para la conexión de Redes Privadas Virtuales internacionales.

| PAIS | OPERADOR |
|---|---|
| Alemania | Deutche Telekom |
| Argentina | Telefónica de Larga Distancia |
| Bélgica | Belgacom |
| Canadá | Teleglobe (*) |
| Chile | Entel Chile (*) |
| Corea del Sur | Korea Telecom |
| Estados Unidos | AT&T<br>MCIW (*)<br>SPRINT (*) |
| Francia | France Telecom |
| Holanda | PTT Holanda |
| Italia | Telecom Itália |
| Japón | JT (Japan Telecom) (*)<br>KDD |
| Reino Unido | Cable & Wireless<br>BT |
| Suecia | Telia Internacional |
| Suiza | Swiss Telecom PTT |

(*) Disponible comercialmente, pero sin acuerdo firmado.

*Tabla D.1. Acuerdos comerciales de Embratel para el servicio VPN.*

### *D.3.2. ESQUEMA DE COMERCIALIZACION*

Embratel comercializa cuatro paquetes de facilidades, conforme las principales demandas corporativas, creando una solución personalizada para su empresa. Los paquetes son:

- Paquete Vip – Formado por facilidades indispensables para crear una red privada virtual, tales como:

- Plan de Numeración Privada: plan de discado privado con apenas siete dígitos, para cualquier localidad de la empresa, sea en el Brasil y en el exterior.

- Sígame: permite que los empleados ausentes de la oficina puedan recibir llamadas internas y externas.

- Tarifa Cierta: efectuando una llamada corporativa discando un número de la lista, este será traducido automáticamente para un número privado, garantizando siempre el menor costo en las llamadas corporativas.

- Paquete Móvil – Cuando la empresa posee varios colaboradores que pasan parte de su tiempo afuera de las oficinas y tienen necesidad de comunicarse con puntos de la red o fuera de ella.

    - Llamada Virtual: permite que usuarios en tránsito (fuera de la empresa) realicen llamadas por medio de un código de autorización como si estuviesen dentro de la empresa.

    - Llame Otra Vez: permite realizar más de una llamada virtual con un único acceso.

    - Ramal Agregado: permite que la empresa pueda incluir en su Plan de Numeración Privado puntos que no pertenecen a la red, tales como proveedores, clientes y asociados comerciales.

- Paquete Fácil – Administración de facilidades de telefonía corporativa. Embratel cuida de la programación de la facilidad, mientras que el cliente se concentra en sus negocios.

    - Discado Abreviado: con apenas tres dígitos, los empleados pueden llamar a los principales teléfonos internos o externos a la corporación, nacionales o internacionales.

- Paquete Control – Conjunto de informes suministrados por Embratel y de facilidades inteligentes para que el cliente obtenga gestión sobre sus costos de telecomunicaciones.

    - Llamada Inteligente: definido por el cliente, determinados ramales discarán, adicionalmente, dos dígitos (código de costo) de forma a asociar el costo de la llamada a proyectos o departamentos.

    - Ramal Restringido: definido por el cliente, determinados ramales podrán efectuar únicamente llamadas corporativas y/o nacionales y/o internacionales.

### *D.3.3. TIPOS DE LLAMADAS VIPNET*

- *Llamadas Corporativas (on-net):* Las llamadas corporativas se realizan a través de un número personalizado de siete dígitos, formado por un prefijo de tres dígitos y un número de extensión de cuatro dígitos. Las unidades conectadas directamente a Embratel y pertenecientes a la red del cliente podrán realizar esta modalidad de llamadas para usufructuar de tarifas especiales.

- *Llamadas de Larga Distancia (off-net):* El cliente disca, a partir de una localidad de la red corporativa, para cualquier lugar del Brasil o para el exterior, utilizando el código 21 de Embratel. Esta llamada tiene una característica semejante a la de cualquier llamada de larga distancia, sin embargo con la calidad de la conexión a la red Embratel, que optimiza el encaminamiento además de los descuentos que a ella están asociados. Estas llamadas se contabilizan para calcular el descuento y aprovechar su ventaja.

- *Llamadas Virtuales (virtual on-net):* El cliente disca para extensiones agregadas (pertenecientes al plan de numeración pero sin conexión directa) o un empleado en viaje origina llamadas desde afuera de la red (por el del acceso remoto). Estas llamadas se contabilizan para poder calcular el descuento, aprovechando sus ventajas.

### *D.3.4. EJEMPLOS DE CLIENTES VIPNET*

#### *VipNet reduce costos del Despacho Administrativo en el Distrito Federal*

(Tomado de http://www.embratel.com.br/cases2001/case.html?id=1243, Via 146, 2001/5)

La telefonía está dejando de representar grandes gastos para transformarse en significativos ahorros para el Despacho Administrativo el Ministerio de Hacienda en el Distrito Federal – y el servicio VipNet de Embratel, es el responsable por ello. Hace ya algunos años que se están realizando ajustes para optimizar los costos con proveedores de contratación externa en ese órgano de la administración pública. En el campo de la telefonía, las medidas de sensibilización asociadas a los avances tecnológicos ya registran una economía equivalente al 50% en los gastos mensuales, si se las compara a los gastos incurridos cuando se comenzó ese esfuerzo en 1998.

La implantación del VipNet representó una gran ganancia económica, comprobada por el delegado de la administración del Ministerio de Hacienda en el Distrito Federal, Marco Antônio Valadares Moreira. La posibilidad de formar una Red Interna de Telefonía (RIT) de alta confiabilidad permite realizar llamadas por medio de un plan de numeración telefónica propio del Ministerio, formado por códigos fácilmente memorizados y aplicados, como explicó el delegado.

Valadares Moreira resaltó también que el sistema presentado por Embratel para interconectar sedes de regiones fiscales en 11 estados y el Distrito Federal atiende la expectativa del Despacho. “Ahora, todo punto en que exista demanda de conexión interurbana será contemplado con el VipNet”, afirmó.

Actualmente, los Despacho Administrativos del Ministerio de Hacienda en la capital federal, 12 capitales de estados y el Distrito Federal ya están interconectados por el VipNet, optimizando costos de telefonía y comunicándose con tarifas equivalentes a las de las llamadas locales. Las ciudades son: Belém, Belo Horizonte, Brasília, Cuiabá, Curitiba, Fortaleza, Manaus, Porto Alegre, Recife, Rio de Janeiro, São Paulo, Salvador y

Florianópolis. En el Distrito Federal, están interconectados los siguientes edificios: Sede, Anexo, Darcy Ribeiro, Órganos Regionales, Órganos Centrales y Esaf.

***VipNet es el nuevo servicio contratado por Philips do Brasil***

(Tomado de http://www.embratel.com.br/cases2001/case.html?id=1244, Via 146, 2001/5)

La asociación ya dura mucho tiempo. Philips do Brasil, una de las mayores fabricantes de electroelectrónicos del país y del mundo, concentró su infraestructura de telecomunicaciones en Embratel, y fue una de las primeras en adherir al VipPhone, avanzando ahora en su pionerismo al migrar para el VipNet, un servicio que, además de las tarifas privilegiadas, asegura también mayor accesibilidad y practicidad en las comunicaciones entre sus unidades.

La empresa también pretende, conjuntamente con Embratel, proyectar una plataforma de servicios inteligentes de telefonía que será implantada en el segundo semestre de este año. “En una primera etapa, tendremos ventajas tales como facilidad de conexión, con códigos abreviados entre todas las unidades de la empresa. En vez de discar, por ejemplo, el número completo de Manaus, tendremos casi que una extensión allí lo que implica ahorro de tiempo y una operación más práctica, además de tarifas mucho más ventajosas”, explicó el gerente de telecomunicaciones de la empresa, Dirk Johannes Bal.

Según él, esta nueva etapa de la relación con Embratel, “que implica que estamos estrechando nuestra alianza”, es resultado de todo un proyecto de reformulación de las telecomunicaciones, que resultó en la contratación de varios servicios. Actualmente, dijo Bal, todo el sistema de telefonía entre las filiales y las unidades industriales está dentro de los parámetros del VipNet, así como para los empleados en tránsito, que podrán comunicarse entre sí desde cualquier lugar donde se encuentren: “Además, ya hemos integrado los servicios de videoconferencia al VipNet para toda la empresa.”

La matriz de la empresa Philips está en São Paulo, y tiene unidades en Manaus (AM), Recife (PE), Varginha (MG), São José dos Campos y otras ciudades del interior de São Paulo. “Queremos expandir los servicios que tenemos con Embratel en el Brasil para toda América Latina”, afirmó Bal. La subsidiaria brasileña es responsable por la operación en América Latina, donde la empresa tiene filiales en los siguientes países: Argentina, Uruguay, Paraguay, Chile, Perú, Colombia, Venezuela, Panamá y El Salvador.

Según Bal, entre los servicios inteligentes que serán implantados se encuentran, por ejemplo, los de re-llamadas entre las unidades (transferencias automáticas de llamadas vía extensiones), llamadas entre tres o más usuarios conjuntamente y llamadas desde afuera de la empresa por el 0800, que colocarán, por ejemplo, a los vendedores en comunicación directa con la empresa a través de códigos abreviados. “Estamos estudiando varios otros servicios que serán colocados a disposición paulatinamente”, adelantó Bal, para quien hoy los servicios de telecomunicaciones son esenciales en los negocios de cualquier empresa. “Nuestra fuerza de ventas, por ejemplo, diseminada por todo el Brasil, está interconectada por IP Discado con la matriz”, subrayó.

***HQ Global centraliza los servicios de telecomunicaciones***

(Tomado de http://www.embratel.com.br/cases2001/case.html?id=1470, Via 154, 2002/1)

Silvio Dechecchi, HQ Global

Son más de 40 mil clientes y cerca de quinientos centros de oficinas ejecutivas en 28 países. Operando en el Brasil hace diez años, HQ Global Workplaces está invirtiendo especialmente en la infraestructura tecnológica para ofrecer un diferencial a sus clientes. "Ellos son, en realidad, nuestros asociados así como nosotros lo somos de Embratel, la operadora en la cual centralizamos nuestras telecomunicaciones", afirmó el director de Tecnología de la empresa, Silvio DeChecchi.

Él opina que esa asociación se convirtió en realidad en mayo de 2000: "Fue cuando la empresa creó una dirección específica para tecnología, en un momento en que notamos patentemente que el apelo de las telecomunicaciones como servicio y como diferencial para nuestros clientes era enorme. Con esa decisión, también decidimos concentrar toda la parte de telecomunicaciones con Embratel. Fue una selección decidida en términos del costo-beneficio, y de la tecnología y calidad de los servicios".

Luiz Henrique Andrade, HQ Global

Cliente de los servicios Vip-Phone, Vipnet, Internet y Videoconferencia, según DeChecchi, la firma HQ cuenta con 11 edificios de oficinas subcontratados en el Brasil: "Cinco quedan en São Paulo y los demás están en Rio de Janeiro, Brasilia, Belo Horizonte, Porto Alegre, Salvador y Curitiba. Nuestros clientes tienen en común una enorme necesidad, por ejemplo, de llamadas DDD y DDI, lo que nos llevó a contratar el Vip-Phone y el Vipnet para poder ofrecer no sólo precios más competitivos sino sobre todo calidad, ya que una gran parte de esas empresas que arriendan oficinas con nosotros son multinacionales o filiales de empresas de otros estados. Consecuentemente, necesitan mantenerse en contacto con sus demás puntos permanentemente".

## D.4. USA – AT&T

La siguiente información fue tomada de la página web de AT&T http://www.att.com.

### *D.4.1. DESCRIPCIÓN DEL SERVICIO*

La red definida por software de AT&T (SDN) es uno de los productos insignia en la arquitectura nodal de AT&T. SDN provee a sus clientes la capacidad de contar con una red privada virtual corporativa (VPN) mientras utiliza las facilidades de la red conmutada de AT&T. SDN es un servicio de VPN de clientes que reside en la Red Inteligente mundial conmutada basada en los conmutadores 4ESS™ de AT&T y proporciona

características basadas en la red y capacidades de administración que no se encuentran generalmente en las redes privadas.

Algunas de características basadas en la red son enrutamiento personalizado, planes de numeración anticipados, investigación de llamadas, códigos de autorización, acceso remoto, códigos de seguridad y facturación personalizada. . SDN es compatible con la mayoría de las redes privadas y PBXs y, como tal, protege estas inversiones existentes. Puesto que SDN no requiere una base sofisticada de PBXs, los clientes pueden elegir el acceso tarifado o por marcación manual. El servicio apoya completamente la transmisión de datos análogos de hasta 28,8 Kbps y la transmisión digital de datos extremo a extremo de 56/64 Kbps.

### *D.4.2. OPCIONES SDN*

SDN proporciona varias características opcionales que permiten a una compañía personalizar el servicio para satisfacer sus necesidades. Entre todas ellas se destacan las siguientes:

- **Red de Datos Definida por Software (SDDN)** - Una red privada virtual de datos que permite a los usuarios negociar llamadas de datos por demanda (marcación manual). Da a los clientes acceso rápido para transmitir datos en 56 y 64 Kbps, 64 Kbps canales dedicados, 384 Kbps, y Nx64 Kbps.

- **SDN Internacional (SDN-I)** - Está disponible para compañías que trabajan en la arena global. Los llamadores pueden transmitir voz, datos, fax, gráficos, y video utilizando accesos dedicados o conmutados.

- **SDN Global (GSDN)** - A diferencia de SDN-I, GSDN es una opción internacional de solamente voz entre los sitios de una compañía en Estados Unidos y sus oficinas en el extranjero. GSDN es el más rentable servicio conmutado internacional de grandes cantidades de voz. Sin embargo, puede ser particularmente rentable para negocios con tan solo 2 horas de tiempo de llamadas por día para una localización internacional dada, durante los períodos de tarifas máximas. El acceso al servicio puede ser directo o conmutado.

- **Correo de Voz SDN** - es un servicio basado en la red diseñado para aplicaciones en las cuales asociados dispersos geográficamente necesitan estar en contacto con los otros y con los administradores centralizados. Las fuerzas de ventas, los técnicos, los asociados en movimiento, y las comunidades de interés dispersas pueden aumentar su comunicación a través del correo de voz de SDN.

- **Llamadas de Celular SDN** - Da a los suscriptores la capacidad para pre-suscribirse al servicio celular de modo que su SDN pueda transportar las llamadas de larga distancia que se originan desde sus teléfonos celulares. El llamador podrá transferir datos a las tarifas soportadas por el operador de servicio celular.

### *D.4.3. TIPOS DE ACCESOS*

SDN soporta una variedad de accesos desde las locaciones de un cliente hasta la red conmutada de AT&T. A continuación se presenta un resumen de los accesos usados más frecuentemente:

- **Acceso Dedicado** - también conocido como un Acceso Especial. Con este tipo de acceso se proporciona sobre: Línea Privada del Grado de Voz (VGPL - análogo), T1, T45, servicio de canal local DS0 de 56/64 digital, o ISDN.

- **Acceso Conmutado** - también conocido como Acceso de Servicio de Intercambio Local (LESA - Local Exchange Service Access) para voz. Este acceso se utiliza para traer a la red las localizaciones de poco volumen que no pueden justificar accesos dedicados. LESA está disponible a través de un Operador de Intercambio Local (LEC - Local Exchange Carrier) o de un operador independiente.

- **SDDN de Acceso Conmutado para Datos** - es un tipo de acceso (10ATT) en el cual las llamadas de datos se pasan a través del LEC a una oficina de AT&T sobre troncales con características del grupo D. Estas troncales se dedican al tráfico conmutado de datos.

- **Llamadas de Celular SDN** - una empresa puede pre-suscribir hasta 5000 números celulares para SDN. Las llamadas se pasan a través de la red del operador celular y se terminan en SDN.

- **Acceso Remoto de Red** (NRA - Network Remote Access) - Este acceso es útil para las locaciones remotas con tráfico SDN ocasional y para los asociados que viajan. NRA proporciona acceso a SDN desde estaciones no-SDN. Se solicita a los llamadores introducir un código válido de autorización antes de que SDN complete la llamada. Un administrador de telecomunicaciones decide cuales destinos de llamadas son válidos para los usuarios de NRA.

### *D.4.4. SERVICIO SDN GLOBAL (GSDN)*

El *Servicio Global de Redes Definidas por Software de AT&T (GSDN)* es un servicio de red virtual internacional de alta calidad. Ofrece conectividad para voz, fax y datos a nivel mundial mediante comunicaciones punto a punto, voz (full duplex) y datos en banda de voz, para clientes actuales SDN a través de sus redes de acceso.

El servicio GSDN utiliza las instalaciones de conmutación y transmisión de la Red Inteligente de alcance Mundial de AT&T. El GSDN de AT&T es ideal para grandes compañías internacionales con redes privadas existentes que necesitan expandirse o ser reemplazadas, o para pequeñas compañías internacionales con volúmenes de llamadas internacionales de larga distancia punto a punto de más de 2 horas al día.

El Servicio GSDN permite que un cliente establezca un camino de comunicación entre estaciones en Estados Unidos continental, Hawaii y/o Puerto Rico y una estación en un

país extranjero, a través de un acceso dedicado, usando un plan de marcación de números privados uniformes en la red o utilizando los formatos de marcación estándares internacionales. Las estaciones extranjeras del cliente se deben conectar a un servicio similar en el país extranjero según lo especificado por la compañía de telecomunicaciones extranjera.

GSDN puede también ser proporcionado en Estados Unidos continental, Hawaii y/o Puerto Rico a través de un acceso conmutado y puede ser conectado por líneas de acceso con una sede de AT&T, en donde se proporciona el servicio de AT&T SDN OneNet. Los clientes deben obtener el servicio de SDN OneNet en una línea de acceso conmutada de intercambio local, para utilizar el acceso conmutado de intercambio local a GSDN.

Las llamadas están disponibles entre cualquier estación designada por el Cliente en el continente de ESTADOS UNIDOS, Hawaii y/o Puerto Rico y una estación extranjera, pero no entre dos estaciones del continente de EUA, de Hawaii y/o de Puerto Rico o entre dos estaciones extranjeras.

GSDN ofrece dos planes de marcación - un plan de marcación privado abreviado de 7 dígitos o la marcación pública internacional (marcando 011) a través de una característica conocida como “enrutamiento forzado en-red”.

La arquitectura para GSDN consiste de dos componentes básicos:

- Red virtual de los EUA: Se basa en la arquitectura de red de SDN. Las instalaciones internacionales se proporcionan vía la red conmutada pública internacional.
- Red virtual no en los EUA: La arquitectura en un país diferente a USA se proporciona a través del servicio de red virtual en ese país.

### *D.1.4.1. Características del Servicio GSDN*

- Llamadas internacionales full duplex en la red.
- Filtro de Llamadas GSDN para restringir el acceso a países específicos, número(s) específico(s), y/o rango(s) de números para llamadas en la red.
- Códigos de Autorización de Cuenta GSDN para anular las funciones de filtro de llamadas.
- Discado abreviado de siete dígitos definido por el usuario para facilitar las llamadas.
- Enrutamiento forzado de todas las llamadas internacionales que vayan hacia la red, mediante el uso de números públicos o privados.
- Desbordamiento fuera de la red cuando la línea está ocupada (sólo en el GSDN entrante).

- Informes de Administración de la Red para el cumplimiento de requisitos específicos de la compañía.
- Centro de Control de Red.
- Desbordamiento de Terminación Directa de llamadas.
- Anuncio de Intercepción de la Red.
- Transmisión Conmutados de Datos.

### *D.1.4.2. Beneficios del Servicio GSDN*

- Es ideal como servicio de red privada virtual internacional que consolida el tráfico de las empresas y sustituye redes privadas con elevado costo fijo.
- Minimiza la necesidad de inversiones en equipos y ofrece un importante ahorro de costos comparado con las líneas internacionales privadas.
- Selecciona la ruta más económica para las llamadas de su compañía, ofreciendo el mejor precio posible sin cambiar las costumbres de discado de sus clientes.
- Mejora la administración de información con informes y facturación sofisticados.
- Le permite agregar nuevas localidades de clientes GSDN y nueva capacidad a su Red Definida por Software de AT&T mediante el cambio de software, eliminando los gastos de re-enrutamiento y re-cableado.
- Ofrece bloqueo mediante códigos de seguridad para reducir los costos asociados con el abuso de la red.
- Reconfigura las localidades de los clientes GSDN de una manera rápida y sencilla mediante una simple actualización del software.
- Ofrece capacidad por demanda y usted sólo paga por lo que usa.

### *D.4.5. ESQUEMA TARIFARIO DEL SERVICIO GVNS*

La siguiente lista de precios fue tomada de la “Guía de Servicios de Negocios de AT&T”, y es efectiva a partir del 31 de julio de 2001. En la tabla se presentan los países de cobertura del servicio GVNS. (Tabla D.2).

| SERVICIO GLOBAL DE REDES DEFINIDAS POR SOFTWARE<br>Locaciones de Acceso Conmutado en Estados Unidos continental<br>Hawaii y/o Puerto Rico – Locaciones Internacionales | | | | |
|---|---|---|---|---|
| Países con acuerdos Comerciales GVNS | Periodo Inicial Pico (18 Sec) | Periodo Inicial Fuera Pico (18 Sec) | Periodo Adicional Pico (6 Sec) | Periodo Adicional Fuera Pico (6 Sec) |
| Argentina | $0.4038 | $0.3552 | $0.1346 | $0.1184 |
| Australia | $0.2943 | $0.2595 | $0.0981 | $0.0865 |
| Belgium | $0.3348 | $0.2952 | $0.1116 | $0.0984 |
| Brazil | $0.3909 | $0.3447 | $0.1303 | $0.1149 |
| Canada | $0.1278 | $0.1140 | $0.0426 | $0.0380 |
| Chile | $0.4170 | $0.3669 | $0.1390 | $0.1223 |
| China | $0.9111 | $0.7998 | $0.3037 | $0.2666 |
| Finland | $0.3105 | $0.2745 | $0.1035 | $0.0915 |
| France | $0.2640 | $0.2328 | $0.0880 | $0.0776 |
| Germany | $0.2856 | $0.2520 | $0.0952 | $0.0840 |
| Hong Kong | $0.4845 | $0.4257 | $0.1615 | $0.1419 |
| Indonesia | $0.6570 | $0.5787 | $0.2190 | $0.1929 |
| Ireland | $0.2775 | $0.2451 | $0.0925 | $0.0817 |
| Israel | $0.5334 | $0.4689 | $0.1778 | $0.1563 |
| Italy | $0.3804 | $0.3348 | $0.1268 | $0.1116 |
| Japan | $0.3543 | $0.3120 | $0.1181 | $0.1040 |
| Korea, South | $0.5007 | $0.4407 | $0.1669 | $0.1469 |
| Mexico - Zone 1 | $0.2001 | $0.1737 | $0.0667 | $0.0579 |
| Mexico - Zone 2 | $0.3108 | $0.2619 | $0.1036 | $0.0873 |
| New Zealand | $0.5217 | $0.4584 | $0.1739 | $0.1528 |
| Philippines | $0.5385 | $0.4731 | $0.1795 | $0.1577 |
| Singapore, Republic of | $0.4536 | $0.3993 | $0.1512 | $0.1331 |
| Spain (Including Balearic Islands, Canary Islands, Ceuta and Melilla) | $0.3957 | $0.3483 | $0.1319 | $0.1161 |
| Sweden | $0.2874 | $0.2541 | $0.0958 | $0.0847 |
| Taiwan | $0.5214 | $0.4581 | $0.1738 | $0.1527 |
| United Kingdom | $0.2370 | $0.2097 | $0.0790 | $0.0699 |

*Tabla D.2. Lista de Precios y Cobertura del Servicio GVNS.*

## D.5. ESPAÑA – EL MERCADO DE RED PRIVADA VIRTUAL

La siguiente información fue tomada del *"Informe Anual 2001 – El mercado de las telecomunicaciones, audiovisual e Internet en España"* de la Comisión del Mercado de las Telecomunicaciones (CMT). El informe se puede encontrar en http://www.cmt.es/cmt/centro_info/publicaciones/Inf Anual 2001/ Inf-Completo.zip

### *D.5.1. DEFINICIÓN DE SERVICIOS DE COMUNICACIONES CORPORATIVAS*

*Tomado Pág. 523 – 524 del Informe Anual CMT 2001.*

" Como se ha comentado en el apartado de telefonía fija, el servicio telefónico en general abarca todas las actividades destinadas a prestar servicios de comunicación de voz entre los usuarios de terminales telefónicos conectados a los Puntos de Terminación de Red de la Red Telefónica Pública, con unos estándares de calidad mínimos (establecidos en las recomendaciones del CCITT).

Dentro de las diferentes modalidades de comercialización de los servicios de telefonía fija ofrecidos actualmente en el mercado nacional, se encuentran los denominados Servicios de Comunicaciones Corporativas, dirigidos a empresas y organizaciones públicas y privadas, y que dan respuesta a sus demandas específicas de telefonía y en general de comunicaciones corporativas (voz, fax y datos).

Estos servicios corporativos consisten en prestaciones especializadas y personalizadas de los servicios de telefonía, fax y datos a empresas, corporaciones y organizaciones, con prestaciones y facilidades propias de una red privada, normalmente superiores a las ordinarias del servicio telefónico fijo disponible al público.

Esto permite una gran flexibilidad y personalización del servicio a las necesidades de cada cliente, así como la integración corporativa de todo tipo de comunicaciones de voz, fax y datos a escala zonal, nacional e internacional, y con precios usualmente más bajos que los del servicio telefónico básico, fax y datos existentes en el mercado prestados desagregada-mente.

De todas maneras, hay que resaltar que con la liberalización total de los servicios de telefonía fija y la convergencia de los servicios de voz y datos, las diferencias entre aquélla, como concepto general, y las comunicaciones corporativas, como concepto específico, se difuminan cada vez más, puesto que en realidad, desde el punto de vista de la prestación del servicio, la telefonía en GCU es una parte integrante (una oferta especializada dirigida a empresas y corporaciones) de un todo más grande, como es la telefonía fija en general. De ahí que los datos aportados en este apartado hayan de tomarse con cierta precaución.

Las principales modalidades de Servicios de Comunicaciones Corporativas existentes en el mercado nacional son las siguientes:

**a) El servicio de telefonía en Grupo Cerrado de Usuarios**

El servicio telefónico en Grupo Cerrado de Usuarios constituye un caso particular de los mencionados Servicios de Comunicaciones Corporativas, y se encuentra plenamente liberalizado desde 1995. Si se ha considerado la telefonía en GCU un mercado diferenciado, ha sido únicamente debido a su tratamiento específico en la normativa legal, que impide interconectar GCU diferentes y efectuar llamadas entre dos terminales de la RTC a través de la red de un GCU. Posiblemente, esta específica regulación busque evitar que se puedan efectuar comunicaciones no corporativas a través del uso de una red GCU, con tarifas más bajas, orillando las tarifas generales del servicio telefónico básico.

Mediante este tipo de servicios, las corporaciones disponen de una única red y de un único acceso a la misma, conectando sus diferentes oficinas y dependencias tanto en la misma área metropolitana como en otra área geográfica nacional o internacional. Una de las tecnologías más utilizadas es el establecimiento de una **Red Privada Virtual (RPV),** es decir, se aprovechan las redes existentes de la Red Telefónica Pública para, normalmente a través de centralitas físicas o virtuales, proporcionar redes privadas virtuales de voz o de voz y datos.

Todo ello permite dar cierta homogeneidad a las comunicaciones corporativas, disponiendo de privacidad, integración de servicios y sistemas, servicio a medida y tarifas homogéneas ventajosas. Los usuarios tienen a su disposición en el mercado un gran abanico de prestaciones y facilidades, soportados bajo diferentes tecnologías y contratables en todo o en parte, ya que son sistemas flexibles, a medida del cliente.

Algunas de las características típicas de estos sistemas son las siguientes:

- Homogeneidad en las comunicaciones.
- Plan de numeración privado –números cortos– y a su vez integrado en la Red Telefónica Pública.
- Calidad y privacidad de las comunicaciones.
- Tarifas ventajosas y reducción de costes globales, con posibilidad de facturación detalla-da, control de gasto, etc.
- Delimitación del ámbito territorial de contratación (metropolitano, provincial, nacional o internacional).
- Disminución del gasto en equipos (centralitas, terminales) que se ofrecen en alquiler o venta.
- Servicio de centralita interna, con locuciones personalizadas.
- Integración y soporte global de diferentes servicios y tecnologías.
- Supervisión y gestión de red realizada por los operadores de manera remota y varios niveles de mantenimiento.

**b) El servicio IBERCOM**

El servicio IBERCOM de Telefónica es peculiar, pues integra los servicios clásicos de telefonía en GCU con el servicio telefónico fijo disponible al público, el servicio de transmisión de datos y el servicio de centralita física corporativa. Se soporta en una Red Digital Multiservicio con capacidades de **Red Privada Virtual** conectada a la Red Telefónica Pública.

Su comercialización se hace a través de múltiples modalidades (integrando las comunicaciones de voz, datos, redes IP, móviles, alquiler o venta de centralitas...) que se adaptan a diferentes tipos de clientes.

Se ha incluido en este apartado pues es un ser-vicio que, en general, satisface necesidades corporativas similares a las cubiertas por los demás operadores de telefonía en GCU, y compite con éxito en este mercado.

**c) El servicio CENTREX**

El servicio CENTREX de Telefónica es un servicio de centralita virtual que permite agrupar un conjunto de líneas diferenciándolas del resto de abonados al servicio telefónico fijo disponible al público, otorgando facilidades y prestaciones semejantes a las de una centralita privada.

Este servicio se caracteriza por no usar una centralita física dedicada al cliente en cuestión, pues utiliza los elementos de la Red Telefónica Pública y las centrales de conmutación públicas, ofreciendo prestaciones equivalentes a las de telefonía de voz en GCU y de centralita virtual.

Está orientado a las comunicaciones de voz en pequeñas empresas y organizaciones, aunque podría admitir también servicios de Red Digital de Servicios Integrados (RDSI) y un gran volumen de líneas.

Sus características principales son: plan privado de numeración, tarifa plana en las llamadas entre las líneas agrupadas, servicio básico de centralita privada (distribución de llamadas, desvío de llamadas, captura,...) sin necesidad de insta-lar una centralita física en las dependencias del cliente, y existencia de un servicio Unicentral (entre líneas conectadas a la misma central de conmutación) o Multicentral (entre líneas conectadas a diferentes centrales, que a su vez se interconectan como una sola).”

### *D.5.2. COMPORTAMIENTO DEL MERCADO DE LAS COMUNICACIONES CORPORATIVAS*

“ La facturación por servicios de comunicaciones corporativas en el año 2001 ascendió a 816,90 millones de euros. Este valor supone un crecimiento del 25,73%, importante pero muy inferior al alcanzado en el ejercicio anterior, que fue del 74,62%.

El número de clientes fue de 8.095, un 8,85% más que en 2000. Este distinto comportamiento de la facturación frente al número de clientes conduce a un aumento del 15,51% en la facturación media por cliente de los servicios de comunicaciones corporativas, que se sitúa en 100,91 euros.

Por operadores, el liderazgo lo ostenta Telefónica de España, S.A.U., con un 50,03% de la facturación, seguido de Telefónica Móviles España, con un 27,13%, y Telefónica Data España, con un 18,97%. El Grupo Telefónica factura, por tanto, un 96,13% del mercado, 1,48 pun-tos porcentuales menos que en el ejercicio 2000. " *Tomado Pág. 150 Informe Anual CMT 2001. (Ver Tabla D.3. y Fig. D.2.)*

| | Año 1999 | | Año 2000 | | % Variación | Año 2001 | | % Variación |
|---|---|---|---|---|---|---|---|---|
| | Millones de euros | % / Total | Millones de euros | % / Total | 1999/2000 | Millones de euros | % / Total | 2000/2001 |
| TELEFÓNICA DE ESPAÑA, S.A.U. | 169,61 | 45,58 | 323,83 | 49,84 | 90,93 | 408,67 | 50,03 | 26,20 |
| TELEFÓNICA MÓVILES ESPAÑA, S.A.U. | 0,06 | 0,02 | 147,43 | 22,69 | 100,00 | 221,64 | 27,13 | 50,34 |
| TELEFÓNICA DATA ESPAÑA, S.A. | 170,84 | 45,92 | 162,88 | 25,07 | -4,66 | 154,98 | 18,97 | -4,85 |
| RETEVISIÓN I, S.A.U. | 0,45 | 0,12 | 7,31 | 1,12 | 1521,43 | 13,92 | 1,70 | 90,45 |
| RESTO | 31,11 | 8,36 | 8,25 | 1,27 | -73,46 | 17,69 | 2,17 | 114,32 |
| TOTAL | 372,07 | 100,00 | 649,70 | 100,00 | 74,62 | 816,90 | 100,00 | 25,73 |

*Tabla D.3. Cuota mercado facturación de servicios de comunicaciones corporativas.*

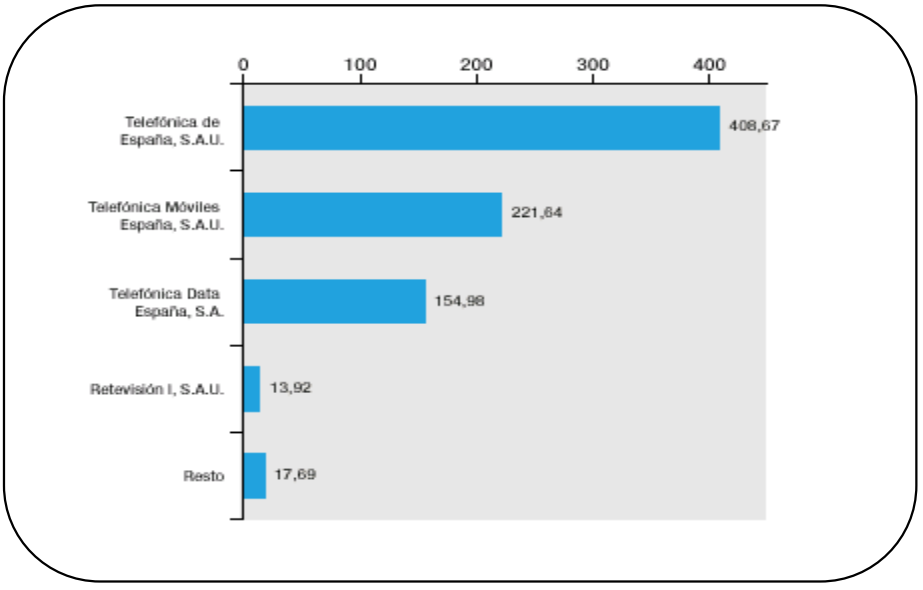



*Fig. D.2. Cuota mercado por facturación de servicios de comunicaciones corporativas.*

Las comunicaciones corporativas no incluyen los servicios de alquiler de circuitos, ni los servicios de transmisión de datos, los cuales son analizados en el informe del CMT separadamente.

En los servicios de alquiler de circuitos se incluyen los servicios de líneas dedicadas de datos, servicios de acceso a Internet y otros servicios de datos, y otros servicios de información. Para el 2001 representaban el 18.93% de los ingresos del mercado.

En los servicios de transmisión de datos se incluyen los servicios ATM, Frame Relay, IP, X.25, RDSI y Redes VSAT. Para el 2001 representaban el 37.87% de los ingresos del mercado.

En los servicios de comunicaciones corporativas se incluyen (como se explicó en el item D.5.1.) el servicio de Grupo Cerrado de Usuarios, el servicio IBERCOM y el servicio CENTREX. Para el 2001 representaban el 43.19% de los ingresos del mercado. (Ver *Tabla D.4.*)

| | Año 2000 | | Año 2001 | | % Variación 2000/2001 |
|---|---|---|---|---|---|
| | Millones de euros | % / Total | Millones de euros | % / Total | |
| Alquiler de circuitos para clientes finales | 284,78 | 18,93 | 367,17 | 18,55 | 28,93 |
| Transmisión de datos | 569,68 | 37,87 | 795,16 | 40,18 | 39,58 |
| Comunicaciones corporativas | 649,70 | 43,19 | 816,90 | 41,27 | 25,73 |
| TOTAL GENERAL | 1504,15 | 100,00 | 1979,22 | 100,00 | 31,58 |

*Tabla D.4. Evolución de los Ingresos por servicios de comunicaciones de empresa.*

### *D.5.3. SERVICIO RPV DE RETEVISION*

La siguiente información fue tomada de la página Web de Retevisión www.retevision.es.

El servicio de RPV de Retevisión proporciona una serie de facilidades y prestaciones propias de una Red Privada para comunicaciones de voz mediante la utilización de la Red Inteligente de Retevisión.

El servicio RPV permite integrar diferentes formas de acceso, como son líneas individuales, centralitas, etc., vía RTB (Red Telefónica Básica) o RDSI (Red Digital de Servicios Integrados), y cuando los acuerdos de interconexión lo permitan, se podrá acceder asimismo desde terminaciones de la red móvil. En la primera fase de lanzamiento, a la que se refiere este documento, los accesos de las líneas integradas en la RPV deberán ser accesos directos de Retevisión.

Se consideran de este modo los siguientes tipos de llamadas, dependiendo si los usuarios llamante y llamado pertenecen a la red:

- Llamadas internas, de posición RPV a posición RPV (on net)
- Llamadas externas, de posición RPV a posición no RPV (off net)

Entre los clientes de Redes Privadas Virtuales de Retevisión se encuentran principalmente instituciones públicas como la Generalitat de Catalunya, la Junta de Andalucía, la Dirección General de Patrimonio y la Junta de la Extremadura.

### *D.5.4. SERVICIO RPV DE VODAFONE*

La siguiente información fue tomada de la página Web de Vodafone www.vodafone.es.

Vodafone en España forma parte de la mayor compañía de telecomunicaciones móviles del mundo, Vodafone Group PLC, que participa en redes de telefonía móvil en 28 países de los cinco continentes.

Previamente conocida como Airtel Móvil, S.A, (constituida en 1994), Vodafone en España fue creada en octubre de 2001, y tras un breve periodo de doble marca Airtel-Vodafone, fue una de las primeras compañías del grupo en adoptar plenamente la marca Vodafone. Hoy en día Vodafone es uno de los líderes de los operadores móviles en España, con más de 7,9 millones de clientes (abril de 2002).

Vodafone ofrece el servicio *"Red Empresas S50",* una Solución de alta tecnología, que incorpora una Red Privada Virtual (VPN) muy flexible.

Gracias a las funcionalidades avanzadas que facilita la VPN, las empresas pueden definir las llamadas que realizan y reciben sus móviles Vodafone, adaptándose a las necesidades diferentes y cambiantes de sus empleados, a través de:

- Restricciones, que facilitarán el control del consumo de los teléfonos móviles Vodafone.

- Marcación abreviada, que facilitará la comunicación entre sus empleados.

Además, todas las llamadas que se realicen desde los móviles Vodafone de la empresa disfrutarán de los siguientes descuentos: (Tarifas a Noviembre de 2001).

- Llamadas Internas en el Grupo Cerrado de usuarios: 16% de descuento.

- Llamadas nacionales: porcentaje sobre valor de consumo por mes, por ejemplo:

  - De 0 a 50.0000 ptas. 4%
  - De 50.001 a 130.000 ptas 6%
  - De 130.001 a 260.000 ptas 7%
  - De 260.001 a 500.000 ptas 8%
  - De 4.000.001 a 5.000.000 ptas 13%
  - De 8.000.001 a 10.000.000 ptas 15%

- Llamadas Internacionales: porcentaje sobre valor de consumo por mes:

  - De 0 a 250.0000 ptas. 22%
  - De 250.001 a 500.000 ptas 30%
  - De 500.001 en adelante 35%

## D.6. ARGENTINA – TELEFÓNICA

La siguiente información fue tomada de la página Web de Telefónica de Argentina http://www.telefonica.com.ar

### *D.6.1. DESCRIPCIÓN DEL SERVICIO RPV*

La Red Privada Virtual de Telefónica ofrece la posibilidad de integrar todos los servicios de voz (líneas telefónicas, internos de centrales privadas y líneas de Servicio de Grupo Privado) en un único plan de numeración privado de cuatro dígitos agilizando y optimizando las comunicaciones tanto corporativas como externas de las empresas y sin la necesidad de erogar en inversiones de infraestructura propia.

El servicio es ofrecido a empresas regionales, instituciones gubernamentales u organizaciones operando a lo largo y ancho de todo el país. En la actualidad, más de 24.000 líneas de los clientes más importantes están adheridas al servicio.

Ventajas que ofrece una RPV

- Integración de líneas telefónicas comunes, centrales privadas, Servicio de Grupo Privado y celulares.
- Ausencia de inversiones.
- Puede usarse como una tarjeta de llamadas, accediendo desde cualquier teléfono de la Red Pública a cargo de la empresa.
- Es un servicio sencillo y ágil, que significa importantes ahorros y cuya gestión y contratación no requiere conocimientos especializados por parte del cliente.
- Amplio rango de facilidades para hacer más productivas y eficaces las comunicaciones (enrutamientos por día y hora, según origen, etcétera).
- Facilidades para un mayor control del consumo (límite de crédito, restricciones a nivel local urbano, interurbano e internacional, listas negras, enrutamiento forzado a On Net, etcétera).
- Privacidad absoluta.

### *D.6.2. FUNCIONAMIENTO DEL SERVICIO RPV*

El servicio RPV está integrado por Acceso Troncal Digital (ATD), Servicio de Grupo Privado (SGP), Telefonía Básica (TB) y celulares. Estos últimos pueden recibir llamadas desde cualquier interno de la RPV, también con un número de cuatro dígitos. De esta manera, la empresa posee virtualmente una Gran Central Privada que está dispersa en todos lados. Para la RPV, no hay diferencia en la ubicación de las líneas. Además, como el medio es la Red Telefónica Pública, las llamadas no sufren encolamientos

El Acceso Troncal Digital (ATD) es un acceso telefónico de alta capacidad ofrecido por una central pública conocida como Centro Frontal (CF) y el Servicio de Grupo Privado (SGP) proporciona las mismas funcionalidades que una central privada pero desde la central pública. (Ver *Fig. D.3*).

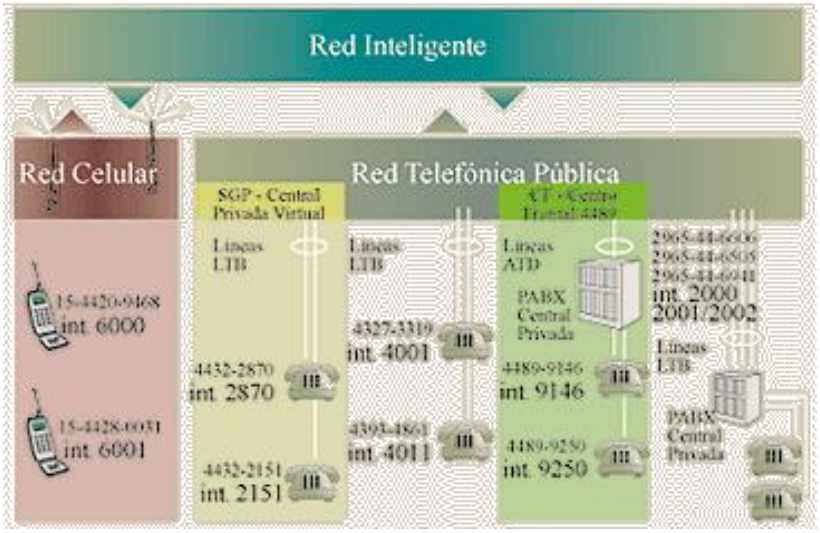



*Fig. D.3. Esquema de Funcionamiento del servicio RPV.*

# ANEXO E – CODIGO DE SOFTWARE

El presente anexo describe el desarrollo del software de animación gráfica “Red Privada Virtual”. Se explica el procedimiento para la creación del software y los programas que fueron utilizados para realizar la animación. Posteriormente se presenta una breve explicación del desarrollo de ambientes html y finalmente se incluye el código de software de cada una de las ventanas que componen el programa.

## E.1. DESCRIPCIÓN DE LA CREACIÓN DE LA ANIMACIÓN GRAFICA

El programa esta compuesto por páginas Web creadas en lenguaje HTML. Se utilizaron dos tipos de gráficos: GIF y JPG, ya que al ser formatos comprimidos, tienen buena calidad y ocupan poco espacio,

Para crear la animación gráfica se siguieron los pasos que se describen a continuación:

- El primer paso fue realizar un diseño previo en papel donde se definió la estructura que iban a tener las páginas y el contenido de cada una de ellas. Se definió el tipo y la cantidad de información para cada una de las páginas.

- Para la sección del tutor se hicieron archivos de texto utilizando el *Microsoft Word Pad* con el fin de no darle formato al documento, y se guardaron los archivos como texto puro.

- Para la sección de la demostración se crearon los dibujos para cada uno de los pasos de la ejecución del servicio de los diferentes tipos de llamadas en un archivo en *Microsoft PowerPoint*.

- Posteriormente los dibujos de PowerPoint fueron capturados y copiados en el programa gráfico *PaintShop Pro* para convertir cada uno de los dibujos en archivos .jpg y .gif.

- El programa *PaintShop Pro* también fue utilizado para crear los botones que realizan los vínculos dentro de la animación.

- Finalmente se utilizó el editor de HTML *Macromedia HomeSite* para la creación de las páginas Web basados en el diseño realizado:
    - El texto fue insertado en el cuerpo (<BODY>) de cada ventana y a continuación se procedió a darle formato utilizando las facilidades de HomeSite para insertar las etiquetas HTML.

- Para que los gráficos aparecieran en la animación se insertó en el código la etiqueta <IMG SRC="*nombre de archivo*">. El nombre del archivo indica el gráfico que se desea desplegar.
- La conexión de las ventanas de la animación gráfica se realizó utilizando vínculos de hipertexto, llamados "vínculos cercanos", que establecían vínculos con otra página Web dentro del mismo directorio. La etiqueta que se utiliza especifica la dirección URL del vínculo <A HREF="*URL*">. Cada vínculo esta asociado con uno de los botones que aparecen en las ventanas de la animación (por ejemplo, Demo, Tutor, Inicio, Siguiente, Anterior, etc.).

### *E.1.1. MACROMEDIA HOMESITE 5*

*Macromedia HomeSite 5* es un poderoso entorno de programación manual que provee un editor de solo código para el desarrollo de páginas web. Las avanzadas características de codificación permiten crear y modificar instrucciones HTML, así como CFML, JSP y XHTML, y cuenta con avanzadas herramientas que permiten validar, reutilizar, navegar y formatear código más fácilmente. (Ver *Fig. E.1.*)

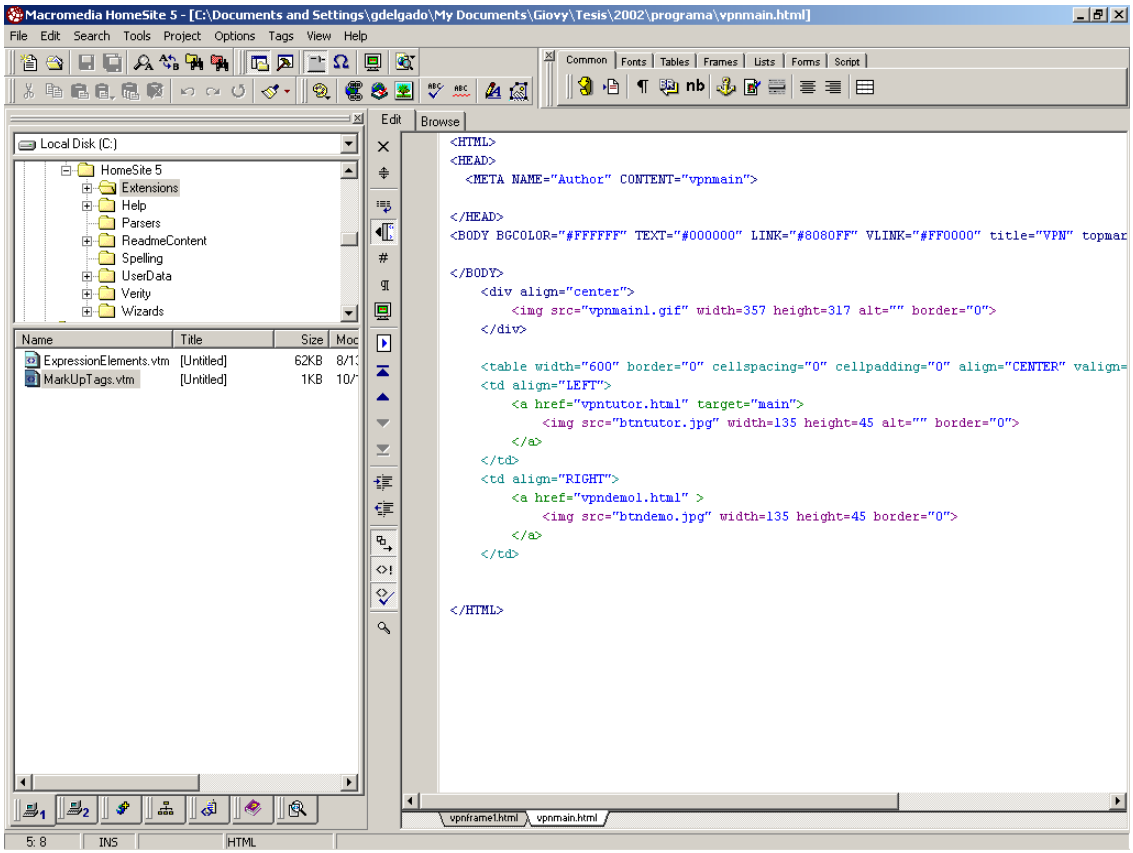



*Fig. E.1. Macromedia HomeSite 5*

Algunas de sus funciones más destacadas son:

- Capacidad de editar múltiples documentos a la vez.
- Asistente para marcos que facilita forjar marcos.
- Etiquetas HTML con claves coloreadas.
- Visor de imágenes.
- Verificador interno de ortografía.
- Navegador interno.
- Búsqueda y reemplazo de texto en múltiples archivos.

### *E.1.2. PAINTSHOP PRO*

*PaintShop Pro* es un editor gráfico para la creación y edición de iconos e imágenes y para el retoque de fotografías. (Ver Fig. E.2).

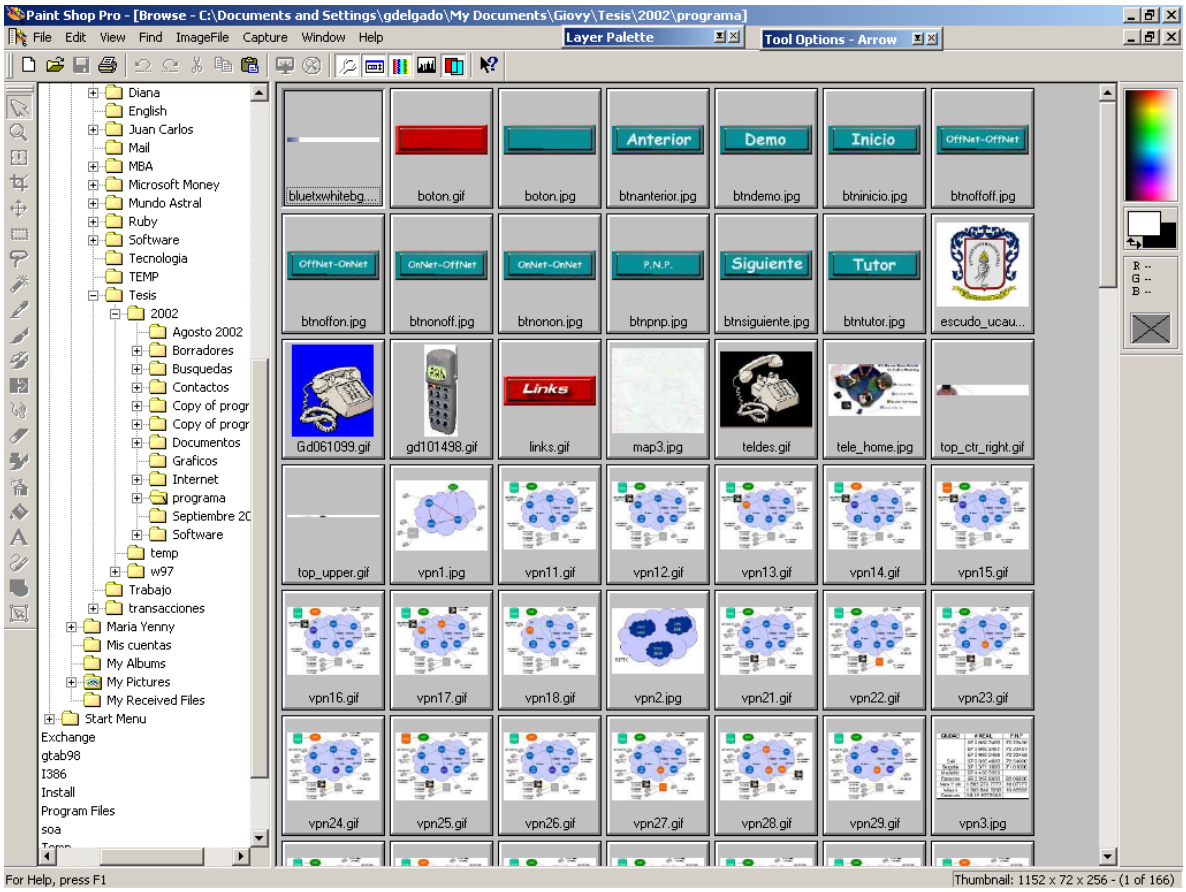



*Fig. E.2. Paintshop Pro*

### *E.1.3. ELABORACIÓN DE PAGINAS HTML*

El código de las páginas HTML está compuesto por una serie de etiquetas (marcadores) que indican como se quieren visualizar las cosas (p.e. texto, gráficos, tablas, etc).

En general las etiquetas utilizan el siguiente formato:

<ETIQUETA> Texto que será afectado por la etiqueta </ETIQUETA>

La parte <ETIQUETA> es un código (generalmente una abreviatura de una o dos letras, pero en ocasiones una palabra completa) que especifica el tipo de efecto que se desea. Estos códigos siempre van entre paréntesis angulares <>.

Todos los documentos HTML están formados por cuatro partes bien definidas y que son insertadas automáticamente por un editor de HTML. Cada una de estas partes está definida por etiquetas:

```
<!DOCTYPE HTML PUBLIC="-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>

<HEAD>
</HEAD>

<BODY>
</BODY>

<HEAD>
```

- *Declaración del tipo de documento*

  Una línea de texto en la que se declara la versión de HTML se está usando para crear el documento.Esto hace referencia a la *definición de tipo de documento o DTD* de la versión HTML que se usa.

  Por ejemplo:

  <!DOCTYPE HTML PUBLIC="-//W3C//DTD HTML 4.0 Transitional//EN" http://www.w3.org/TR/REC-html40/loose.DTD>

  La declaración de tipo de documento comienza con un signo menor que, seguido de un signo de admiración y por la expresión DOCTYPE (tipo de documento) HTML.
  PUBLIC identifica la DTD como accesible al público.

  La siguiente cadena de caracteres encerrada entre comillas es conocida como el identificador público para esta DTD particular: //W3C, indica que W3C es el autor de la DTD.

  //EN indica que se está utilizando la versión en inglés.
  El URL conduce hasta la copia pública de la DTD en la red.

- *El elemento HTML*

  Describe el documento como un documento HTML. Todos los contenidos de un documento HTML, con la excepción de la declaración del tipo de documento, deben encerrarse entra las etiquetas <HTML> y </HTML>

- *El encabezado del documento*

  Después de la etiqueta HTML viene el encabezado del documento. Esta sección es como una introducción a la página. Se conoce también como ***contenedor*** y va delimitado por la etiqueta <HEAD> Metadatos </HEAD>.
  Entre esta etiqueta se suele incluir información relacionada con el documento como son por ejemplo el título y otros metadatos. Los metadatos incluyen información diversa como puede ser, por ejemplo: Palabras clave, descripciones cortas, nombre del autor del documento, etc.
  La mayor parte de los navegadores web no muestran la información localizada en el contenedor, pero es reconocida por los buscadores de la Red que clasifican a diario la información que hay accesible en la Web.

- *El cuerpo del documento*

  En el cuerpo del documento se sitúan los contenidos del documento, por lo que es considerada la parte principal de todo documento HTML.
  Los contenidos deben encerrarse entre el elemento <BODY> Contenido del documento </BODY>.
  Todo lo que se incluye entre el elemento <BODY></BODY> será presentado por el navegador.

## E.2. VENTANA PRINCIPAL DEL PROGRAMA

El archivo inicial de ejecución del programa es el archivo “vpn.html”. Después de ejecutarlo aparece la *“ventana principal del programa”* que se muestra en la *Fig. E.3*.

Esta ventana está compuesta por dos marcos (frames): el primero se encuentra en la parte superior de la ventana e incluye el título de la animación y el escudo de la Universidad del Cauca, el segundo marco se encuentra en la parte inferior de la ventana e incluye los botones para llamar a las áreas que componen la animación.

Para crear estos marcos fue necesario crear una “página de marcos”, cuya misión es definir el tamaño del marco y especificar que documentos HTML se despliegan en cada uno. En este tipo de página no se puede colocar ni texto normal ni etiquetas HTML.

Archivo: ***vpn.html***

```
<HTML>
<HEAD>
  <!-- Created by Homesite 4.0 -->
  <TITLE>VPN</TITLE>
</HEAD>
<FRAMESET rows="14%, 86%">
<FRAME src="vpnframe1.html" scrolling="no">
<FRAME src="vpnmain.html" name="main"  scrolling="auto"> </FRAMESET>
</HTML>
```


*Fig. E.3. Ventana principal del programa*

El marco de la parte superior de la pantalla, permanece siempre fijo mientras el usuario navega a través de todas las ventanas de la animación.

Archivo: ***vpnframe1.html***

```
<HTML>
<HEAD>
  <TITLE>Menu</TITLE>
    <script language="Javascript">

<!-- hide and go seek

// bgFade by Jeff Pinyan || jefpin@bergen.org
```

```
// http://www.bergen.org/~jefpin

// This script changes the background color from black to white and

// then loads a page up.  I am working on making it go from color to

// color as needed (i.e. red to blue...)

n = -1

timerID = null

bgFade()

function bgFade(){

      n++

      if (n <= 15){

            color = 0

            if (n == 10){ color = "AAAAAA" }

            else if (n == 11){ color = "BBBBBB" }

            else if (n == 12){ color = "CCCCCC" }

            else if (n == 13){ color = "DDDDDD" }

            else if (n == 14){ color = "EEEEEE" }

            else if (n == 15){ color = "FFFFFF" }

            else{ color = 111111 * n }

            document.bgColor = "#" + color

            timerID = setTimeout("bgFade()",50)

   }

}

// end the game -->

</script>
</HEAD>
<BODY BGCOLOR= "#FFFFFF" LINK="#8080FF" VLINK="#FF0000" title="VPN" topmargin=2>
</BODY>
<table width="800" border="0" cellspacing="0" cellpadding="0" align="CENTER" valign="TOP">
            <td align="LEFT">
                  <img src="escudo_ucauca.gif" width=110 height=90 alt="" border="0">
            </td>
            <td align="LEFT">
                  <font face="Arial Black" size="+3" title="VPN" color="Navy">
                        <b>RED PRIVADA VIRTUAL - VPN</b>
                  </font>
            </td>

</table>
</HTML>
```

El marco que forma la parte inferior de la pantalla incluye un gráfico decorativo y dos botones que se enlazan con las dos áreas en las que se encuentra dividido el programa: el área de tutor y el área de demostración.

Archivo: ***vpnmain.html***

```
<HTML>
<HEAD>
  <META NAME="Author" CONTENT="vpnmain">

</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#8080FF" VLINK="#FF0000" title="VPN" topmargin=50
background="BACK_tirol.gif">

</BODY>
        <div align="center">
                <img src="vpnmain1.gif" width=357 height=317 alt="" border="0">
        </div>

        <table width="600" border="0" cellspacing="0" cellpadding="0" align="CENTER" valign="TOP">
        <td align="LEFT">
                <a href="vpntutor.html" target="main">
                        <img src="btntutor.jpg" width=135 height=45 alt="" border="0">
                </a>
        </td>
        <td align="RIGHT">
                <a href="vpndemo1.html" >
                        <img src="btndemo.jpg" width=135 height=45 border="0">
                </a>
        </td>


</HTML>
```

## E.3. AREA DE TUTOR

Al seleccionar el botón “Tutor” se crea un vínculo con el archivo “vpntutor.html” (corresponde a una página de marcos al igual que el archivo inicial “vpn.html”) y aparece la *ventana principal del programa* presentada en la *Fig. E.4.*


Archivo: ***vpntutor.html***

```
<HTML>
<HEAD>
  <!-- Created by Homesite 4.0 -->
  <TITLE>VPN</TITLE>
</HEAD>
<FRAMESET cols="20%, 80%">
        <frame name="" src="vpnmenu.html" frameborder="0" noresize scrolling="auto">
        <frame name="main2" src="vpnmain2.html" frameborder="0" noresize scrolling="auto">
</FRAMESET>
</HTML>
```

Esta ventana está compuesta por tres marcos. El primero es un marco fijo que se encuentra en la parte superior de la ventana y fue explicado en la sección E.2. El segundo marco se encuentra en la parte izquierda de la ventana y permite acceder a cada uno de los temas del tutor. El tercer marco en la parte derecha de la ventana incluye un gráfico decorativo que será reemplazado por el texto de cada uno de los temas del tutor.


*Fig. E.4. Ventana principal del tutor.*

La Parte Izquierda de la ventana es fija para todas las ventanas en el área del tutor, e incluye los botones de menú para los temas del tutor.

Archivo: ***vpnmenu.html***

```
<HTML>
<HEAD>
  <TITLE>Menu</TITLE>
</HEAD>
<BODY BGCOLOR= "#FFFFFF" LINK="#8080FF" VLINK="#FF0000" title="VPN" topmargin=25
background="backblue1.jpg" leftmargin=2 alink="#00FF00">
<a href="vpnmain.html" target="main"><img src="btntutinicio.jpg" width=149 height=32 alt="" border="0"></a><br>
<a href="vpntut1.html" target="main2"><img src="btnvpn.jpg" width=149 height=32 alt="" border="0"></a><br>
<a href="vpntut2.html" target="main2"><img src="btnpartic.jpg" width=149 height=32 alt="" border="0"></a><br>
<a href="vpntut3.html" target="main2"><img src="btngrpint.jpg" width=149 height=32 alt="" border="0"></a><br>
<a href="vpntut4.html" target="main2"><img src="btnbenusu.jpg" width=149 height=32 alt="" border="0"></a><br>
<a href="vpntut5.html" target="main2"><img src="btnbensus.jpg" width=149 height=32 alt="" border="0"></a><br>
<a href="vpntut6.html" target="main2"><img src="btnbenope.jpg" width=149 height=32 alt="" border="0"></a><br>
<a href="vpntut7.html" target="main2"><img src="btncaract.jpg" width=149 height=32 alt="" border="0"></a><br>
<a href="vpntut8.html" target="main2"><img src="btnarqred.jpg" width=149 height=32 alt="" border="0"></a><br>
<a href="vpntut9.html" target="main2"><img src="btnmetacc.jpg" width=149 height=32 alt="" border="0"></a><br>
<a href="vpntut10.html" target="main2"><img src="btntiplla.jpg" width=149 height=32 alt="" border="0"></a><br>
<a href="vpntut11.html" target="main2"><img src="btnnummar.jpg" width=149 height=32 alt=""
border="0"></a><br>
<a href="vpntut12.html" target="main2"><img src="btnvpndatos.jpg" width=149 height=32 alt=""
border="0"></a><br>
<a href="vpntut13.html" target="main2"><img src="btnvpnip.jpg" width=149 height=32 alt="" border="0"></a><br>
```

```
<a href="vpntut14.html" target="main2"><img src="btnngnvpn.jpg" width=149 height=32 alt="" border="0"></a><br>
</BODY>
</HTML>
```

La Parte Derecha de la ventana es similar a la página principal pero sin los botones Tutor y Demo.

Archivo: ***vpnmain2.html***

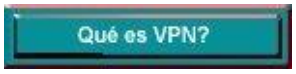
```
<HTML>
<HEAD>
 <META NAME="Author" CONTENT="vpnmain">

</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#8080FF" VLINK="#FF0000" title="VPN" leftmargin=80 topmargin=70 background="BACK_tirol.gif">

</BODY>
        <div align="left">
                <img src="vpnmain1.gif" width=357 height=317 alt="" border="0">
        </div>
</HTML>
```

### *E.3.1. CODIGO VENTANA "QUE ES VPN?"*

Al presionar el botón "Qué es VPN?" se crea un vínculo con el archivo "vpntut1.html" y aparece la ventana presentada en la *Fig. E.5.*



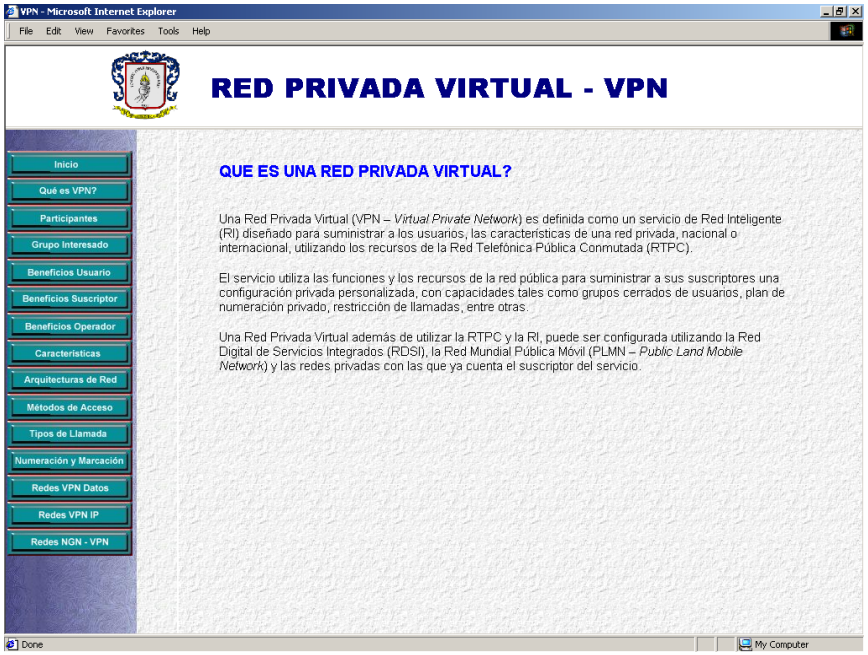




*Fig. E.5. Ventana del tutor "Qué es VPN?".*

Como ya se explicó, la parte superior (vpnframe1.html) y la parte izquierda (vpnmenu.html) de la ventana son fijas. Solamente presenta cambios la parte derecha de la ventana en la cual aparece el texto de cada uno de los temas del tutor.

Archivo: ***vpntut1.html***

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html xmlns:v="urn:schemas-microsoft-com:vml"
xmlns:o="urn:schemas-microsoft-com:office:office"
xmlns:w="urn:schemas-microsoft-com:office:word"
xmlns="http://www.w3.org/TR/REC-html40">

<head>
<meta http-equiv=Content-Type content="text/html; charset=windows-1252">
<meta name=ProgId content=Word.Document>
<meta name=Generator content="Microsoft Word 9">
<meta name=Originator content="Microsoft Word 9">
<link rel=File-List href="./vpntut1_files/filelist.xml">
<title>Menu</title>
<!--[if gte mso 9]><xml>
 <o:DocumentProperties>
  <o:Author>gdelgado</o:Author>
  <o:LastAuthor>gdelgado</o:LastAuthor>
  <o:Revision>15</o:Revision>
  <o:TotalTime>38</o:TotalTime>
  <o:Created>2002-07-25T17:19:00Z</o:Created>
  <o:LastSaved>2002-08-03T22:08:00Z</o:LastSaved>
  <o:Pages>1</o:Pages>
  <o:Words>125</o:Words>
  <o:Characters>715</o:Characters>
  <o:Company>Clarent Corporation</o:Company>
  <o:Lines>5</o:Lines>
  <o:Paragraphs>1</o:Paragraphs>
  <o:CharactersWithSpaces>878</o:CharactersWithSpaces>
  <o:Version>9.2720</o:Version>

 </o:DocumentProperties>
</xml><![endif]--><!--[if gte mso 9]><xml>
 <w:WordDocument>
  <w:Zoom>BestFit</w:Zoom>
 </w:WordDocument>
</xml><![endif]-->
<style>
<!--
 /* Style Definitions */
p.MsoNormal, li.MsoNormal, div.MsoNormal
        {mso-style-parent:"";
        margin:0in;
        margin-bottom:.0001pt;
        mso-pagination:widow-orphan;
        font-size:12.0pt;
        font-family:"Times New Roman";
        mso-fareast-font-family:"Times New Roman";}
h1
        {mso-style-next:Normal;
        margin:0in;
        margin-bottom:.0001pt;
        text-align:justify;
        mso-pagination:widow-orphan;
        page-break-after:avoid;
        mso-outline-level:1;
        font-size:11.0pt;
        mso-bidi-font-size:12.0pt;
```

```
		font-family:Arial;
		mso-font-kerning:0pt;
		mso-ansi-language:ES-CO;
		font-weight:normal;
		text-decoration:underline;
		text-underline:single;}
a:link, span.MsoHyperlink
		{color:#8080FF;
		text-decoration:underline;
		text-underline:single;}
a:visited, span.MsoHyperlinkFollowed
		{color:red;
		text-decoration:underline;
		text-underline:single;}
p
		{margin-right:0in;
		mso-margin-top-alt:auto;
		mso-margin-bottom-alt:auto;
		margin-left:0in;
		mso-pagination:widow-orphan;
		font-size:12.0pt;
		font-family:"Times New Roman";
		mso-fareast-font-family:"Times New Roman";}
@page Section1
		{size:8.5in 11.0in;
		margin:1.0in 1.25in 1.0in 1.25in;
		mso-header-margin:.5in;
		mso-footer-margin:.5in;
		mso-paper-source:0;}
div.Section1
		{page:Section1;}
-->
</style>
<!--[if gte mso 9]><xml>
 <o:shapedefaults v:ext="edit" spidmax="1027"/>
</xml><![endif]--><!--[if gte mso 9]><xml>

 <o:shapelayout v:ext="edit">
  <o:idmap v:ext="edit" data="1"/>
 </o:shapelayout></xml><![endif]-->
</head>

<body bgcolor=white background="BACK_tirol.gif" lang=EN-US link="#8080ff"
vlink=red style='tab-interval:.5in' title=VPN topmargin=0 leftmargin=0
bgproperties=FIXED alink="#00FF00">

<div class=Section1>

<p style='margin-right:.75in;tab-stops:8.5in'><![if !supportEmptyParas]> <![endif]><o:p></o:p></p>

<p style='margin-right:.75in;margin-left:.5in;tab-stops:320.25pt 8.5in'><b><span
lang=ES-CO style='font-size:14.0pt;mso-bidi-font-size:18.0pt;font-family:Arial;
color:blue;mso-ansi-language:ES-CO'>QUE ES UNA RED PRIVADA VIRTUAL? <o:p></o:p></span></b></p>

<p style='margin-top:0in;margin-right:.75in;margin-bottom:0in;margin-left:.5in;
margin-bottom:.0001pt;tab-stops:320.25pt 8.5in'><span lang=ES-CO
style='font-family:Arial;mso-ansi-language:ES-CO'><![if
!supportEmptyParas]> <![endif]><o:p></o:p></span></p>

<p style='margin-right:.75in;margin-top:0in;margin-left:.5in;tab-stops:8.5in'><span
lang=ES-CO style='font-size:11.0pt;mso-bidi-font-size:13.5pt;font-family:Arial;
color:black;mso-ansi-language:ES-CO'>Una Red Privada Virtual (VPN – <i>Virtual
Private Network</i>) es definida como un servicio de Red Inteligente (RI)
diseñado para suministrar a los usuarios, las características de una red
privada, nacional o internacional, utilizando los recursos de la Red Telefónica
Pública Conmutada (RTPC).<o:p></o:p></span></p>
```

```
<p style='margin-right:.75in;margin-top:0in;margin-left:.5in;tab-stops:8.5in'><span
lang=ES-CO style='font-size:11.0pt;mso-bidi-font-size:12.0pt;font-family:Arial;
mso-ansi-language:ES-CO'>El servicio utiliza las funciones y los recursos de la
red pública para suministrar a sus suscriptores una configuración privada
personalizada, con capacidades tales como grupos cerrados de usuarios, plan de
numeración privado, restricción de llamadas, entre otras.<o:p></o:p></span></p>

<p style='margin-right:.75in;margin-top:0in;margin-left:.5in;tab-stops:8.5in'><span
lang=ES-CO style='font-size:11.0pt;mso-bidi-font-size:12.0pt;font-family:Arial;
mso-ansi-language:ES-CO'>Una Red Privada Virtual además de utilizar la RTPC y
la RI, puede ser configurada utilizando la Red Digital de Servicios Integrados
(RDSI), la Red Mundial Pública Móvil (PLMN – <i>Public Land Mobile Network</i>)
y las redes privadas con las que ya cuenta el suscriptor del servicio.</span><span
lang=ES-CO style='font-size:11.0pt;mso-bidi-font-size:13.5pt;font-family:Arial;
color:black;mso-ansi-language:ES-CO'> <o:p></o:p></span></p>

<p class=MsoNormal style='margin-top:0in;margin-right:.75in;margin-bottom:0in;
margin-left:.5in;margin-bottom:.0001pt;text-align:justify;tab-stops:8.5in'><span
lang=ES-CO style='font-family:Arial;mso-bidi-font-family:"Times New Roman";
mso-ansi-language:ES-CO'><![if !supportEmptyParas]> <![endif]><o:p></o:p></span></p>

</div>

</body>

</html>
```

### *E.3.2. REFERENCIA VENTANAS ADICIONALES DEL TUTOR*

No se incluye el código de las ventanas adicionales del tutor, ya que el encabezado (<HEAD>) es similar al encabezo de la ventana “Qué es VPN?”, y el cuerpo (<BODY>) del código incluye la explicación de cada tema, la cual ya fue presentada en la monografía del trabajo de grado.

En la *Tabla E.1.* se presentan los botones de los demás temas del Tutor, los archivos que son ejecutados al presionar cada botón, y los archivos gráficos que se despliegan en cada una de las nuevas ventanas.

| VENTANA | CODIGO FUENTE | ARCHIVOS INCLUIDOS |
|---|---|---|
|  | vpntut2.html | No |
|  | vpntut3.html | No |
|  | vpntut4.html | No |

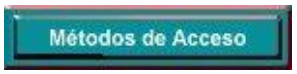
| | | |
|---|---|---|
|  | vpntut5.html | Vpntut5img1.gif<br>Vpntut5img2.gif |
|  | vpntut6.html | No |
|  | vpntut7.html | /vpntut7_archivos/image001.gif |
|  | vpntut8.html | vpntut8img1.gif<br>vpntut8img2.gif<br>vpntut8img3.gif<br>vpntut8img4.gif<br>/vpntut8_archivos/image001.gif |
|  | vpntut9.html | Vpntut9img6.gif<br>Vpntut9img3.gif<br>Vpntut9img5.gif<br>/vpntut9_archivos/image001.gif<br>/vpntut9_archivos/image003.gif |
|  | vpntut10.html | Vpntut10img1.gif<br>/vpntut10_archivos/image001.gif |
|  | vpntut11.html | /vpntut11_archivos/image001.gif<br>/vpntut11_archivos/image002.gif |
|  | vpntut12.html | /vpntut12_archivos/image001.gif<br>/vpntut12_archivos/image002.gif<br>/vpntut12_archivos/image003.gif |
|  | vpntut13.html | Vpntut13img2.gif<br>/vpntut13_archivos/image001.gif |
|  | vpntut14.html | /vpntut14_archivos/image001.gif<br>/vpntut14_archivos/image002.gif<br>/vpntut14_archivos/image003.gif<br>/vpntut14_archivos/image004.gif<br>/vpntut14_archivos/image005.gif |

*Tabla E.1. Referencia ventanas adicionales del tutor*

## E.4. AREA DE DEMOSTRACION

Al seleccionar el botón “Demo” en la *ventana principal del programa* se crea un vínculo con el archivo “vpndemo1.html” y aparece la ventana presentada en la *Fig. E.6*.

Esta ventana está compuesta por dos marcos. El primero es un marco fijo que se encuentra en la parte superior de la ventana y fue explicado en la sección E.3. El segundo marco se encuentra en la parte inferior de la ventana y permite acceder a las ventanas del Plan de Numeración Privado y de las demostraciones de cada uno de los cuatro tipos de llamadas que se pueden realizar en una VPN.

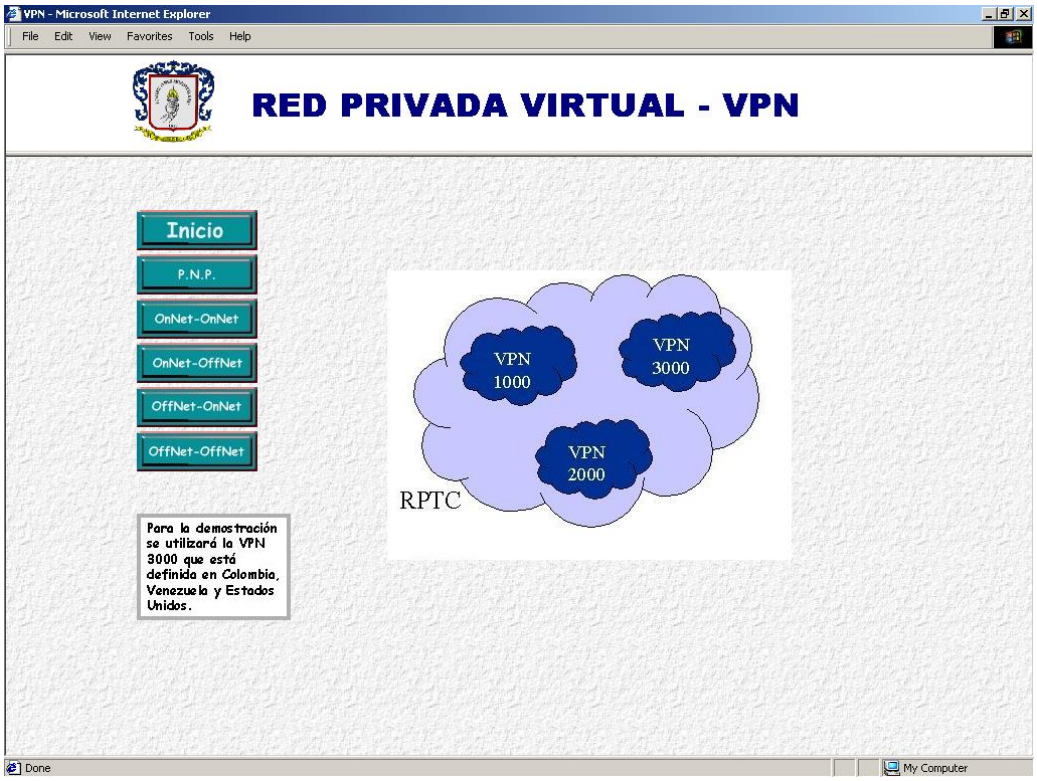



*Fig. E.6. Ventana principal de la demostración*

Archivo: ***vpndemo1.html***

```
<HTML>
<HEAD>
  <META NAME="Author" CONTENT="vpnmain">
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#8080FF" VLINK="#FF0000" title="VPN" topmargin=50 background="BACK_tirol.gif">


</BODY>
        <table width="750" border="0" align="CENTER" valign="TOP">
            <td width="100" align="LEFT">
                <a href="vpnmain.html" target="main"><img src="btninicio.jpg" width=120 height=40 alt="" border="0"></a>
```

```
                    <a href="vpndemo10.html" target="main"><img src="btnpnp.jpg" width=120
height=40 alt="" border="0"></a>
                    <a href="vpndemo11.html" target="main"><img src="btnonon.jpg" width=120
height=40 alt="" border="0"></a>
                    <a href="vpndemo20.html" target="main"><img src="btnonoff.jpg" width=120
height=40 alt="" border="0"></a>
                    <a href="vpndemo30.html" target="main"><img src="btnoffon.jpg" width=120
height=40 alt="" border="0"></a>
                    <a href="vpndemo40.html" target="main"><img src="btnoffoff.jpg" width=120
height=40 alt="" border="0"></a>
                    <br><br><img src="vpncuad2.jpg" width=153 height=106 alt="" border="0">
                </td>
                <td align="CENTER"><div align="center">
                    <img src="vpn2.jpg" width=402 height=288 alt="" border="0">
                </div></td>
        </table>
</HTML>
```

### *E.4.1. CODIGO VENTANA "P.N.P."*

Al presionar el botón P.N.P. en la *ventana principal de la demostración* se crea un vínculo con el archivo "vpndemo10.html" y aparece la ventana presentada en la Fig. E.7.

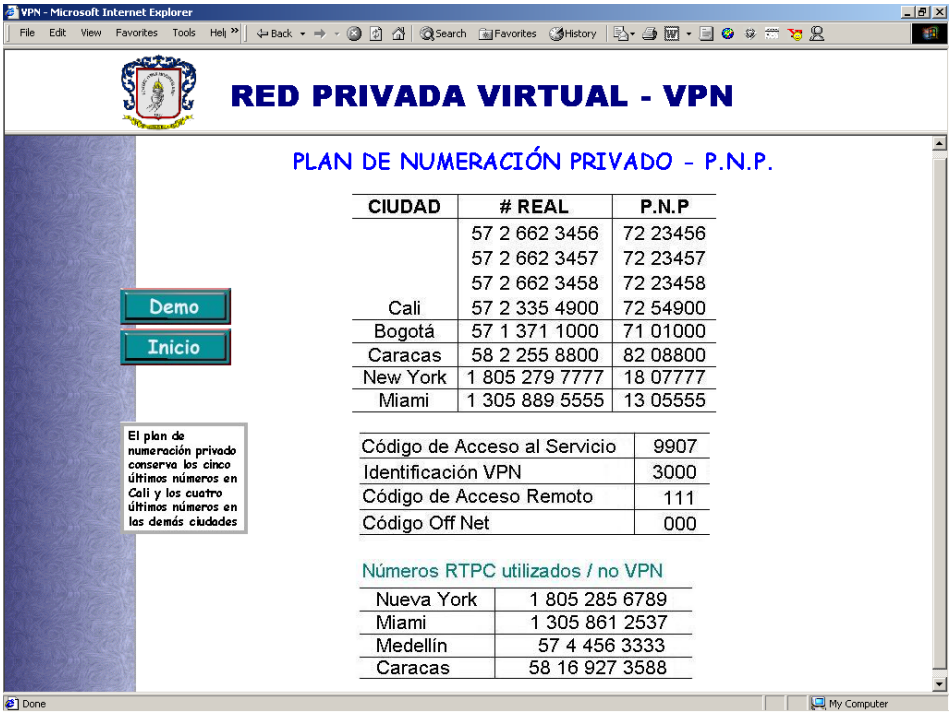




*Fig. E.7. Ventana del Plan de Numeración Privado*

Archivo: ***vpndemo10.html***

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
  <META NAME="Author" CONTENT="vpnmain">
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#8080FF" VLINK="#FF0000" title="VPN"
background="bluetxwhitebg.gif">

</BODY>
        <table width="760" border="0" align="CENTER" valign="TOP">
                <td width="100" align="LEFT">
                        <a href="vpndemo1.html" target="main"><img src="btndemo.jpg" width=120
height=40 alt="" border="0"></a>
                        <a href="vpnmain.html" target="main"><img src="btninicio.jpg" width=120 height=40
alt="" border="0"></a>
                        <br><br><br><p></p>
                        <img src="vpncuad1.jpg" width=138 height=122 alt="" border="0">
                </td>
                <td align="CENTER"><div align="center">
                        <font face="Comic Sans MS" size="5" color="#0000FF">
                                <b>PLAN DE NUMERACI&Oacute;N PRIVADO - P.N.P.</b>
                        </font><br><br>
                        <img src="vpn3a.jpg" width=394 height=238 alt="" border="0"><br><br>
                        <img src="vpn31b.jpg" width=380 height=120 alt="" border="0"><br><br>
                        <img src="vpn3b.jpg" width=385 height=130 alt="" border="0">
                </div></td>
        </table>
</HTML>
```

### *E.4.2. CODIGO VENTANA "ON-NET – ON-NET"*

Al presionar el botón OnNet – OnNet en la *ventana principal de la demostración* se crea un vínculo con el archivo "vpndemo11.html" y aparece la ventana presentada en la Fig. E.8.


Archivo: ***vpndemo11.html***

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
  <META NAME="Author" CONTENT="vpnmain">
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#8080FF" VLINK="#FF0000" title="VPN"
background="bluetxwhitebg.gif">

</BODY>
        <table width="800" border="0" align="CENTER" valign="TOP">
                <td width="100" align="left" valign="center">
                        <a href="vpndemo12.html" target="main"><img src="btnsiguiente.jpg" width=120
height=40 alt="" border="0"></a>
                        <a href="vpndemo1.html" target="main"><img src="btndemo.jpg" width=120
height=40 alt="" border="0"></a>
                        <a href="vpnmain.html" target="main"><img src="btninicio.jpg" width=120 height=40
alt="" border="0"></a>
                        <br><br><br>
```

```
                    </td>
                    <td align="CENTER" valign="TOP"><div align="center">
                            <font face="Comic Sans MS" size="+3" color="#0000FF">
                                    <b>OnNet (1807777) - OnNet (7101000)</b>
                            </font><br><br>
                            <img src="vpn11a.gif" width=574 height=430 alt="" border="0">
                    </div></td>
            </table>
</HTML>
```

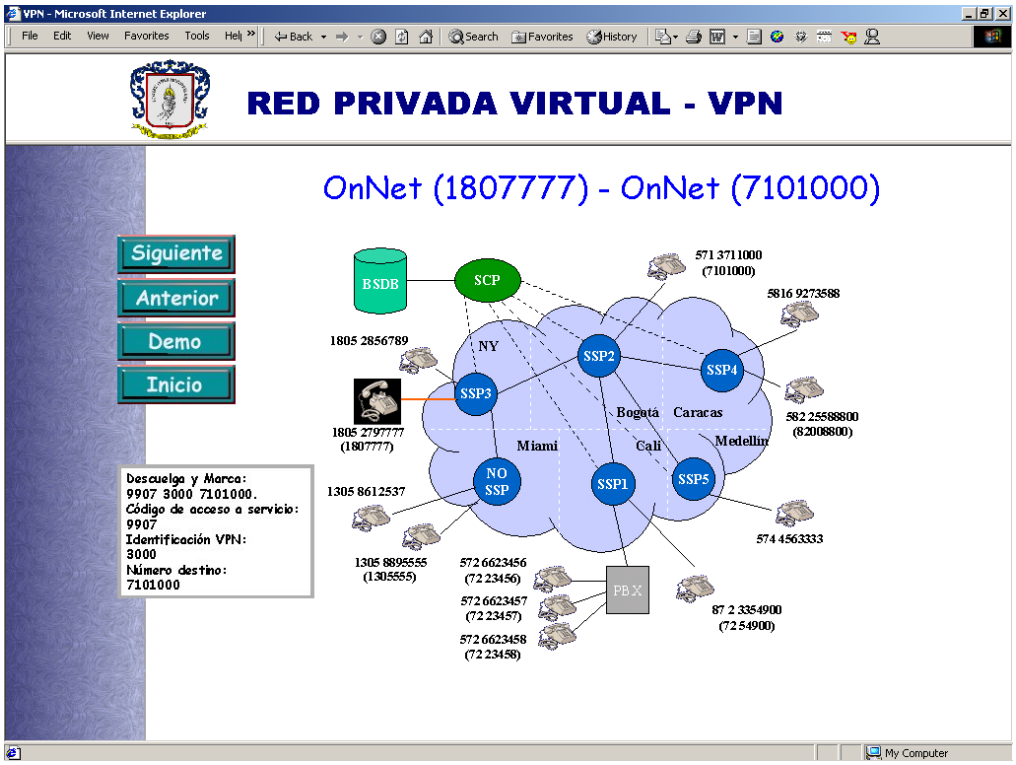



*Fig. E.8. Ventana Tipo de Llamada On-Net – On-Net*

En la *Tabla E.2.* se presentan los pasos de la Ejecución del Servicio de una llamada On-Net – On-Net, el archivo código fuente para cada una de las ventanas que presentan dichos pasos y los archivos gráficos que se despliegan en cada una de las ventanas.

| EJECUCIÓN DEL SERVICIO | CODIGO FUENTE | ARCHIVOS INCLUIDOS |
|---|---|---|
| Descuelga y marca número destino. | vpndemo12.html | Vpncuad12.jpg<br>Vpn12a.gif |
| SSP identifica llamada VPN y solicita información al SCP. | vpndemo13.html | Vpncuad13.jpg<br>Vpn13a.gif |

| | | |
|---|---|---|
| SCP consulta la base de datos. | vpndemo14.html | Vpncuad14.jpg<br>Vpn14a.gif |
| La Base de datos devuelve la información al SCP. | vpndemo15.html | Vpncuad15.jpg<br>Vpn15a.gif |
| SCP envía respuesta al SSP. | vpndemo16.html | Vpncuad16.jpg<br>Vpn16a.gif |
| SSP enruta la llamada y establece la comunicación. | vpndemo17.html | Vpncuad17.jpg<br>Vpn17a.gif |
| Usuario origen cuelga la llamada. SSP envia registro de llamada al SCP. | vpndemo18.html | Vpncuad18.jpg<br>Vpn18a.gif |

*Tabla E.2. Referencias ejecución del servicio en llamadas OnNet – OnNet.*

### *E.4.3. CODIGO VENTANA "ON-NET – OFF-NET"*

Al presionar el botón OnNet – OffNet en la *ventana principal de la demostración* se crea un vínculo con el archivo "vpndemo20.html" y aparece la ventana presentada en la Fig. E.9.


Archivo: ***vpndemo20.html***

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
  <META NAME="Author" CONTENT="vpnmain">
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#8080FF" VLINK="#FF0000" title="VPN"
background="bluetxwhitebg.gif">

</BODY>
        <table width="830" border="0" align="CENTER" valign="TOP">
                <td width="100" align="LEFT" valign="CENTER">
                        <a href="vpndemo21.html" target="main"><img src="btnsiguiente.jpg" width=120
height=40 alt="" border="0"></a>
                        <a href="vpndemo1.html" target="main"><img src="btndemo.jpg" width=120
height=40 alt="" border="0"></a>
                        <a href="vpnmain.html" target="main"><img src="btninicio.jpg" width=120 height=40
alt="" border="0"></a>
                        <br><br><br>

                </td>
                <td align="CENTER" valign="TOP"><div align="center">
                        <font face="Comic Sans MS" size="+3" color="#0000FF">
                                OnNet (7223456) - OffNet (574 4563333)
                        </font><br><br><br>
                        <img src="vpn11a.gif" width=574 height=430 alt="" border="0">
                </div></td>
        </table>
</HTML>
```

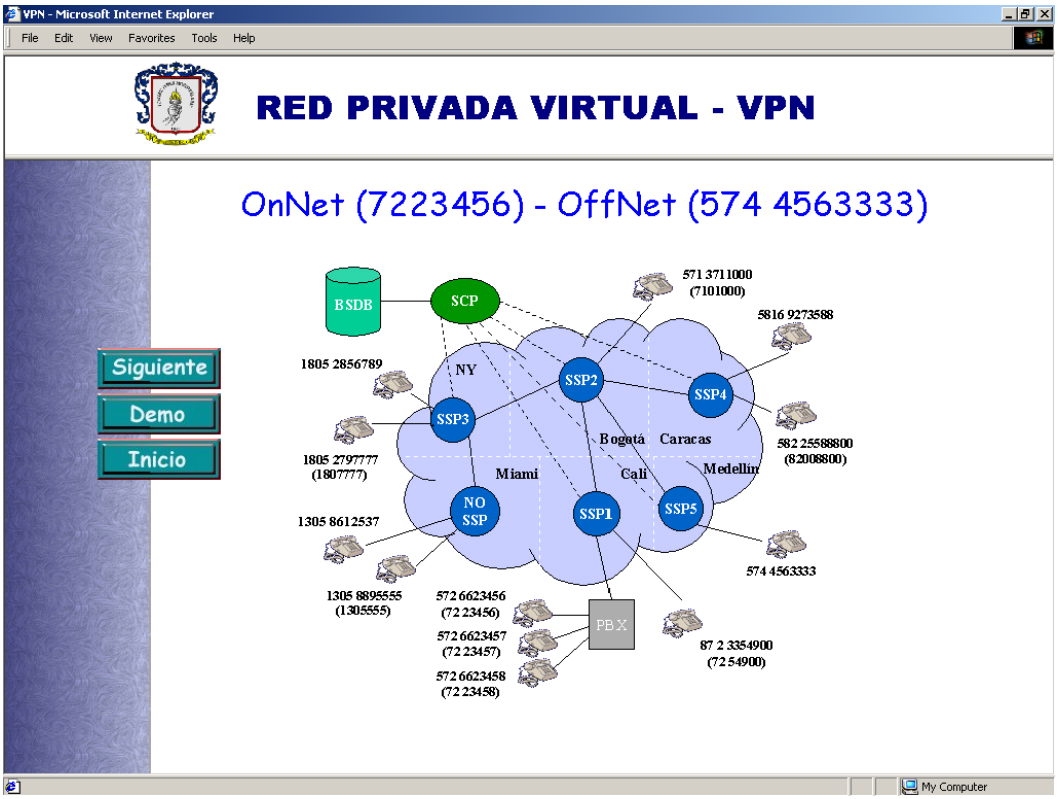



*Fig. E.9. Ventana Tipo de Llamada On-Net – Off-Net*

En la *Tabla E.3.* se presentan los pasos de la Ejecución del Servicio de una llamada On-Net – Off-Net, el archivo código fuente para cada una de las ventanas que presentan dichos pasos y los archivos gráficos que se despliegan en cada una de las ventanas.

| EJECUCIÓN DEL SERVICIO | CODIGO FUENTE | ARCHIVOS INCLUIDOS |
|---|---|---|
| Descuelga y marca número de salida a la red pública. | vpndemo21.html | Vpncuad21.jpg<br>Vpn21.gif |
| Recibe tono de la red pública y marca Código Off-Net. | Vpndemo22.html | Vpncuad22.jpg<br>Vpn22.gif |
| SSP identifica llamada VPN y código Off-Net. Solicita información al SCP. | Vpndemo23.html | Vpncuad23.jpg<br>Vpn23.gif |
| SCP consulta la base de datos para determinar si usuario tiene autorización llamadas Off-Net. | Vpndemo24.html | Vpncuad24.jpg<br>Vpn24.gif |

| | | |
|---|---|---|
| La Base de datos devuelve la respuesta al SCP. | Vpndemo25.html | Vpncuad25.jpg<br>Vpn25.gif |
| SCP determina que es posible realizar la llamada y solicita número destino al SSP. | Vpndemo26.html | Vpncuad26.jpg<br>Vpn26.gif |
| SSP envia anuncio solicitando número destino. Abonado marca el número. | Vpndemo27.html | Vpncuad27.jpg<br>Vpn27.gif |
| SSP reconoce los dígitos y los envía al SCP. | Vpndemo28.html | Vpncuad28.jpg<br>Vpn23.gif |
| SCP detecta llamada larga distancia y consulta base de datos para definir procesamiento. | Vpndemo29.html | Vpncuad29.jpg<br>Vpn24.gif |
| La Base de datos devuelve la respuesta al SCP. | Vpndemo210.html | Vpncuad15.jpg<br>Vpn25.gif |
| SCP envía respuesta al SSP con información de procesamiento de llamada. | Vpndemo211.html | Vpncuad211.jpg<br>Vpn26.gif |
| SSP enruta la llamada y establece la comunicación. | Vpndemo212.html | Vpncuad212.jpg<br>Vpn28.gif |
| Usuario origen cuelga la llamada. SSP envia registro de llamada al SCP. | Vpndemo213.html | Vpncuad213.jpg<br>Vpn29.gif |

*Tabla E.3. Referencias ejecución del servicio en llamadas OnNet – OffNet.*

### *E.4.4. CODIGO VENTANA "OFF-NET – ON-NET"*


Al presionar el botón OffNet – OnNet en la *ventana principal de la demostración* se crea un vínculo con el archivo "vpndemo30.html" y aparece la ventana presentada en la Fig. *E.10*.

En la *Tabla E.4.* se presentan los pasos de la Ejecución del Servicio de una llamada Off-Net – On-Net, el archivo código fuente para cada una de las ventanas que presentan dichos pasos y los archivos gráficos que se despliegan en cada una de las ventanas.

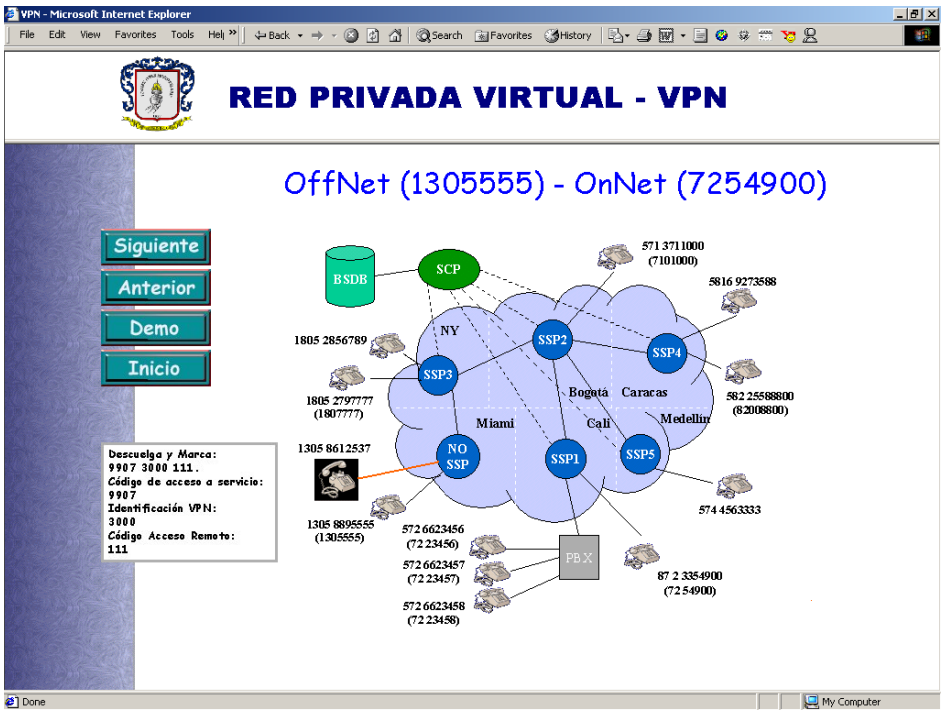



*Fig. E.10. Ventana Tipo de Llamada Off-Net – On-Net*

Archivo: ***vpndemo30.html***

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
  <META NAME="Author" CONTENT="vpnmain">
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#8080FF" VLINK="#FF0000" title="VPN"
background="bluetxwhitebg.gif">

</BODY>
        <table width="850" border="0" align="CENTER" valign="TOP">
                <td width="100" align="LEFT" valign="center">
                        <a href="vpndemo31.html" target="main"><img src="btnsiguiente.jpg" width=120
height=40 alt="" border="0"></a>
                        <a href="vpndemo1.html" target="main"><img src="btndemo.jpg" width=120
height=40 alt="" border="0"></a>
                        <a href="vpnmain.html" target="main"><img src="btninicio.jpg" width=120 height=40
alt="" border="0"></a>
                        <br><br><br>

                </td>
                <td align="CENTER" valign="TOP"><div align="center">
                        <font face="Comic Sans MS" size="+3" color="#0000FF">
                                OffNet (1305555) - OnNet (7254900)
                        </font><br><br>
                        <img src="vpn11a.gif" width=574 height=430 alt="" border="0">
                </div></td>
        </table>
</HTML>
```

| EJECUCIÓN DEL SERVICIO | CODIGO FUENTE | ARCHIVOS INCLUIDOS |
|---|---|---|
| Descuelga y marca número de acceso remoto. | Vpndemo31.html | Vpncuad31.jpg<br>Vpn31a.gif |
| No SSP identifica llamada VPN y la entrega al SSP más cercano | Vpndemo32.html | Vpncuad32.jpg<br>Vpn32a.gif |
| SSP reconoce Código de Acceso Remoto. Solicita información al SCP. | Vpndemo33.html | Vpncuad33.jpg<br>Vpn33q.gif |
| SCP determina que es posible realizar la llamada y solicita al SSP PNP y PIN del abonado. | Vpndemo36.html | Vpncuad36.jpg<br>Vpn36a.gif |
| SSP envia anuncio solicitando número PNP y PIN. Abonado marca los números solicitados. | Vpndemo37.html | Vpncuad37.jpg<br>Vpn37a.gif |
| SSP envía los números PNP y PIN al SCP y solicita información de procesamiento de llamada. | Vpndemo38.html | Vpncuad38.jpg<br>Vpn33q.gif |
| SCP consulta base de datos para definir si abonado es miembro de la VPN y si puede realizar llamadas de acceso remoto. | Vpndemo39.html | Vpncuad39.jpg<br>Vpn34a.gif |
| La Base de datos devuelve la respuesta al SCP. | Vpndemo310.html | Vpncuad15.jpg<br>Vpn35a.gif |
| SCP determina que es posible realizar la llamada y solicita al SSP número destino | Vpndemo311.html | Vpncuad311.jpg<br>Vpn311a.gif |
| SSP envia anuncio solicitando número destino. Abonado marca número destino. | Vpndemo312.html | Vpncuad312.jpg<br>Vpn312a.gif |
| SSP envía el número al SCP y solicita información de procesamiento de llamada. | Vpndemo313.html | Vpncuad313.jpg<br>Vpn313a.gif |
| SCP consulta la base de datos para determinar si completa la llamada. | Vpndemo314.html | Vpncuad14.jpg<br>Vpn34a.gif |
| La Base de datos devuelve la respuesta al SCP. | Vpndemo315.html | Vpncuad15.jpg<br>Vpn35a.gif |

| | | |
|---|---|---|
| SCP envía respuesta al SSP con información de procesamiento de llamada. | Vpndemo316.html | Vpncuad16.jpg<br>Vpn311a.gif |
| SSP enruta la llamada y establece la comunicación. | Vpndemo317.html | Vpncuad17.jpg<br>Vpn38a.gif |
| Usuario origen cuelga la llamada. SSP envia registro de llamada al SCP. | Vpndemo318.html | Vpncuad18.jpg<br>Vpn39a.gif |

*Tabla E.4. Referencias ejecución del servicio en llamadas OnNet – OffNet.*

### *E.4.5. CODIGO VENTANA "OFF-NET – OFF-NET"*

Al presionar el botón OffNet – OffNet en la *ventana principal de la demostración* se crea un vínculo con el archivo "vpndemo40.html" y aparece la ventana presentada en la *Fig. E.11.*

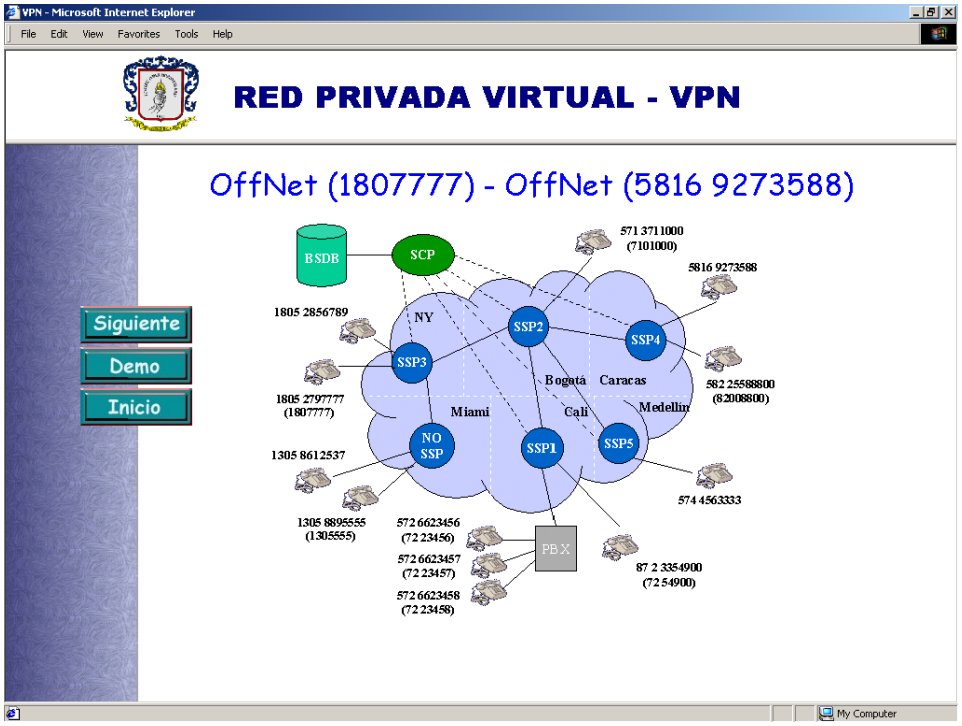




*Fig. E.11. Ventana Tipo de Llamada Off-Net – Off-Net*

Archivo: ***vpndemo40.html***

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
```

```
<HEAD>
  <META NAME="Author" CONTENT="vpnmain">
</HEAD>
<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#8080FF" VLINK="#FF0000" title="VPN"
background="bluetxwhitebg.gif">

</BODY>
        <table width="850" border="0" align="CENTER" valign="TOP">
                <td width="100" align="LEFT" valign="center">
                        <a href="vpndemo41.html" target="main"><img src="btnsiguiente.jpg" width=120
height=40 alt="" border="0"></a>
                        <a href="vpndemo1.html" target="main"><img src="btndemo.jpg" width=120
height=40 alt="" border="0"></a>
                        <a href="vpnmain.html" target="main"><img src="btninicio.jpg" width=120 height=40
alt="" border="0"></a>
                        <br><br><br>

                </td>
                <td align="CENTER" valign="TOP"><div align="center">
                        <font face="Comic Sans MS" size="+3" color="#0000FF">
                                OffNet (1807777) - OffNet (5816 9273588)
                        </font><br><br>
                        <img src="vpn11a.gif" width=574 height=430 alt="" border="0">
                </div></td>
        </table>
</HTML>
```

En la *Tabla E.5.* se presentan los pasos de la Ejecución del Servicio de una llamada Off-Net – Off-Net, el archivo código fuente para cada una de las ventanas que presentan dichos pasos y los archivos gráficos que se despliegan en cada una de las ventanas.

| EJECUCIÓN DEL SERVICIO | CODIGO FUENTE | ARCHIVOS INCLUIDOS |
|---|---|---|
| Descuelga y marca número de acceso remoto. | Vpndemo41.html | Vpncuad31.jpg<br>Vpn41.gif |
| SSP reconoce Código de Acceso Remoto. Solicita información al SCP. | Vpndemo42.html | Vpncuad33.jpg<br>Vpn42.gif |
| SCP determina que es posible realizar la llamada y solicita al SSP PNP y PIN del abonado. | Vpndemo43.html | Vpncuad36.jpg<br>Vpn43.gif |
| SSP envia anuncio solicitando número PNP y PIN. Abonado marca los números solicitados. | Vpndemo44.html | Vpncuad44.jpg<br>Vpn44.gif |
| SSP envía los números PNP y PIN al SCP y solicita información de procesamiento de llamada. | Vpndemo45.html | Vpncuad38.jpg<br>Vpn42.gif |
| SCP consulta base de datos para definir si abonado es miembro de la VPN y si puede realizar llamadas de acceso remoto. | Vpndemo46.html | Vpncuad39.jpg<br>Vpn46.gif |
| La Base de datos devuelve la respuesta al SCP. | Vpndemo47.html | Vpncuad15.jpg<br>Vpn47.gif |

| | | |
|---|---|---|
| SCP determina que es posible realizar la llamada y solicita al SSP número destino | Vpndemo48.html | Vpncuad311.jpg<br>Vpn48.gif |
| SSP envia anuncio solicitando número destino. Abonado marca Código Off-Net. | Vpndemo49.html | Vpncuad49.jpg<br>Vpn49.gif |
| SSP reconoce Código Off-Net y pregunta al SCP si tiene autorización para llamadas Off-Net. | Vpndemo410.html | Vpncuad410.jpg<br>Vpn410.gif |
| SCP consulta la base de datos para determinar si el abonado tiene autorización para llamadas Off-Net. | Vpndemo411.html | Vpncuad24.jpg<br>Vpn46.gif |
| La Base de datos devuelve la respuesta al SCP. | Vpndemo412.html | Vpncuad15.jpg<br>Vpn47.gif |
| SCP determina que abonado tiene autorización para realizar llamadas Off-Net y le solicita al SSP número destino. | Vpndemo413.html | Vpncuad413.jpg<br>Vpn48.gif |
| SSP envia anuncio solicitando número destino. Abonado marca número destino. | Vpndemo414.html | Vpncuad414.jpg<br>Vpn49.gif |
| SSP envía numero destino al SCP y solicita información de procesamiento de llamada. | Vpndemo415.html | Vpncuad313.jpg<br>Vpn410.gif |
| SCP consulta la base de datos para determinar si termina la llamada. | Vpndemo416.html | Vpncuad14.jpg<br>Vpn46.gif |
| La Base de datos devuelve la respuesta al SCP. | Vpndemo417.html | Vpncuad15.jpg<br>Vpn47.gif |
| SCP envía respuesta al SSP con información de procesamiento de llamada. | Vpndemo418.html | Vpncuad16.jpg<br>Vpn48.gif |
| SSP enruta la llamada y establece la comunicación. | Vpndemo419.html | Vpncuad17.jpg<br>Vpn411a.gif |
| Usuario origen cuelga la llamada. SSP envia registro de llamada al SCP. | Vpndemo420.html | Vpncuad18.jpg<br>Vpn412.gif |

*Tabla E.5. Referencias ejecución del servicio en llamadas OffNet – OffNet.*