UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERIA

SERVICIOS DE COMUNICACIONES AVANZADOS EN SISTEMAS INALÁMBRICOS DE PRÓXIMA GENERACIÓN CON TECNOLOGÍA MVPN

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A:

DANIEL ALEJANDRO PATIÑO ROA

ASESOR: ING. JOSÉ ARTURO LANDEROS AYALA

CIUDAD UNIVERSITARIA 2004

ÍNDICE

ESTRUCTURA DE LA TESIS

Las redes privadas virtuales móviles tienen un gran potencial para mejorar en forma significativa la productividad de las empresas y además pueden dar a los proveedores de servicio ganancias adicionales, sin embargo, debido la rápida evolución de las tecnologías inalámbricas, en México, los especialistas en esta área son pocos.

Es por ello que con este trabajo de tesis se pretende brindar a todo aquel lector interesado en el tema, una referencia con los conocimientos y análisis necesarios de esta tecnología.

Con este objetivo, el trabajo de tesis está organizado de la siguiente manera:

El capítulo 1 proporciona una introducción a lo que son las aplicaciones comerciales de la tecnología MVPN.

El capítulo 2 trata sobre los tópicos más relevantes en las redes y comunicaciones de datos, tales como las tecnologías de *tunneling* y etiquetado, y tecnologías para la seguridad.

El capítulo 3 proporciona una revisión de las interfaces de radio fundamentales y detalles de los principales sistemas celulares.

El capítulo 4 proporciona información de los servicios inalámbricos de conmutación de circuitos y paquetes en los sistemas de segunda y tercera generación.

En el capítulo 5 entramos de lleno a los fundamentos de MVPN, proporcionando información de las taxonomías y las tecnologías de VPN.

El capítulo 6 entra más en detalle en las cuestiones de direccionamiento y seguridad en las redes inalámbricas; también toca el tema de roaming.

El capítulo 7 se enfoca en los servicios MVPN proporcionados en los sistemas GSM, UMTS y CDMA2000.

El capítulo 8 brinda una explicación de los cuerpos y procesos de estandarización, así como de los principales estándares para los sistemas inalámbricos.

El capítulo 9 analiza brevemente los principales tipos de equipos involucrados en las MVPNs.

El capítulo 10 proporciona un panorama de los principales operadores y servicios inalámbricos de datos en México.

El capítulo 11 analiza los servicios móviles que se proporcionarán en los sistemas inalámbricos de tercera generación.

Finalmente, en el capítulo 12 se proporcionan las conclusiones que se obtuvieron en la realización de este trabajo.

De manera adicional, se incluye una sección con los principales acrónimos empleados en la industria de las redes de datos, y una sección con la bibliografía utilizada en la elaboración de esta tesis.

CAPÍTULO 1

INTRODUCCIÓN A MVPN

Los recargos y las rentas contraídas por el usuario, la competencia basada en el costo, y el enfoque en la retención del cliente son signos de que la telefonía móvil probablemente no muestre un crecimiento significativo en sus ingresos -comparable al disfrutado durante la década pasada- durante los próximos años. Los proveedores de servicio por lo tanto están forzados a buscar maneras innovadoras para invertir en nuevas tecnologías, que puedan llegar a ser los próximos habilitadores del crecimiento. Por ejemplo, en años recientes la mayor parte de la atención ha sido puesta a los servicios de Internet móvil, los cuales se cree, poseen un potencial significativo de generación de ingresos para los proveedores de servicio.

Esta creencia fue en parte responsable de la inversión masiva en el espectro para las tecnologías de radio acceso de la nueva generación, con el potencial para soportar velocidades de transferencia de datos más altas para servicios de Internet móvil, comúnmente conocidas como la tercera generación (3G). Más recientemente, los proveedores de servicio han reconocido que el acceso a Internet en sí no puede justificar las inversiones significativas que hicieron. Como consiguiente, han vuelto a la búsqueda de modos innovadores de generar ingresos usando las nuevas capacidades de servicio ofrecidas por el despliegue de sistemas basados en paquetes de datos tales como GPRS, UMTS, o CDMA2000. Hasta ahora, la clase más prometedora de servicios mezcla las capacidades de la voz móvil tradicional y los nuevos servicios basados en la localización y los servicios de mensajería. Tales sistemas deben proporcionar a los usuarios acceso personalizado y confiable a redes privadas donde ellos pueden pertenecer a comunidades de interés tanto de negocios como de entretenimiento, como redes corporativas o grupos de mensajería instantánea. El valor de tales redes para los clientes parece estar estrictamente relacionado a:

- Garantizar el acceso seguro a la red con un funcionamiento fiable.
- Asegurarse que el acceso a tales redes es exclusivo para miembros con permisos apropiados.

Estos requerimientos de servicio están obligando a los proveedores de servicio a utilizar redes privadas virtuales móviles (MVPN), que definimos como la emulación de redes de datos privadas seguras sobre instalaciones móviles e inalámbricas compartidas generalmente inseguras. Esta definición está basada en varias características:

- La movilidad de los datos de usuario está definida como la conectividad ininterrumpida o la capacidad para permanecer conectado y comunicarse a una red de datos posiblemente remota mientras que cambia el medio de acceso a la red o los puntos de conexión.
- El servicio de MVPN es proporcionado generalmente sobre medios inalámbricos.
- El término "instalaciones inalámbricas" se refiere a generaciones actuales y futuras de sistemas celulares como GSM, CDMA2000, TDMA y UMTS, redes inalámbricas como LANs Inalámbricas (WLANs), y sistemas inalámbricos de paquetes de datos como GPRS.

Una visualización simple de MVPN puede ser encontrada en la figura 1.1, que muestra túneles seguros que conectan un dispositivo móvil con una variedad de redes privadas sobre múltiples redes públicas compartidas, como el Internet y un sistema celular inalámbrico arbitrario o una red WLAN.

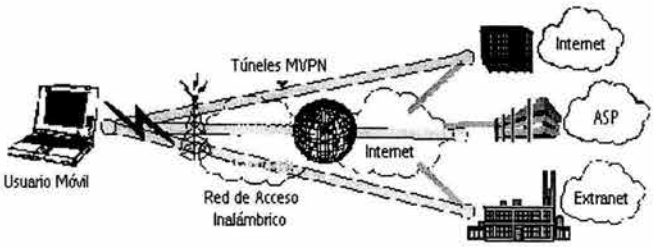


Figura 1.1 Ejemplo de una red privada virtual móvil

1.1 La Era de la Movilidad Generalizada

Somos afortunados de atestiguar el principio de una era de movilidad generalizada, cuando el acceso a los recursos de información no estará determinado por la disponibilidad o el tipo de tecnología de acceso de red, sino más bien por factores como el deseo, la necesidad, y la habilidad para obtener información o servicios.

La información y los servicios serán solicitados y accedidos no sólo por individuos sino también por entidades físicas y virtuales tales como procesos automatizados de fabricación, máquinas vendedoras inteligentes, dispositivos que colectan información como medidas de utilidad, cajas registradoras inteligentes, estaciones de cobro en carreteras, sistemas de seguridad, y equipo médico. Las características de servicio de acceso a redes remotas no serán dependientes de la posición geográfica, sino más bien de la existencia de roaming apropiado y de acuerdos de servicio entre las redes de datos local y visitada, permitiendo la recuperación del perfil de servicio local dentro de las redes exteriores. Cuando los acuerdos apropiados toman lugar, las entidades o individuos móviles serán capaces de recibir servicios idénticos a aquellos disponibles en su ambiente de red local mientras andan en redes exteriores.

1.1.1 Conductores de la Movilidad Generalizada

¿Qué conduce a la necesidad de la movilidad generalizada, o a la conectividad ininterrumpida sobre demanda permanentemente disponible? Los conductores más importantes son las ganancias de productividad vía el avance de la tecnología IT (*Information Technology*), el ascenso del Internet, la velocidad creciente de la evolución de los dispositivos móviles, la cobertura celular y no celular de red, y la caída en picada de los costos del servicio inalámbrico celular.

1.1.1.1 Incremento en la Productividad

El papel cambiante de la tecnología de la información en corporaciones e instituciones en todo el mundo fue responsable de las principales ganancias de productividad en el lugar de trabajo durante la década pasada. Esto fue, desde luego, acompañado por el ascenso del Internet, que juntó masas de información y unió comunidades de intereses dispares por todo el mundo. Sin embargo, la computación masiva también trajo consigo una dependencia total de los recursos computacionales y de información, a menudo disponibles sólo en un número limitado de sitios seleccionados, como oficinas centrales corporativas o centros de datos. Los nuevos servicios disponibles, tan indispensables para los usuarios en sus oficinas, son cada vez más solicitados desde posiciones remotas como oficinas en casa, sitios de clientes, etc. Estas necesidades por su parte conducen a la demanda de servicio de roaming global y de acceso de red remoto ubicuo[1]. La incertidumbre de la posición donde el usuario requerirá el acceso impone la necesidad de conectividad móvil (dinámica) privada hacia la red local para estar disponible en todas partes de una área amplia (acceso ubicuo).

[1] Ubicuo: Que se encuentra a un mismo tiempo en todas partes.

1.1.1.2 Evolución de los Dispositivos Móviles

Es difícil subestimar el papel de las comunicaciones personales y de los dispositivos informáticos - como Asistentes Personales Digitales (PDAs), teléfonos móviles inteligentes, y computadoras portátiles (*laptops*), que abandonan la fábrica con múltiples interfaces inalámbricas incorporadas- en la evolución de las comunicaciones móviles. La caída a plomo de los precios, el aumento de la amigabilidad hacia el usuario, y la riqueza de características hacen ahora a estos dispositivos no sólo cada vez más aprovechables y deseables por grupos crecientes de profesionales móviles, sino muchas veces indispensables.

El último ejemplo de tales dispositivos es un montón de PDAs y de teléfonos móviles basados en PDAs que parecen computadoras de escritorio de una generación más temprana en cuanto a la memoria y el poder de procesamiento. Los fabricantes como HP, Toshiba, Sony, Nokia, y Palm conducen esta tendencia. Estas maravillas pequeñas, de poca potencia pueden soportar múltiples modos de comunicaciones inalámbricas (Infrarrojo, Bluetooth, WLAN, y GPRS o CDMA2000), clientes VPN, y un micronavegador empaquetado con el sistema operativo. Esta combinación de características los hace ideales para el acceso seguro a redes corporativas remotas.

1.1.1.3 Avances en los Sistemas Celulares

El tercer conductor hacia la movilidad generalizada es el rápido establecimiento y consolidación de los sistemas celulares que resultan en una cobertura inalámbrica de área amplia cada vez más uniforme y los servicios cada vez más baratos. La cobertura celular ha llegado a ser tan extensa y barata que está conduciendo otras tecnologías fuera de negocios. Esto dio lugar a una situación donde los sistemas inalámbricos de acceso de área amplia alternativos, tales como el satélite, habían sido juzgados innecesarios por un público de pago cuya baja demanda los forzó a la bancarrota o hacia mercados más convenientes. Buenos ejemplos de ésos son los ahora difuntos operadores de satélites Iridium e Inmarsat, que fueron forzados a especializarse en la navegación marítima. De hecho, el servicio celular en algunas áreas, extendiéndose desde mercados europeos y japoneses altamente saturados hasta los países en desarrollo que carecen totalmente de infraestructura de línea terrestre se hizo tan ubicuo y económico que comenzó a sustituir el servicio de teléfono de línea terrestre.

1.1.2 Estilos de Vida y Lugares de Trabajo Móviles

Estos y otros avances tecnológicos explican el ascenso de la movilidad generalizada, que por su parte sigue trayendo cambios profundos en el curso de nuestra sociedad, en el modo de vivir, y en el lugar de trabajo en como nos comunicamos, como recibimos información y noticias, y como tratamos la información. Los años 90 y los primeros años del nuevo milenio fueron esenciales en la formación de la tecnología móvil. La manera que nuestra sociedad ahora utiliza redes celulares inalámbricas y, específicamente, las tecnologías inalámbricas de datos tal como el servicio de mensajes cortos (SMS) es el mejor indicador de estos cambios. Desde adolescentes que usan SMS para comunicaciones "secretas" hasta profesionales en Japón que usan dispositivos de *i-mode* para servicios bancarios, los usuarios de datos inalámbricos se acercan rápido a usuarios de voz en número e ingresos generados. De hecho, se espera que los datos inalámbricos se conviertan en la principal fuerza motriz de las telecomunicaciones.

1.2 Antecedentes de VPN

Las Redes Privadas Virtuales (VPN) fueron originalmente definidas y aplicadas en comunicaciones de voz. Durante años, las compañías telefónicas entregaron servicios de voz utilizando lo que ellos llamaron "Redes Privadas Virtuales," a pesar de que no existían. De hecho, hoy en día cualquier grupo de usuarios definido por software provisionado sobre cualquier medio físico es considerado VPN por las compañías telefónicas.

Con el ascenso de las comunicaciones de datos, el término VPN fue adoptado por industria de las redes de datos y se le ha dado un nuevo y más exacto significado. Las llamadas VPNs de datos tradicionales fueron creadas inicialmente con tecnologías dedicadas de la capa de enlace tales como enlaces PVC (*Permanent Virtual Cicuit*) de Frame Relay o VC (*Virtual Circuit*) de ATM, establecidos entre terminales individuales o redes. En aproximadamente 10 años después del advenimiento de estas tecnologías, las VPNs de datos han sido implementadas típicamente de esta manera con el objetivo principal de sustituir redes privadas menos eficientes basadas en instalaciones dedicadas arrendadas de punto a punto.

Como el uso de redes públicas basadas en el protocolo de Internet (IP) tales como el Internet rápidamente ganaron el interés del público y la aceptación del mercado, una nueva generación de servicios VPN basados en tecnologías de la capa de red ha sido introducida en el mercado. Como en las VPNs tradicionales, las IP VPNs utilizan instalaciones compartidas para emular redes privadas y entregas confiables, y servicios seguros para los usuarios finales. Durante las pruebas iniciales de la tecnología IP VPN, los fabricantes de equipo y las organizaciones de estándarización como el IETF[2] propusieron varias técnicas de encapsulación y codificación en un esfuerzo por entregar las ventajas prometidas de los costos y la reducción de la complejidad, sin comprometer los requerimientos de seguridad que muchos clientes potenciales de VPN tienen. Los mecanismos propietarios como *Layer Two Forwarding* (L2F) ideado por Cisco y el protocolo de *tunneling* punto a punto (PPTP) introducido por Microsoft incluyen tales ejemplos.

Últimamente, la industria se decidió por el uso de tecnologías estándar como IPSec, L2TP, GRE (*Generic Routing Encapsulation*), y MPLS (*Multi-Protocol Label Switching*), entre otras. Métodos comunes de autenticación y de contabilidad en gran parte basados en el protocolo RADIUS antes definido para satisfacer la demanda para la administración de suscriptores centralizados en la industria remota de dial-up fueron escogidos y estandarizados para el uso con IP VPN. Las VPNs móviles inalámbricas son los últimos miembros de este grupo.

1.3 El Caso Comercial de MVPN

VPN móvil es un servicio de datos que puede ser proporcionado dentro de cualquier sistema o red que soporte acceso certificado (generalmente inalámbrico) a una red de datos. Vamos a ver el caso comercial de MVPN como una combinación de VPN y casos de negocios de datos inalámbricos y analizamos su valor para los operadores, en la forma de ingresos y mercados potenciales, y para los clientes, como un vehículo para entregar nuevos servicios y funcionalidades. Veremos el mercado de MVPN desde las perspectivas de los proveedores de servicio y de los clientes y evalúamos la proposición de beneficios y valores de MVPN para segmentos específicos de clientes y proveedores.

1.3.1 Moviéndose Hacia MVPN

El Internet, ahora accesible desde casi cualquier sitio donde las líneas telefónicas, el servicio celular, o los servicios de satélite están disponibles, ha cambiado fundamentalmente el modo en que nos comunicamos y tenemos acceso a la información y a los servicios. El Internet llega rápidamente a ser el medio de elección para las comunicaciones de negocios. Sin embargo, esta es una red pública compartida, mientras que las comunicaciones comerciales requieren instalaciones privadas seguras. Esto significa que si el Internet es usado para comunicaciones privadas, la información del usuario transportada sobre ella debe ser de alguna manera asegurada.

Series de tecnologías de redes y seguridad fueron ideadas en respuesta a este requerimiento y llegaron a ser rápidamente los métodos más populares para conducir comunicaciones privadas sobre Internet, o cualquier otra red IP compartida. Estas fueron conocidas como tecnologías IP VPN. En el curso del desarrollo de las redes inalámbricas, la exigencia de movilidad se hizo cada vez más rigurosa en el aprovisionamiento de servicios IP VPN. Esta investigación fomentó, los

[2] IETF: Internet Engineering Task Force; ver Capítulo 8.

esfuerzos de estándarización, y el desarrollo de tecnologías de MVPN en la industria. Hoy, los operadores preparan proyectos y arquitecturas comerciales para soportar una variedad de ofrecimientos MVPN para servir a las necesidades de sus clientes comerciales e institucionales.

1.3.2 Comunicaciones Inalámbricas con MVPN

Para los operadores inalámbricos que desplegaron los sistemas celulares de última generación basados en conmutación de paquetes de datos tales como GPRS y CDMA2000, y especialmente para aquellos clientes de negocios que concentran una porción significativa de su corriente de renta, la importancia de los servicios basados en tecnologías MVPN es difícil de subestimar. Para los operadores, MVPN no es sólo una de las tecnologías requeridas para el acceso de red privado de los clientes comerciales sino también un fundamento para otros servicios que requieren la interacción con redes privadas tales como comercio-m, presencia virtual y aplicaciones de juego, y las aplicaciones multimedia (que incluyen servicios basados en Voz sobre IP).

Los beneficios de desplegar VPNs móviles para negocios e instituciones incluyen:

- Conectividad a redes privadas ininterrumpida e independiente de la localización.
- Movilidad continua y acceso privado a la red.
- Conectividad a un proveedor de servicio de Internet (ISP) o proveedor de servicios de aplicación (ASP) particular.
- Acceso remoto móvil que externaliza las posibilidades.
- Habilitador seguro de comercio-m.
- Accesibilidad constante para trabajadores remotos.
- Rentabilidad más alta.

Como consiguiente, los negocios, que ya tenían una experiencia positiva con servicios de VPN alámbricos, contemplan ahora a operadores inalámbricos para ampliar estos servicios en ambientes inalámbricos. Durante los próximos años cuando las últimas generaciones de sistemas celulares y otras tecnologías inalámbricas salgan, una enorme oportunidad de mercado espera a los portadores inalámbricos quienes pueden encontrar demanda de servicios que requieren el acceso de red privado.

1.3.3 MVPN Como una Herramienta de Diferenciación

VPN móvil es un instrumento poderoso de diferenciación sobre todo para los proveedores de servicio que dedican una porción significativa de sus ofertas a servir a clientes de negocios. Pero ¿por qué la diferenciación es tan importante? Durante las últimas décadas, nosotros presenciamos el ascenso gradual de las comunicaciones celulares, de artículo de lujo y símbolo de prestigio a instrumento necesario y luego repentinamente se convierten en una comodidad. La comodización es indeseable para cualquier industria. Pero esto es también una parte natural del ciclo de vida de casi cualquier producto y no es nada extraño para las telecomunicaciones inalámbricas. Como los servicios Web basados en Internet retumbaron en años recientes, el acceso ubicuo y rápido a Internet llegó a ser una meta inmediata de la industria inalámbrica de datos. Sin embargo, los servicios de datos inalámbricos que consisten principalmente en el acceso a Internet son considerados tan genéricos como los servicios celulares de voz de hoy, y afrontan la competencia basada en el precio que está dañando a los ingresos de voz inalámbrica. Los suscriptores no tendrán bastantes incentivos para permanecer con un portador particular por otros motivos más que los precios. La situación es además complicada por la comodidad de cambiarse de un portador a otro, conocida por los operadores como *agitación del cliente,* que ha molestado a la industria inalámbrica desde su inicio.

MVPN parece ser una de las respuestas probables a estos problemas. Puesto que la tecnología de MVPN es altamente costeable y se puede poner en ejecución de diversas maneras para acomodar las diferentes necesidades de los clientes, los servicios ofrecidos por MVPN pueden ser también empaquetados y vendidos por diferentes operadores inalámbricos. Esto significa que serían

capaces de ofrecer servicios únicos, y por lo tanto prevenir que el precio se base en la agitación del cliente. Esto es especialmente verdad para instituciones y empresas grandes que esperan hacer de los servicios únicos de MVPN de operadores inalámbricos diferentes una parte integrante de sus infraestructuras IT.

1.4 El Mercado de MVPN

El mercado de MVPN, como cualquier otro mercado, consiste en compradores (clientes de acceso privado a la red) y vendedores (portadores inalámbricos y otros proveedores de servicio) quienes entran en transacciones acerca de un producto particular o categoría de producto (acceso de red privado en el ambiente móvil en nuestro caso). Veamos ahora cada grupo, tomando en cuenta los diferentes beneficios de MVPN y las estrategias de despliegue más convenientes para diferentes clientes y proveedores.

1.4.1 Proveedores de Servicio de MVPN

Los proveedores de servicio de MVPN pueden ser clasificados en tres grupos principales:

- Operadores inalámbricos.
- Operadores Privados Virtuales Móviles (MVNOs, *Mobile Virtual Network Operators*) y otros subcontratistas y revendedores.
- Proveedores de servicio de Internet inalámbrico.

El grupo de operadores inalámbricos incluye a portadores, que ofrecen tanto servicios actuales de MVPN basados en red como el acceso a Internet con calidad comercial con las propiedades convenientes para una VPN estable de punta-a-punta para ser creada entre el equipo móvil del cliente y los gateways VPN del cliente. Los portadores inalámbricos son con mucho el grupo de proveedores de servicio de MVPN más grande. Esto no es sorprendente, ya que los portadores inalámbricos poseen tanto licencias del espectro como la infraestructura de radio. Para ofrecer los servicios de MVPN basados en red, los portadores inalámbricos tendrían que establecer acuerdos apropiados con las empresas e instituciones definiendo relaciones de confianza, responsabilidades legales, calidad de servicios, disponibilidad, y otros parámetros. Si la empresa elige un método VPN de punta-a-punta, el papel de los portadores inalámbricos debería soportar MVPN de punta-a-punta compatible con el esquema de direccionamiento IP basado en el uso de direcciones IP ruteables o mecanismos de traducción de dirección privados diseñados apropiadamente. Desde luego, en el caso de VPN de punta-a-punta, los portadores inalámbricos podrían ser evitados totalmente y ni se enterarían de la comunicación privada que ocurre sobre su infraestructura, debido a la naturaleza de la VPN de punta-a-punta, los paquetes transmitidos entre los puntos finales del túnel son encriptados. Esto hace al servicio basado en red más atractivo para los portadores inalámbricos; ellos pueden introducir una multitud de ofrecimientos con altos potenciales de generación de ingresos y tener más control de los suscriptores móviles.

La segunda categoría de potenciales proveedores de MVPN incluye a los Operadores Privados Virtuales Móviles (MVNOs) y a otros subcontratistas de servicio inalámbrico, como aquellos contratados para lograr acuerdos para compartir infraestructura (la red de acceso de radio y la licencia del espectro normalmente pertenecen a sus socios de negocio). Este grupo debería estar sobre todo interesado en servicios VPN basados en red por las mismas razones que los portadores inalámbricos regulares. Además, cuando la opción VPN de punta-a-punta es seleccionada por los clientes corporativos del MVNO, el papel del MVNO estaría muy restringido y los ingresos serían probablemente marginales, desde el papel de intermediario los objetivos del MVNO serían bastante limitados. Entonces los MVNOs aún con mayor probabilidad se esforzarán por añadir tanto valor como sea posible poniendo en práctica servicios inteligentes en la red.

El último grupo de proveedores de servicio, incluye a los tradicionales proveedores de servicio de Internet alámbrico. Este grupo puede participar en el suministro del servicio de MVPN basado en red a través de acuerdos con los operadores inalámbricos. Las ventajas de ofrecer el servicio de

MVPN para este grupo no mienten sobre todo en nuevas capacidades que generan ingresos pero en la línea de extensión del producto—eso es, en aumentar sus ofertas alámbricas tradicionales con las nuevas opciones disponibles de MVPN. Esto permite a los ISPs alámbricos hacerse provedores de servicios universales para sus clientes tradicionales sin tener en cuenta el método de acceso de red (alámbrico o inalámbrico). También tenemos que acentuar que los proveedores de servicio alámbrico en algunos países comienzan a conducir el despliegue de una infraestructura de cobertura de tipo "lugar-caliente" (*hot-spot*) basada en WLAN, buscando así tanta independencia posible de operadores celulares inalámbricos y al mismo tiempo tratando de competir con ellos en servicios de datos inalámbricos de alta velocidad.

1.4.2 Clientes de MVPN

Las ventajas de desplegar VPNs móviles son tan significativas para los clientes así como ellos lo son para los proveedores de servicio. Las MVPNs proporcionan conectividad constante a trabajadores remotos, independiente de los medios a redes corporativas o a los ISPs y ASPs de su elección. Las MVPNs permiten a las corporaciones externalizar el acceso remoto móvil, y en algunos casos pueden sustituir completamente infraestructuras alámbricas de acceso remoto, eliminando así los gastos de compra y soportar el equipo de acceso remoto al permitir a las redes privadas mantener el control completo sobre las asignaciones de dirección al usuario, la autenticación, y la seguridad.

Generalmente, los usuarios pueden ser clasificados en las siguientes categorías:

- Negocios pequeños
- Empresas grandes
- Instituciones, tanto del gobierno como académicas
- Proveedores de servicios de aplicaciones (ASPs)

1.4.2.1 Negocios Pequeños

La principal motivación para los negocios pequeños para usar MVPN es principalmente la conveniencia y sus capacidades de reducción de gastos. MVPN es generalmente usado por pequeños negocios para el acceso remoto para centralizar los recursos de información, acceso a correo electrónico, y el monitoreo de ciertos acontecimientos, como el monitoreo médico y la facturación. El servicio de MVPN para pequeños negocios con mayor probabilidad será conseguido vía conectividad de punta-a-punta, que no requiere el establecimiento de acuerdos complejos con portadores inalámbricos. En cambio, el personal responsable debe asegurarse que los empleados y los socios son proveídos del acceso a Internet inalámbrico para negocios con la calidad apropiada para soportar el servicio de MVPN de punta-a-punta.

Otra razón por la que VPN de punta-a-punta es más probable de ser utilizada dentro de este segmento es su comodidad relativa de implementación y el precio bajo. Para soportar este servicio, los trabajadores remotos deben ser proveídos de dispositivos móviles equipados con clientes VPN disponibles o propietarios y software de seguridad y equipo como la pila de protocolos IPSec y tarjetas *RSA SecureID*. A menudo los clientes son empaquetados con los sistemas operativos -por ejemplo, los clientes de IPSec son empaquetados con *Microsoft Windows 2000* usado con computadoras portátiles (*laptops*).

1.4.2.2 Empresas

La razón principal por la que las empresas más grandes estarían interesadas en MVPN es la potencial productividad de ganancias. El recorte de costos y la facilidad de despliegue serán cuestiones secundarias. En una empresa, los servicios de MVPN son más probablemente externalizados vía un acuerdo o varios acuerdos con los portadores inalámbricos, los cuales son los responsables de proporcionar a empleados y socios remotos de una empresa con tipos específicos y clases de servicios MVPN. En esta situación, todos los tipos de MVPN pueden ser

usados con resultados igualmente buenos mientras satisfagan el costo, la seguridad, la conveniencia, la facilidad de soporte, y otras exigencias de una empresa.

Generalmente, las empresas grandes no son tan sensibles al costo como los pequeños negocios o instituciones de gobierno. A menudo desean servicios de tecnología avanzada para sus trabajadores remotos móviles -como acceso móvil de datos de alta velocidad y medidas especiales de seguridad— que requieren una variedad de tecnologías de MVPN. Por lo general, los departamentos IT de la empresa requieren estar implicados en muchos aspectos de los servicios proporcionados por los portadores, los cuales, por ejemplo, les permitirían a los proveedores retener el control de la política de aprovisionamiento, autenticación, o asignación de direcciones IP. En estas situaciones, la gestión de interfaces abiertas, así como los arreglos de aprovisionamiento cuidadosamente estructurados, son críticos.

1.4.2.3 Instituciones

El gobierno y otras instituciones públicas podrían estar interesados en servicios MVPN por motivos diferentes de aquellos motivos del sector privado. Por ejemplo, el teletrabajo es alentado por el gobierno de EEUU principalmente no por razones de recorte de costos sino para reducir la contaminación eliminando el viaje diario hacia el trabajo. Las oficinas en casa llegan a ser cada vez más populares con muchas instituciones públicas. Esta tendencia, sin embargo, requiere mecanismos de acceso remoto en gran escala como la línea terrestre IP VPN combinada con MVPN para trabajadores sobre el camino.

Los requerimientos de servicio de una institución del gobierno a menudo pueden ser bastante imprevisibles e inesperadas, a menudo por una buena razón o al menos con intenciones buenas. Por esta razón, la flexibilidad en los ofrecimientos y las tecnologías de MVPN debería ser la clave para tratar con instituciones públicas de varios tamaños y funciones. Por ejemplo, los requerimientos de seguridad pueden ser a menudo muy fuertes y exceden de aquellas acostumbradas para el sector privado.

Por otra parte, las instituciones del gobierno requieren a menudo que estén conscientes sobre todo de los costos y deben estructurar sus gastos según los proyectos anuales. Esto apunta al uso de acuerdos al nivel de servicio muy detallados entre las instituciones del gobierno y los portadores inalámbricos definiendo todos los precios y los servicios que estos precios comprarían. El ofrecimiento del servicio VPN obligatorio también alivia a una institución de la responsabilidad de participar en la instalación de la VPN, el aprovisionamiento, y el mantenimiento -todo lo cual puede ser externalizado a los portadores inalámbricos y sus socios.

Las instituciones académicas y médicas están por lo general ligadas por objetivos similares del uso cuidadoso de los recursos a menudo sustanciales y el deseo de usar la última tecnología disponible para conseguir ciertos objetivos únicos como apoyo a proyectos de investigación de telecomunicaciones o el diagnóstico remoto a pacientes. Los requerimientos de MVPN para este grupo a menudo tienen los atributos tanto de empresas grandes como de organismos públicos. A menudo el servicio que presenta las características correctas quizás consista en una combinación de ofertas y arreglos únicos, tal como una combinación de servicios de punta-a-punta y servicios de VPN basados en red, el uso de políticas granulares por flujo, y arreglos únicos para la diferenciación de tráfico y el paquete de servicio.

1.4.2.4 Proveedores de Servicio de Aplicaciones

Esta clase de clientes MVPN crecerá cuando los portadores inalámbricos tomen las ventajas de la aplicación de paquetes ofrecida por sus socios alámbricos o sus proveedores. Estos jugadores deben confiar en redes dedicadas privadas virtuales de modo que el control de acceso a los servicios que ellos ofrezcan puede ser impuesto fácilmente. Los ofrecimientos de ASP VPN también vienen con características avanzadas de contabilidad, de modo que el proveedor inalámbrico y sus socios puedan intercambiar mutuamente el tráfico correlacionado y los datos

usados y aplicar estas políticas de descuento y ofrecer servicios como el análisis de dirección y el monitoreo del comportamiento de los clientes. Estas MVPNs permiten a los miembros conseguir acceso a los servicios ASP y ofrecen el acceso basado en suscripción a una terminal de servicios en un paquete de servicios sin forzar a los clientes a realizar procedimientos individuales de autenticación.

CAPÍTULO 2

TECNOLOGÍAS DE REDES DE DATOS

2.1 Tecnologías de *Tunneling* y Etiquetado

Las redes privadas virtuales móviles (MVPNs) requieren usar tecnologías que saquen ventajas de la infraestructura pública disponible, operada por los proveedores de servicio, que permiten conectividad "virtualmente privada" entre los sitios de red de los clientes y las estaciones móviles lógicamente pertenecientes a ellos, conocidos como *miembros VPN Móvil o suscriptores*. Tales tecnologías están basadas en la encapsulación de los paquetes de datos del cliente (también conocidos como datos del usuario) dentro de otros paquetes, que son entregados usando la tecnología de la red compartida. La entrega de los datos de los usuarios es hecha usando diferentes esquemas de direccionamiento y diferentes protocolos de la capa de red o de la capa de enlace.

Esta encapsulación, o *tunneling*, como es mayormente referida en el mundo de las redes de datos, no solo proporciona la capacidad para la entrega de los datos desde y hacia estaciones móviles, sino que además añade protección a la integridad y confidencialidad de los datos. Además cuando el operador desea soportar QoS, estas tecnologías facilitan la distribución del tránsito pronostiable de red, por ejemplo, mediante trayectorias de ingeniería de tráfico identificadas por una secuencia de etiquetas, como en MPLS (*Multi-Protocol Label Switching*). MPLS proporciona los medios para mantener la conectividad entre múltiples sitios de una red del cliente de forma automática.

Algunas veces los servicios ofrecidos por un portador pueden ser simplemente el transporte de los datos desde un *gateway* de acceso inalámbrico hacia el sitio de red del cliente vía un túnel o una línea de acceso fija. Otra ocasiones el servicio puede extenderse a un servicio VPN de administración de múltiples sitios, donde el *gateway* de acceso inalámbrico llega a ser simplemente uno de los sitios de la red del cliente. Los túneles son usados además para soportar movilidad, guardando un punto final fijo y teniendo el otro nodo de datos móvil en su punto de enlace a la red (donde normalmente la capa de enlace de la red de acceso está terminada). Son buenos ejemplos de esto último los protocolos *IP Móvil y GPRS Tunneling Protocol*.

Los datos pueden ser transferidos en la capa de red o en la capa de enlace usando un protocolo como PPP (*Point-to-Point Protocol*). En este caso, la red inalámbrica simplemente termina los protocolos de acceso inalámbrico y retransmite el protocolo PPP u otro protocolo de la capa de enlace hacia un servidor de acceso a la red en la red del cliente. Este es regularmente el caso con MVPNs basadas en conmutación de circuitos, pero también se puede encontrar frecuentemente en servicios inalámbricos de datos basados en paquetes, que es favorecido por el extenso uso del acceso remoto basado en PPP por las empresas sobre medios de acceso inalámbricos. El enfoque implicado en PPP normalmente está basado en un protocolo de *tunneling* llamado L2TP.

2.1.1 L2TP (*Layer Two Tunneling Protocol*)

El protocolo L2TP está definido como un protocolo del IETF que proporciona un enfoque estándar que facilita la creación de túneles para enviar tramas PPP sobre redes IP. Cisco y Microsoft tuvieron originalmente el desarrollo de modos propietarios para llevar a cabo ésto (vía *Layer Two Forwarding, L2F, y Point-to-Point Tunneling Protocol, PPTP*, respectivamente). Pero la industria reconoció la necesidad de un enfoque estándar. Como resultado, el Grupo de Trabajo de las Extensiones PPP del IETF (PPPEXT) se dio a la tarea de definir tal estándar. El resultado fue un protocolo de *tunneling* que potencialmente podría ser transportado sobre cualquier célula, trama, o red de transporte basada en paquetes. En particular, el transporte UDP/IP, ampliamente utilizado, fue elegido como el protocolo preferente, (UDP, *User Datagram Protocol*).

L2TP define dos entidades de red con dos papeles distintivos:

- El Concentrador de Acceso L2TP (LAC, *L2TP Access Concentrator*) está localizado en el punto de terminación del protocolo de la red de acceso, y es capaz de establecer túneles hacia los servidores L2TP de acceso a la red (LNSs, *L2TP Network Access Servers*); el LAC es el dispositivo que físicamente termina una llamada.
- El LNS termina los túneles de los LACs y además ofrece servicios de acceso a la red tales como autenticación del usuario y asignación de dirección.

Un cliente LAC que está corriendo en una laptop o cualquier otro dispositivo apropiado podría ser usado para iniciar los túneles L2TP hacia un LNS. El uso de L2TP basado en la utilización de un cliente LAC constituye una forma independiente para las redes de acceso remoto, con la condición de que éstas sean alcanzables en la capa de red. La figura 2.1 ilustra este modelo.

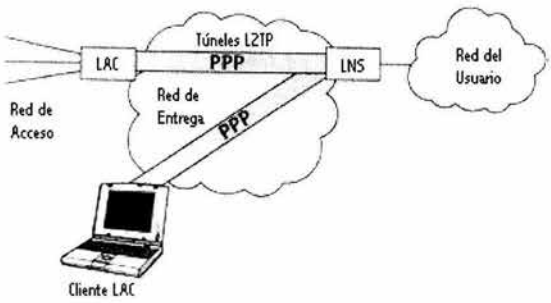


Figura 2.1 Modelo de L2TP.

L2TP define un canal de control confiable. Sobre este canal de control es posible establecer un túnel entre el LAC y el LNS. La fase de establecimiento del túnel normalmente incluye autenticación vía el intercambio L2TP de un secreto entre el LAC y el LNS (en la forma túnel L2TP; contraseña). La autenticación en el intento por establecer un túnel es importante, ya que no es deseable que un LNS acepte cualquier comando L2TP proveniente de un LAC desconocido si no está autorizado para hacerlo. Sin embargo, ya que el protocolo L2TP no viene con autenticación del origen de los datos y confidencialidad, L2TP no puede ser considerado un protocolo seguro. Sin duda, sería posible para un atacante mandar paquetes hacia un LNS o un LAC y hacer el papel de par de cada nodo. La seguridad de L2TP requiere otro protocolo definido para el soporte de seguridad IP: IPSec.

Cuando un túnel es establecido entre el LAC y el LNS, es posible iniciar y terminar una sesión PPP y enviar las tramas asociadas entre los dos nodos usando el formato de encapsulación L2TP sobre el canal de datos de L2TP. El encabezado L2TP (figura 2.2) incluye información del identificador del túnel (ID Túnel) y del identificador de la sesión (ID Sesión) para permitir dos niveles de multiplexación. El identificador del túnel define un túnel entre dos pares, y por lo tanto identifica implícitamente el nodo par en el lado del receptor. El identificador de la sesión identifica una sesión PPP particular dentro del túnel. Debido a que la información del identificador de la sesión puede ser intercambiada sólo después de que tenga lugar el túnel entre el LAC y el LNS, el retardo de iniciación de la llamada PPP podría ser reducido si el túnel L2TP ya está instalado cuando una sesión PPP necesita ser dirigida.

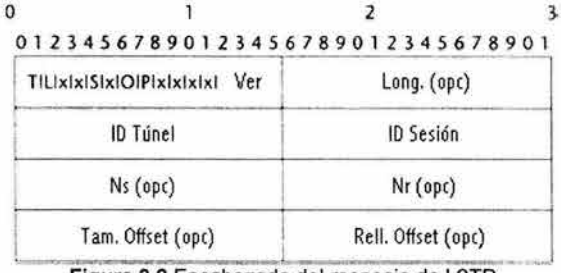


Figura 2.2 Encabezado del mensaje de L2TP.

La autenticación del usuario dentro de las sesiones PPP normalmente toma lugar de manera transparente para el LAC. El LAC meramente decide a cuál LNS instalar la sesión L2TP y subsecuentemente le manda las tramas PPP entrantes. La selección del LNS puede estar basada en información tal como el número destino llamado, o cuando es usado en la red GPRS, en el identificador de la red a la que el usuario PPP está solicitando acceso. El envío de las tramas PPP hacia el LNS correcto permite que la fase de autenticación ocurra entre el LNS y el cliente PPP en el dispositivo remoto. El LAC puede además funcionar como un servidor *proxy* de autenticación colectando datos de autenticación de la llamada entrante y enviándolos hacia el LNS usando señalización L2TP. Para que ésto sea establecido, se requieren relaciones mutuas entre el operador del LAC y el operador del LNS. El LNS, después de haber recibido los datos de autenticación del *proxy*, opcionalmente puede reautenticar al usuario en el nivel PPP iniciando una nueva fase de autenticación PPP antes de pasar a la configuración de la capa de red.

El LAC puede determinar dinámicamente la dirección IP del LNS basado en el nombre de usuario y la contraseña recibidos, los cuales deben contener el Identificador de Acceso a la Red (NAI, *Network Access Identifier*). El LAC puede en este caso conducir un primer paso de autenticación del usuario con la infraestructura AAA[1]. La infraestructura AAA determina el servidor AAA local del usuario basada en el componente del dominio del NAI. La infraestructura AAA podría regresar, cuando es concedido el acceso al usuario, información del túnel L2TP tal como la dirección IP del LNS y la contraseña L2TP. De hecho, el LAC debe decidir si el usuario requiere un túnel L2TP hacia un LNS o simplemente el acceso a la red directamente ligada basado en el componente del dominio del nombre de usuario (con formato como este: dominio\usuario). De esta forma, trabaja como un servidor regular de acceso a la red (NAS, *Network Access Server*). Por ejemplo, el usuario Jdoe, necesita para acceder a Internet usar el nombre de usuario *Inet-acces\Jdoe*, y la red corporativa que usa L2TP vía el nombre de usuario *Corpnet-access\Jdoe*. L2TP puede manejar las llamadas que vienen de la red de acceso hacia el LAC, denominadas "llamadas de entrada", así como solicitudes del LNS para llamar a una terminal específica en la red de acceso (para implementar, por ejemplo, un servicio *call-back*), denominadas "llamadas de salida".

L2TP ha sido ampliamente utilizado para separar la localización de la terminación de acceso de la localización de la terminación del protocolo PPP, con grandes despliegues en instalaciones de acceso remoto global para grandes corporaciones. Este se convirtió en el estándar de facto para servicios tales como acceso remoto cuando una empresa releva a un proveedor de servicio para manejar las sesiones PPP de sus trabajadores remotos en sus instalaciones (POPs equipados con servidores de acceso remoto) entonces los sustituyen para incorporar centros de datos para autenticación y asignación de dirección IP.

2.1.2 IP en IP *Tunneling*

IP en IP, también referido como IPIP, es el servicio de *tunneling* más básico, encapsula un paquete IP dentro de otro paquete IP. En IPIP el encabezado del paquete IP exterior identifica las

[1] AAA: Authentication, Authorization, Accounting; ver sección 2.3.

direcciones de los puntos finales del túnel, donde la dirección fuente es la dirección del encapsulador y la dirección destino es la dirección del desencapsulador.

Algunas veces la encapsulación de un paquete IP dentro de otro paquete IP puede conducir a encabezados excesivos, especialmente cuando paquetes IP de carga útil pequeña son pasados por un túnel, ésto hizo necesario definir una forma para comprimir la información asociadada con el encabezado del paquete IP interno. [RFC2004] describe la IP mínima en la encapsulación IP que define un encabezado de encapsulación insertado entre el paquete IP externo y la carga útil del paquete interno de tal manera que el desencapsulador pueda reconstruir el encabezado del paquete IP interno (figura 2.3). Este puede conducir al ahorro de 8 a 12 bytes por paquete.

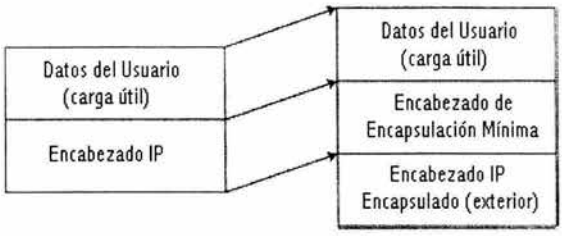


Figura 2.3 Encapsulación mínima para IP.

2.1.3 GRE (*Generic Routing Encapsulation*)

El protocolo GRE es un estándar del IETF que define el formato de encapsulación de múltiples protocolos que puede ser apropiado para pasar por un túnel cualquier protocolo de la capa de red sobre cualquier protocolo de la capa de red. Este concepto fue originalmente especificado en [RFC1701]. Cuando este protocolo original fue movido a vestigio de estándares, la decisión fue hecha para remplazarlo con dos RFCs[2] separados: [RFC2784] y [RFC2890]. [RFC2890] es una extensión del encabezado básico GRE descrito en [RFC2784]. Esto se determinó necesario porque [RFC2784] no permitía por sí mismo la encapsulación de tramas PPP, ya que no tiene un número de secuencia en el formato de encapsulación GRE. Esta limitación fue quitada añadiendo una extensión del número de secuencia al encabezado básico GRE. Además, [RFC2784] no permitía la multiplexación hacia el mismo túnel GRE de paquetes pertenecientes a diferentes entidades administrativas que posiblemente adoptan el traslape de espacios de direcciones privadas (una característica muy usada para la provisión de VPNs). Esta limitación fue quitada añadiendo un campo clave –que es un valor numérico usado únicamente para identificar lógicamente un flujo de paquetes correlacionados dentro del túnel GRE– como una extensión del encabezado básico GRE. Estas extensiones definidas por [RFC2890] fueron especialmente utilizadas en comunicaciones de datos inalámbricas. Por ejemplo, permitieron la entrega de tramas PPP sobre la interfaz R-P en CDMA2000, y el aprovisionamiento de servicios MVPN.

GRE es normalmente usado en dos clases de aplicaciones: el transporte de diferentes protocolos entre redes IP y la provisión de servicios VPN para redes configuradas con traslape de espacio de direcciones privadas. El campo clave del encabezado de GRE puede ser usado para discriminar la identidad de la red cliente donde se originó la encapsulación de los paquetes. De esta forma, proporciona una manera de ofrecer muchas interfaces virtuales a la redes clientes sobre un túnel GRE. Esta característica permite el ruteo basado en políticas (esto es, cuando las decisiones de ruteo no solo están basadas en la dirección IP destino sino en la combinación de un identificador de interfaz virtual y la dirección IP destino) y es relativamente fácil de usar para la contabilidad de red. Además, un encabezado GRE permite la identificación del tipo de protocolo que está siendo

[2] RFC: Request for Comments; ver Capítulo 8.

transportado sobre el túnel GRE, entonces permite a las redes IP servir como un servicio portador sobre el cual una red virtual multiprotocolo puede ser definida e implementada.

2.1.4 IP Móvil

IP Móvil está basado en una variedad de mecanismos de *tunneling*, pero en sí mismo, no proporciona uno. IP móvil fue definido originalmente por [RFC2002], el cual más tarde se volvió obsoleto para soportar la movilidad de la terminal en la capa de red (IP). IP Móvil fue originalmente concebido para permitir nodos con direcciones IP estáticas fijas para estar permanentemente alcanzables si cambian su punto de conexión hacia la red. Esta aplicabilidad fue limitada para soportar la movilidad de las terminales de Internet y de los ruteadores sólo en ciertos ambientes tales como campus o redes universitarias. No hubo soporte para la asignación dinámica de direcciones y no tuvo características de contabilidad y autenticación de usuarios. Sin embargo, IP Móvil más tarde fue adoptado por los sistemas celulares como el Motorola IDEN desarrollado por Nextel y más recientemente por el estándar CDMA2000 para redes centrales, esto involucró tomar en cuenta las necesidades de los ambientes comerciales. Hoy en día IP Móvil está siendo considerado como un método preferente para soportar tecnologías multiacceso y *roaming* intersistemas.

IP Móvil está definida como una tecnología independiente para instalación de túneles y mantenimiento de protocolos utilizada para permitir *roaming* entre terminales o ruteadores de Internet para mantener constante la dirección IP y la conectividad ininterrumpida a nivel IP hacia la red local mientras cambian los puntos de conexión y la tecnología de acceso a la red.

2.1.4.1 Implementación de IP Móvil

Al igual que L2TP, IP Móvil proporciona un modelo de arquitectura que define los papeles de diferentes entidades que están involucradas en la operación de IP Móvil. IP Móvil debe estar implementado en tres funciones principales:

- Agente Local (HA, *Home Agent*)
- Agente Exterior (FA, *Foreign Agent*)
- Nodo Móvil (MN, *Mobile Node*)

HA y FA soportan el protocolo IP Móvil sobre las redes local y exterior (visitada) del nodo móvil, respectivamente.

Durante la sesión de comunicación de IP Móvil el HA está siendo comunicado continuamente por el MN de su localización actual vía mensajes de petición de registro, ya que el MN anda a través de diferentes redes. El HA y los FAs disponibles en redes exteriores anuncian su disponibilidad por medio de mensajes de *anuncio del agente* difundidos sobre los enlaces directamente conectados a ellos.

La localización del MN está representada por su *cargo de dirección* (CoA) siendo temporalmente asignado por el FA (o adquirida por el mismo MN en la red visitada cuando IP Móvil opera en el modo *cargo de dirección colocado*). El HA envía el tráfico al MN (siempre a través de un FA) y acepta el tráfico de un MN (posiblemente vía FA) cuando un túnel de reversa es usado. Además procesa la petición de registro del FA y administra los túneles IP Móvil para los usuarios que tienen acceso a la red mediante el HA mismo. El modelo típico de una red IP Móvil es mostrado en la siguiente figura.

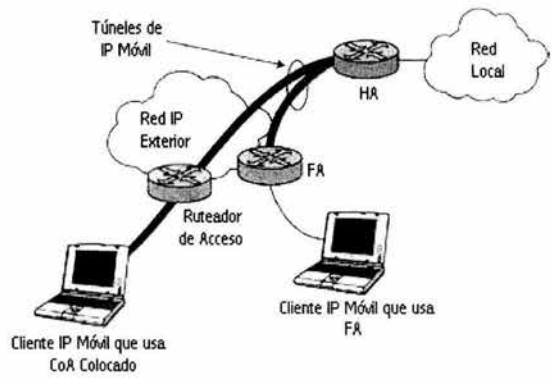


Figura 2.4 Modelo de IP Móvil

El FA puede enviar los paquetes del MN directamente hacia Internet o pasarlos por un túnel hacia el HA que es llamado *túnel de regreso de IP Móvil*. La construcción de un túnel de regreso muchas veces es necesaria para permitir a las corporaciones y a los proveedores de acceso a la red operar el HA para crear VPNs en las cuales todo el tráfico desde y hacia el MN puede estar opcionalmente asegurado y siempre atravesaría el HA en su red privada para mayor control y seguridad. Los estándares además permiten al MN registrarse directamente con el HA cuando el FA no está disponible, después de esto adquiere un cargo de dirección IP en la red visitada, el cual en este caso es llamado *cargo de dirección colocado*. Esta dirección podría entonces ser usada por el MN para intercambiar mensajes de registro y para pasar paquetes por túneles desde y hacia el HA, todo sin la necesidad de un FA.

Un MN puede tener asignada una dirección IP estática o puede obtenerla dinámicamente de un *pool* de direcciones IP pertenecientes a las redes servidas por el HA. El FA, siendo un ruteador en la red visitada, es capaz de atender a los MNs visitantes. Como se ilustra en la figura 2.5, el FA anuncia su presencia vía anuncios del agente periódicos, o respondiendo con anuncios del agente a los mensajes de solicitación de agente de IP Móvil enviados por los MNs que visitan una de las redes atendidas por el FA. Cuando un MN se mueve a una red controlada por un cierto FA, puede mandar una petición de registro al FA, el cual registra al MN con su HA enviando un mensaje de petición de registro al HA apropiado. El HA puede aceptar esta petición y entrega una respuesta de registro al FA, que lo entrega al MN. Después de que este mensaje se intercambia y todas las fases de autenticación son completadas, el HA crea los túneles IPIP o GRE hacia el FA y entonces comienza a enviar paquetes destinados a un MN registrado hacia el FA, el cual los entrega al MN.

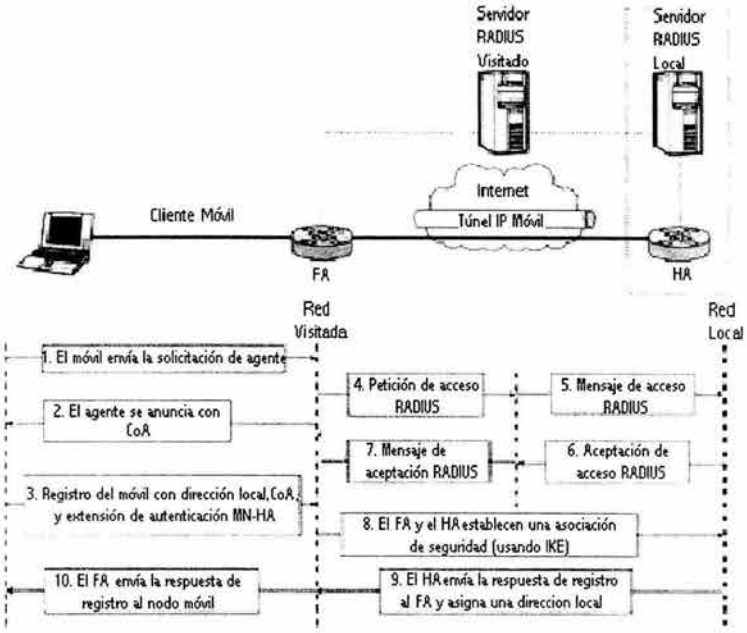


Figura 2.5 Procedimiento de registro en IP Móvil

El protocolo IP Móvil por sí mismo ha sufrido muchos cambios y adiciones en la última década, para hacerlo adecuado para su desarrollo comercial en varios sistemas, especialmente por las recomendaciones de la TIA especificadas en IS835, las cuales definen a IP Móvil como una base para la movilidad de los datos del usuario en la capa de red en CDMA2000. Por ejemplo, ha sido añadida protección a los mensajes de registro a través del uso de una extensión *Demanda-Respuesta*. Además, le fueron añadidos soporte para *roaming* vía la extensión NAI y asignación dinámica de direcciones locales.

La asignación dinámica de direcciones locales es una característica importante de IP Móvil. Originalmente, IP Móvil estuvo basado en la asunción de que todos los HAs en la red fueron asignados estáticamente. Este modelo, sin embargo, es menos conveniente para el desarrollo comercial en amplias áreas porque expone a los proveedores de servicio en el extremo del uso ineficiente de direcciones IP. Este modelo además hace al HA un simple punto de fallas, porque una vez que el HA que atiende a un MN particular falla, le son negados los servicios de datos al MN hasta que el HA funcione correctamente. La asignación dinámica del HA proporcionaría ruteo más óptimo y mejor utilización de la infraestructura de datos de la línea terrestre cuando un MN está a una distancia significativa de su red local.

Los estándares están trabajando en la definición del llamado *ruteo óptimo*. En esta definición, el MN puede actualizar el nodo involucrado en una sesión, llamado el nodo correspondiente (CN), de la dirección IP que ha sido adquirida en la red visitada. Entonces el CN podría ser solicitado para mandar paquetes directamente a esta dirección IP. El ruteo óptimo, sin embargo, resulta ser no tan seguro, ya que la carga para los nodos correspondientes de millones de nodos móviles (como los servidores Web) podría ser verdaderamente sustancial.

En contraste con IPv4, IP Móvil para IPv6 está basado en un ruteo óptimo y se espera que sea soportado por cualquier terminal o ruteador compatible con IPv6.

2.1.5 Protocolo de *Tunneling* de GPRS

El protocolo de *tunneling* de GPRS (GTP) es un protocolo usado para soportar la movilidad de las estaciones móviles de GPRS y UMTS que andan a lo largo de las localidades geográficas atendidas por diferentes nodos SGSN *(Serving GPRS Support Nodes)*. La estación móvil (MS) de la red local está representada por los nodos GGSN *(Gateway GPRS Support Nodes)*. Los GGSNs se conectan a los SGSNs vía el protocolo GTP. Al contrario de IP Móvil, GTP no tiene que ser soportado en la MS. Este es un protocolo usado sólo dentro de la red, y trabaja con otros protocolos para interactuar con la MS y entonces permitir su rastreo.

Existen dos versiones del protocolo GTP. La Versión 0, es usada en los sistemas basados en el subsistema de la estación base de GSM (BSS) y se aplica a las liberaciones R97 y R98 de GSM. La Versión 1 se aplica a sistemas basados en las redes de radio acceso de GSM y UMTS. 3GPP[3] decidió crear una nueva versión del protocolo GTP porque los miembros del grupo decidieron introducir nuevas características que no podrían ser soportadas por la versión antigua del protocolo GTP. Decidieron separar el protocolo en un protocolo de usuario (GTP-U) y un protocolo de control (GTP-C). La razón de esta división fue dictada por la necesidad para soportar la creación de túneles basados en GTP-U sobre la interfaz entre la central de UMTS y la red de radio acceso de UMTS (interfaz Iu), sin la necesidad de usar GTP-C para instalar túneles Iu. Otra característica significante que diferencia GTPv1 de GTPv0 es el soporte de múltiples niveles de QoS por cada dirección IP asignada a una MS, lo cual requiere el establecimiento de múltiples portadores UMTS y del uso de múltiples túneles por cada sesión de datos de la MS. Esto conduce a la necesidad de un campo de multiplexaje en el encabezado de GTPv1 (el identificador del punto final del túnel), el cual fue entonces usado para remplazar una bastante incómoda y compleja estructura de campos de identificación de una sesión de datos en GTPv0. La figura 2.6 ilustra la diferencia en la estructura del encabezado entre GTPv0 y GTPv1.

[3] 3GGP es un acuerdo entre los cuerpos regionales de estándares para telecomunicaciones; ver Capítulo 8.

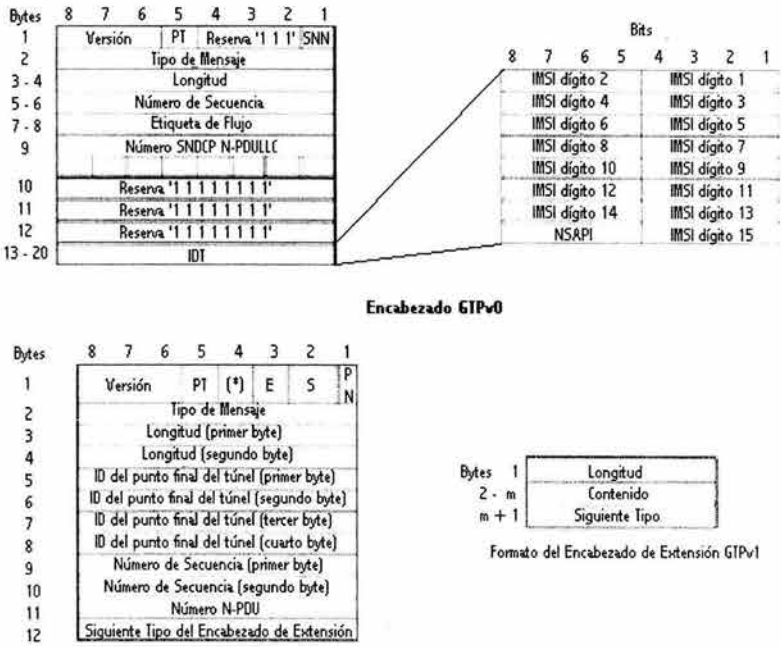


Figura 2.6 Encabezados de GTPv0 y GTPv1

GTPv0 podría ser transportado sobre TCP o UDP. TCP fue sugerido para ser usado para ofrecer transferencia confiable de los datos de usuario, lo cual podría ser requerido para el transporte de datos X.25. El mercado de redes inalámbricas de datos ha decidido realizar el transporte de datos solo sobre UDP. El número de puerto UDP para GTPv0 es 3386, y los números de puertos para GTPv1 son 2023 para GTP-C y 2052 para GTP-U.

La mensajería de GTP-C incluye lo siguiente:

- Mensajes de gestión de túneles usados para detectar condiciones de fallas, pérdidas de conectividad, y reinicio de un nodo par.
- Mensajes de gestión de sesión utilizados para instalar túneles entre GGSNs y SGSNs, y para actualizar los cambios de nodo par en los parámetros del túnel como QoS, nuevo plano de usuario, y plano de control de direcciones IP del nuevo SGSN hacia el que se movió la MS.
- Mensajes de gestión de localización usados para implementar procedimientos de instalación de la sesión GTP.
- Mensajes de gestión de la movilidad usados para transferir información del contexto de la MS y del contexto de la sesión en caso de *handoff*.

GTP-U simplemente es usado para encapsular paquetes de usuario, pero puede además monitorear la trayectoria de transmisión para detectar fallas usando mensajes de gestión de túneles. Es utilizado entre SGSNs, entre GGSNs y SGSNs, y entre el SGSN y el RNC de UMTS.

Cuando una sesión es instalada, GTP puede transferir datos de la MS y datos relacionados con el suscriptor al GGSN -usando el elemento de información "Opciones de Configuración del Protocolo"- así como alguna información sobre si el suscriptor tiene derechos de acceso, vía

suscripción, al punto de acceso (AP) de la red donde el túnel GTP va a ser creado. Esta información es insertada dentro de GTP por el nodo SGSN.

El IMSI[4] (un identificador único del suscriptor) y el MSISDN[5] (el número telefónico de la MS) son enviados por el SGSN al GGSN usando GTP-C, y el GGSN puede transmitir esta información a servidores externos, los cuales, por ejemplo, podrían aplicar políticas de identificación de usuarios. Además, GTP es usado entre SGSNs para transmitir información relacionada a la MS cuando sucede un proceso de *handoff*. Es también utilizado cuando una MS se enlaza a un nuevo SGSN, y este nuevo SGSN necesita recuperar información de la identidad del suscriptor del SGSN al cual la MS estaba previamente enlazada.

GTP puede ser usado para encapsular diferentes protocolos de datos de usuario tales como PPP, IPv4, e IPv6. Otros protocolos como X.25 fueron originalmente permitidos por el estándar, pero más tarde las comunidades de vendedores y operadores desecharon su soporte.

2.1.6 Seguridad de Direccionamiento

Existe una percepción común de que IP no es un protocolo seguro y que el público de Internet está expuesto a toda una serie de ataques por parte de individuos y grupos, desde adolescentes quienes "*hackean*" terminales hasta cibercriminales que usan Internet para dañar instituciones o robar bancos. La inseguridad es una debilidad reconocida de la tecnología IP. Se necesita garantizar la integridad de los datos, la autenticación del origen de los datos, y confidencialidad:

- Añadiendo mecanismos de seguridad para las aplicaciones y los dispositivos que usan IP (algunos ejemplos incluyen servicios basados en Web tales como comercio electrónico, bancos electrónicos, o acceso al correo corporativo vía interfaces Web).
- Haciendo seguro al protocolo IP por sí mismo vía algunas extensiones y protocolos. Estas extensiones del protocolo IP permiten un nivel adecuado de seguridad y son conocidas bajo el nombre de IPSec.

2.1.6.1 IPSec

La arquitectura IPSec define los componentes necesarios para proporcionar una comunicación segura entre entidades pares del protocolo IP. IPSec extiende el protocolo IP con dos encabezados de extensión: el encabezado ESP (*IP Encapsulating Security Payload*) y el encabezado AH (*Authentication Header*). El encabezado ESP es usado para proporcionar confidencialidad implícita a los datos, integridad de la carga útil, y autenticación, mientras que el encabezado AH es usado para ofrecer integridad a la carga útil de datos y garantizar la integridad de los campos no mudables del encabezado IP. Ambos encabezados pueden ser usados cada uno para encapsular un paquete IP dentro de otro paquete IP (modo túnel de IPSec) o para encapsular solo la carga útil de un paquete IP (modo transporte de IP). En la figura 2.7, AH es usado para proporcionar modo transporte de IPSec y ESP para proporcionar modo transporte de IPSec, pero además es posible una combinación de AH y ESP, de acuerdo a los estándares.

[4] IMSI: International Mobile Station Identifier.
[5] MSISDN: Mobile Station ISDN.

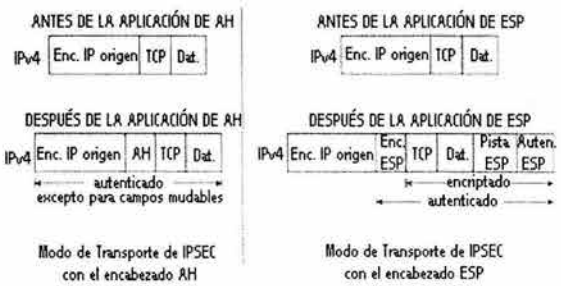


Figura 2.7 Modo de Túnel y Modo de Transporte de IPSec con los encabezados ESP y AH

Aunque existen implementaciones interoperables de AH, en la industria de las VPNs los modos de túnel y de transporte con ESP son los enfoques más comúnmente utilizados. Esto es porque AH solo proporciona una parte de las capacidades de ESP y porque, incluye en el algoritmo de autenticación todos los campos no mudables del encabezado IP, la autenticación del origen de los datos proporcionada por AH puede ser ofrecida usando el modo de túnel IP con ESP. Sin duda, con el servicio de encriptación ofrecido en el modo de túnel ESP, el paquete IP interno, el encabezado IP, y las cargas útiles están implícitamente protegidas de alteraciones a lo largo de la ruta desde el punto de ingreso del túnel hasta el punto de salida del túnel. AH es sin embargo usado por algunos protocolos, como IP Móvil, el cual requiere mensajes de control para estar protegido vía el modo de transporte.

Estos mecanismos de seguridad, sin embargo, son generales y no están forzados a usar un algoritmo predefinido de encriptación o autenticación. Por lo tanto, las implementaciones pueden añadir los algoritmos de encriptación que ellos dispongan sin cambiar el modelo arquitectural. El protocolo de encriptación más comúnmente usado es 3DES (*Triple Data Encryption Standard*), y los protocolos de autenticación más usados están basados en una mezcla de funciones tales como SHA-1 y MD-5 (SHA por *Secure Hash Algorithm*, MD por *Message Digest*).

Los componentes fundamentales de la arquitectura de IPSec son la base de datos de políticas de seguridad (SPD, *Security Policy Database*) y la base de datos de asociación de seguridad (SAD, *Security Association Database*). Cada interfaz IP para la cual IPSec es habilitada debe ser equipada con una base de datos de reglas de clasificación de seguridad y acciones de seguridad. Cada par individual regla-acción es conocido como una política de seguridad. Una asociación de seguridad (SA, *security association*) define un tratamiento unidireccional de los paquetes en términos de política de seguridad forzando a acciones que definen cuáles encabezados IPSec son aplicados, cuáles algoritmos de encriptación o autenticación son usados, y cuáles claves son usadas para ejecutar estos algoritmos. Para cada interfaz IP, existe un par de tales bases de datos: una para el tráfico entrante y otra para el tráfico saliente. Si un paquete no cumple alguna regla, la interfaz puede ser configurada para descartarlo.

Para entender mejor estos conceptos, podemos usar el siguiente ejemplo de una entrada en una IPSec SPD e IPSec SAD. Una posible política de seguridad puede ser definida por la siguiente entrada en la base SPD de una interfaz IP: "Para todos los paquetes con rumbo a la dirección IP (192.43.56.82) y puerto número 8080, aplicar la asociación de seguridad *ALFA*." La asociación de seguridad ALFA es una entrada en la base SAD de la misma interfaz IP, definida en base al modo túnel de IPSec con ESP y el algoritmo de encriptación 3DES y con una clave de encriptación manualmente intercambiada y provisionada en los puntos finales.

Las claves de seguridad pueden ser simétricas o asimétricas. Las claves simétricas o privadas son distribuidas a las dos partes involucradas en una comunicación segura. Las claves asimétricas están basadas en el paradigma de criptografía de claves públicas patentado por *RSA Data Security*

Inc., ampliamente utilizado en la industria para encriptación y autenticación. En esta instalación, la parte que desea librar comunicaciones seguras con otros hace disponible una clave pública. Este enfoque es conocido como clave asimétrica porque usa un par de claves: una que es pública y ampliamente distribuida y otra privada que es mantenida en secreto y nunca divulgada. El material encriptado usando una clave pública puede ser desencriptado sólo usando la clave privada asociada. Inversamente, sólo la clave pública puede ser usada para desencriptar el material encriptado con la clave privada.

Un sistema de clave asimétrica puede ser usado para intercambiar una clave secreta necesaria para correr un algoritmo de encriptación basado en claves simétricas. En otras palabras, si una parte conoce la clave pública de una entidad, puede mandarle a ésta última una clave secreta, encriptada por medio de la clave pública, y esta parte podría desencriptarla usando la clave privada. Para comunicarse con un par usando una clave pública, es necesario acreditar la fuente de esta clave. Por lo tanto es necesario que los depositarios de tal información puedan estar acreditados. Estos depositarios son conocidos como autoridades de certificación (CAs). Una asociación de seguridad puede ser manualmente provisionada o dinámicamente administrada, junto con las claves de seguridad necesarias para correr los protocolos de encriptación o autenticación. Este protocolo es conocido como Protocolo de Administración de Claves y Asociaciones de Seguridad, y el actual estándar IETF para ésto es conocido como *Internet Key Exchange* (IKE).

El protocolo IPSec puede ser desplegado en la forma terminal-a-terminal, terminal-a-ruteador, o ruteador-a-ruteador. Un ruteador con implementación IPSec y aplicación de políticas de seguridad para tráfico IP es a menudo referido como un *gateway* IPSec. La figura 2.8 ejemplifica los casos terminal-a-ruteador y ruteador-a-ruteador, los cuales son de especial interés para el servicio de VPN.

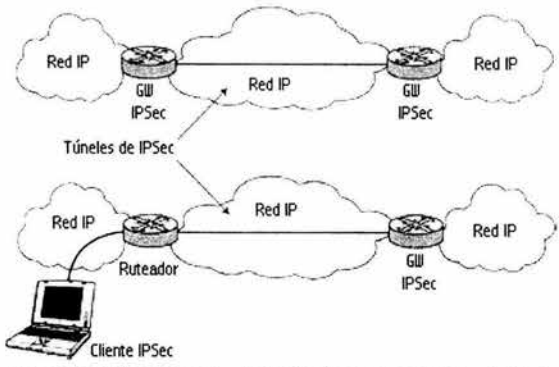


Figura 2.8 Arquitectura de IPSec (*gateways* y terminales).

Cuando IPSec es usado para VPNs IP sitio-a-sitio, se usa el modo túnel de IPSec. Un ejemplo de una aplicación del modo transporte de IPSec son los túneles L2TP para la protección de la integridad y de la confidencialidad. Tiene sentido el uso del modo transporte para protección por túneles L2TP ya que L2TP es en sí misma una tecnología de tunneling y el uso de modo túnel de IPSec podría resultar en encapsulación redundante, o túneles anidados. Por el contrario, tiene sentido usar el modo túnel de IPSec para VPNs sitio-a-sitio, ya que de todos modos los paquetes necesitan ser pasados por un túnel y este modo proporciona la construcción de túneles y la seguridad requeridas para esta aplicación.

2.1.6.2 Infraestructura de Clave Pública (PKI)

La infraestructura de clave pública es un importante concepto de seguridad. Las claves públicas, usadas en las redes de datos para verificar firmas digitales, por sí mismas no aportan información alguna acerca de las entidades de donde provienen las firmas. La industria de las redes de datos reconoció este problema y adoptó los certificados de seguridad enlazando la clave pública y la identidad de la entidad que emite la clave, la cual puede ser verficada usando una clave pública acreditada, tal vez conocida usando un certificado emitido por una autoridad de mayor nivel jerárquico. Los certificados son emitidos y puestos en vigor por una autoridad certificadora, la cual está autorizada para proporcionar tales servicios. Para presentar estas funciones, una autoridad certificadora debe estar acreditada por todas las entidades (miembros de la infraestructura de clave pública) dependientes de sus servicios.

Un certificado contiene la siguiente información:

- El nombre del emisor del certificado.
- La entidad para la cual el certificado está siendo emitido (conocida como sujeto).
- La clave pública del sujeto.
- Estampillas de tiempo (necesarias para determinar le edad de un certificado y su validez).

Todos los certificados son firmados usando la clave privada de la autoridad certificadora. Un usuario del certificado puede verificar que la información del certificado es válida desencriptando la firma y verificándola mediante la comparación del compendio del contenido recibido en el certificado. La firma es normalmente un resumen encriptado del contenido –esto es, una cadena de bits obtenida mediante encriptación.

Los miembros de la infraestructura PKI deben acordar un tiempo de vida estándar de un certificado y entonces determinar cuándo un certificado es anticuado o ha expirado. Además, una autoridad certificadora puede publicar una lista de revocación de certificados (CRL), así que los miembros de la infraestructura pueden consultar los certificados validados por la autoridad certificadora checándolos en la lista CRL.

Las relaciones entre la autoridad certificadora y otros miembros de la infraestructura PKI deben ser establecidas antes de cualquier transacción PKI. Tales relaciones pueden ser establecidas sobre bases geográficas, políticas, sociológicas, de negocios, o étnicas y pueden abarcar industrias, ciudades, grupos de población, u otras entidades unidas por intereses comunes.

En la figura 2.9 se describe el caso de dos partes, A y B, dispuestas a intercambiar un secreto. La parte A recupera la clave pública de B del certificado de B. El certificado puede ser verificado porque está firmado con la clave privada de la autoridad certificadora de B, y esto puede ser checado recuperando la clave pública de la autoridad certificadora de B del certificado de la autoridad certificadora de B, la cual puede ser verificada usando la clave pública de una autoridad de certificación raíz que garantiza que es válida, por ejemplo, porque funciona dentro del código del cliente PKI sobre el módulo de software de A. Una vez que la clave pública de B está disponible, A encripta el secreto usando ésta, y entonces envía este mensaje encriptado a B, junto con su propio certificado (certificado de A) y un resumen del secreto encriptado, calculado usando la clave privada de A. En la recepción de este paquete, B checa que el secreto encriptado efectivamente viene de A checando el resumen usando la clave pública de A, obteniéndola del certificado de A, entonces procede a desencriptar el secreto usando la clave privada de B.

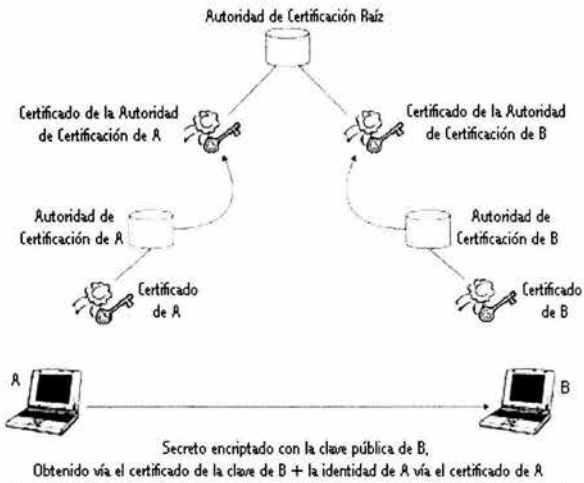


Figura 2.9 PKI basada en la jerarquía distribuida de la Autoridad de Certificación

Los certificados pueden ser emitidos en varios formatos. El estándar de seguridad de facto ampliamente aceptado por la industria es [X509] definido por la ITU. Entidades públicas y privadas confían en los servicios proporcionados por una autoridad certificadora común y aceptan sus certificados de la infraestructura PKI. Los miembros de grupos de la infraestructura PKI pueden identificarse fácilmente de otros basados en certificados proporcionados por la autoridad certificadora. Para este propósito los miembros de la infraestructura solo necesitan establecer relaciones de confianza con un miembro de la infraestructura, la autoridad certificadora y no con los otros miembros. Así, en corto, la infraestructura PKI puede ser definida como una entidad virtual compuesta por múltiples entidades físicas con una serie de políticas y reglas ligadas a claves públicas para las identidades de las entidades emisoras de claves vía el uso de una autoridad certificadora.

Las tres principales funciones de la infraestructura PKI incluyen:

- Certificación
- Validación
- Revocación

La *certificación*, u obligación de una clave para identificación mediante una firma, es ejecutada por la autoridad certificadora, mientras que la *validación*, o más específicamente, la verificación de la autenticidad de un certificado, puede ser ejecutada por cualquier entidad de la infraestructura. Este proceso de certificación incluye la generación de pares de claves públicas, que incluyen claves públicas y privadas, generadas por el usuario y sometidas a la autoridad certificadora como parte de una solicitud, o generadas por la autoridad certificadora en provecho del usuario. La validación involucra checar la firma emitida por la autoridad certificadora en la lista de revocación de certificados y la clave pública de la autoridad certificadora. La *revocación* de un certificado existente antes de su fecha de expiración es ejecutada por una autoridad certificadora. Después de que el certificado es revocado, la autoridad certificadora actualiza la lista de revocación de certificados con la nueva información. En un escenario típico, cuando el usuario necesita obtener o validar un certificado que ha sido presentado, emite una solicitud a la autoridad certificadora. Después de que el certificado solicitado es emitido o es válidamente verificado, la información apropiada es enviada por la autoridad a un depósito de certificados.

La infraestructura PKI es un concepto de redes relativamente reciente definido por estándares del IETF y la ITU, que está siendo rápidamente adoptado por la industria de las redes de datos. Los servicios de autenticación y de administración de claves proporcionados por PKI vía el uso de certificados son un perfecto mecanismo para soportar los requerimientos de seguridad de VPN. Para usar estos servicios, los clientes y los *gateways* VPN deben soportar las funcionalidades PKI tales como generación de clave, solicitudes de certificado, y relaciones con la autoridad certificadora común.

2.1.6.3 SSL y TLS

La tecnología SSL (*Secure Sockets Layer*), originalmente desarrollada por *Netscape Communications Corporation*, es vista como una manera fácil y barata para proporcionar servicios similares a los proporcionados por VPNs IP cuando la necesidad de seguridad de la comunicación IP entre pares de terminales es solo ocasional, depende de la aplicación, o cuando un nivel extra de seguridad es requerido para proteger las aplicaciones de intercambio de datos. La razón es simple: SSL es usualmente inluido en los navegadores comerciales de Internet y no requiere ningún software adicional del lado del cliente y además no involucra al usuario final en el establecimiento de una conexión segura. En años recientes SSL se ha convertido muy popular para aplicaciones de comercio electrónico y pagos en línea y para soportar transacciones seguras se requiere una pequeña participación del usuario.

La tecnología SSL es implementada en las capas de aplicación y de sesión del modelo de referencia OSI. Una sesión de comunicación SSL es implementada entre el cliente SSL y el servidor SSL en una red privada creando una conexión punto a punto en la capa de sesión para aplicaciones basadas en TCP/IP. El establecimiento de una sesión SSL involucra autenticación vía certificados X.509 y encriptación de hasta 168 bits tan fuerte como 3DES usado en IPSec basado en VPNs. Una conexión SSL sencilla soporta sólo una aplicación cliente/servidor, así que los clientes que están corriendo más de una aplicación deben establecer una conexión SSL por aplicación.

Recientemente SSL ha sido sucedida por TLS (*Transport Layer Security*), definido como el estándar de seguridad de la capa de aplicación/sesión. TLS trabaja incluyendo software de cliente TLS en la aplicación del usuario que puede localizar a un par situado en la aplicación del servidor. El cliente y el servidor se autentican mutuamente vía un protocolo RSA (por *Rivest-Shamir-Adleman*) basado en la encriptación de clave pública (usando certificados) llamado *TLS Handshake Protocol*. Durante la fase de saludo de TLS, los pares intercambian claves simétricas para ser usadas en la fase de comunicación, llamadas *TLS Record Protocol*, para correr un protocolo de encriptación de claves simétricas –por ejemplo, 3DES. Al igual que SSL, TLS es usado para soportar aplicaciones seguras basadas en Web tales como bancos en línea y acceso a servicios corporativos, como correo electrónico, calendarización, y acceso seguro a bases de datos corporativas.

2.1.7 Etiquetado con MPLS (*Multi-Protocol Label Switching*)

MPLS es el mejor ejemplo conocido de una tecnología de etiquetado. Las tecnologías de etiquetado son muy similares a las tecnologías de *tunneling*. Con las tecnologías de *tunneling*, los paquetes que son pasados a través de un túnel son entregados desde el punto de ingreso del túnel hasta el punto de salida del túnel por los ruteadores. Con MPLS, los paquetes son transportados desde un punto de ingreso de una trayectoria de conmutación de etiquetas (LSP, *Label Switching Path*) hasta un punto de egreso de la LSP buscando una etiqueta perteneciente a ésta en cada salto.

La construcción de túneles y el etiquetado tienen algunas diferencias, las cuales se destacan en la figura 2.10:

- La etiqueta tiene significancia salto-por-salto.

- La instalación de una trayectoria de conmutación de etiquetas requiere instalar una etiqueta de información base con la información apropiada en cada salto.

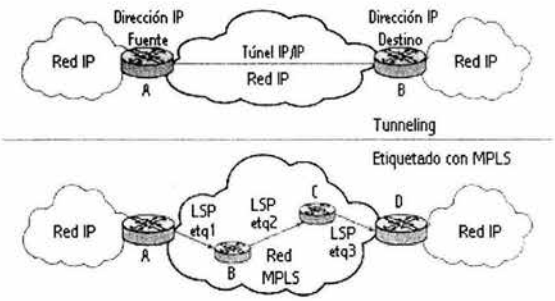


Figura 2.10 MPLS (etiquetado) vs *tunneling*

Por ejemplo, en el ruteador B, debe existir un mapeo entre la etiqueta de entrada, Etiqueta 1, y la etiqueta de salida, Etiqueta 2, y es requerido un protocolo de señalización para instalar esta información en cada nodo. En contraste, un túnel pueder ser instalado por Operaciones, Administración, y Mantenimiento (*OA&M*) en el extremo de la red, y cualquier protocolo de señalización no afecta a los ruteadores que intervienen en la trayectoria atravesada por los paquetes desde el punto de ingreso al punto de salida. Además, las LSPs, pueden ser instaladas de acuerdo a una trayectoria de encaminamiento específica. La trayectoria de entrega puede ser seleccionada basándose más en criterios de ingeniería de tráfico y no sólo por la elección de la trayectoria más óptima.

Aunque el etiquetado y la construcción de túneles siguen objetivos similares, tienen una serie de aplicaciones diferentes. Ya que cada salto que interviene en la trayectoria es afectado por la señalización MPLS y tiene que guardar el estado MPLS, entonces, intuitivamente, MPLS no puede ser usado con la granularidad de las tecnologías de *tunneling*. Esto es, una LSP usualmente agrega mucho más flujos IP que un túnel. Un túnel puede sin duda ser establecido entre dos terminales y estar dedicado solo a ellas (por ejemplo, un cliente VPN y un *gateway*), y acarrear tráfico significativo a solo estas dos terminales. Por otra parte, MPLS normalmente es una tecnología sólo de ruteadores, ya que la granularidad de una LSP está normalmente asociada con un número de sesiones de usuario. Además, reconociendo que MPLS puede presentar problemas de escalabilidad en las redes centrales, los estándares permitidos para apilar etiquetas, hacen posible agregar un número de LSPs en la central y conmutarlas de acuerdo a una etiqueta exterior común añadida a cada etiqueta LSP individual.

Aunque en principio es posible mandar paquetes por un túnel recursivamente –esto es, envolver muchos túneles IP dentro de un túnel IP externo- esto es algo que no se emprende intencionalmente muy a menudo, y sucede más por casualidad, cuando túneles IP son portados sobre otro túnel IP dentro de su trayectoria extremo-a-extremo.

MPLS nació de la fusión de múltiples propuestas de vendedores como *Cisco Systems, Ascend Communications, e IBM* que definieron los conceptos fundamentales y la arquitectura para redes basadas en MPLS.

La arquitectura MPLS está basada en dos clases de ruteadores MPLS: ruteadores LERs (*label edge routers*) y ruteadores LSRs (*label switching routers*). Los ruteadores LERs están ubicados en el extremo de un dominio MPLS y clasifican los paquetes que entran en el dominio en clases equivalentes de entrega (FECs, *forwarding equivalence clasess*). La clase equivalente puede estar basada solo en la dirección IP destino, en la combinación de una interfaz virtual de entrada y la

dirección IP destino, y otras políticas. El ruteador LER puede ser configurado estáticamente para saber qué etiqueta aplicar a qué FEC, por ejemplo, cuando una clasificación compleja de políticas está definida localmente en el ruteador LER. Alternativamente, cuando los protocolos de ruteo están conduciendo la asociación de las FECs con las etiquetas, la asociación está definida dinámica y automáticamente. Esta propiedad puede ser usada para hacer el aprovisionamiento de VPNs multisitio automáticas, aplicando la extensión BGP apropiada. Una vez que los paquetes son clasificados y una etiqueta es asignada a la FEC, la entrega en el siguiente salto LSR del dominio MPLS estará basada únicamente en el valor de la etiqueta. En cada LSR intermedio, un protocolo de instalación de etiqueta establece una información base que define la asociación de una interfaz de entrada y una interfaz de salida. El protocolo de instalación de etiqueta puede ser LDP (*Label Distribution Protocol*) o RSPV extendido con objetos de etiqueta MPLS (conocido como extensiones RSPV para túneles LSP).

Ahora veamos cómo la información de la etiqueta es asociada a cada paquete enviado entre un par de nodos MPLS. Hay dos formas de realizar esto. Un método es asociando la etiqueta a los campos de los protocolos de las capas bajas (por ejemplo, los campos ATM VPI/VCI o el Frame Relay DLCI). El otro es insertando un encabezado entre las capas bajas y el protocolo IP, comúnmente conocido como el enfoque "*shim header*". Note que el enfoque *shim header* toma en cuenta el apilamiento de etiquetas, permitiendo así la agregación de múltiples LSPs en una LSP sencilla en diferentes niveles de jerarquía. Una etiqueta dentro de la pila de etiquetas es una cadena de bits con longitud de 4 bytes y es codificada según como lo describe la figura 2.11.

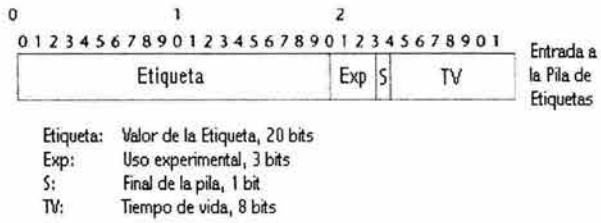


Figura 2.11 Opciones de la pila de etiquetas para el encabezado codificado

La codificación de la pila de etiquetas incluye un campo que debemos tener en mente: el campo EXP. Este campo es usado por las LSRs para clasificar los paquetes pertenecientes a la misma LSP en hasta ocho clases diferentes, esto permite manejar la diferenciación de tráfico dentro una LSP.

2.2 Calidad de Servicio y VPN

El desarrollo de la calidad de servicio en las redes IP se convirtió en un tópico muy importante en la segunda mitad de la década de los 90's, debido a la fenomenal explosión de los servicios basados en IP después de la introducción del *World Wide Web*.

La diferenciación de los paquetes enviados basada en clases de tráfico (incluyendo voz) o sumas de tráfico que comparten un funcionamiento de envío común dentro de los ruteadores ha probado ser el enfoque más razonable y escalable para ofrecer QoS de extremo-a-extremo en Internet. Después de que fue probado que la iniciativa de Servicios Integrados (*IntServ*) –la cual se definió para servicios de flujo de paquetes de extremo-a-extremo basada en la identificación del flujo dentro de cada ruteador a través de la trayectoria- no era escalable en la central IP de alta velocidad, el IETF decidió optar por una menos ambigua, para la diferenciación QoS de las clases de tráfico. Este enfoque es conocido como Servicios Diferenciados (DS), o *DiffServ*.

2.2.1 Tipos de Funcionamiento por Salto

DiffServ está basado en la clasificación de los paquetes en cada salto –esto es, en cada nodo a través de la trayectoria de extremo a extremo– dependiendo de un campo particular en el encabezado IP, llamado campo DSCP (*Differentiated Services Code Point*). Después de que los paquetes han sido clasificados, el nodo con rendimiento *DiffServ* está esperando entregar un PBH estándar (*Per-Hop Behavior*). Cada nodo debe ser configurado para asociar un PBH a un valor particular del campo DSCP.

Hasta ahora, el IETF ha definido un número de PBHs estándares:

- *Default* PHB—mejor conocido como *Best Effort*—proporciona tratamiento de los paquetes para Internet.
- *Class Selector* PHB define hasta ocho funcionamientos configurables, los cuales incluyen el *Default PHB*. Este PHB define un esquema de compatibilidad para el mecanismo de clase precedente.
- *Assured Forwarding* PHB (AF PHB) define cuatro clases de servicio con tres niveles de caída de precedencia cada una, que permiten la diferenciación de diferentes clases de tráfico y la modulación de pérdidas y retarda la ejecución de figuras en cada clase basado en el espacio del *buffer*, gestión del *buffer*, políticas de horarios, y asignación del ancho de banda a cada una de ellas. La caída de precedencia debe ser cambiada a una caída de precedencia más alta si, una clase AF particular de tráfico excede un grado el perfil de tráfico. El administrador debe decidir marcar el tráfico proveniente de diferentes usuarios con diferente caída de precedencia antes de que el tráfico AF sea medido y comprobado con el perfil de tráfico negociado. Por ejemplo, puede ser una política del administrador marcar el tráfico de los empleados con caídas de precedencia más altas que la del vicepresidente y personal de niveles superiores. Los acuerdos de condiciones de tráfico para el tráfico AF deben estar definidos para cada clase de tráfico y para algunas caídas precedentes, dentro de una clase de tráfico existe un nivel de tráfico permitido, y hay reglas para el movimiento del tráfico de una caída precedente a otra.
- *Expedited Forwarding* PHB (EF PHB) garantiza un límite en la variación del retardo en cada salto, tomando en cuenta un servicio que es apropiado para aplicaciones como emulación de circuitos sobre IP.

La entrega de un servicio predecible en un dominio de servicios diferenciados está basado en una buena definición de las reglas para la admisión de tráfico. El tráfico intercambiado con otros dominios está asentado dentro de los acuerdos de condiciones de tráfico definidos bilateralmente entre las entidades administradoras de los dominios. Si todas las redes cumplen con los acuerdos, y si los recursos dentro de los nodos de cada dominio diferenciado son proporcionados adecuadamente, entonces es posible obtener una calidad de servicio predecible de extremo a extremo.

2.2.2 QoS y Túneles

Cuando un paquete IP pasa por un túnel, puede atravesar múltiples dominios *DiffServ*, permanecer dentro de un dominio *DiffServ*, o igual transitar dominios no *DiffServ*. Estas condiciones necesitan ser tomadas en cuenta cuando se está diseñando un servicio basado en túneles y es ofrecido QoS basado en servicios diferenciados.En corto, [RFC2983] describe dos modelos básicos:

- En el modelo "envoltura transparente", el túnel simplemente ocurre para ser una envoltura transparente desde un punto de vista de *DiffServ*, en el que el campo DSCP del paquete interior es copiado en el campo DSCP del encabezado del paquete exterior en el punto de ingreso al túnel. Entonces el valor del campo DSCP del encabezado del paquete IP exterior es copiado en el campo DSCP del encabezado del paquete IP interno en el punto de egreso del túnel.

- En el modelo "tubo" el túnel es considerado un servicio portador con un perfil de QoS dado, y el campo DSCP del encabezado de los paquetes IP enviados sobre el túnel no es copiado en el encabezado IP externo (y, de igual manera, el campo DSCP del encabezado IP externo no es copiado en el campo DSCP del encabezado IP interno cuando el paquete es recibido en el túnel de salida). El modelo de tubo, por consiguiente, puede ser considerado como un circuito (virtual) caracterizado por un perfil de servicio determinado por la clase de Servicios Diferenciados pertenecientes al encabezado externo del paquete IP.

Para satisfacer los requerimientos de QoS de todos los flujos IP transportados sobre una VPN basada en túneles del modelo de tubo, la clase de Servicios Diferenciados que necesita ser negociada con el proveedor de servicio debe cumplir los más rigurosos requerimientos de QoS de todos los flujos IP transportados sobre el conducto. Esta forma resulta ser muy cara si solo una pequeña fracción del volumen del tráfico transportado sobre el túnel requiere un alto nivel de QoS. En este caso, puede ser aconsejable definir un paquete de VPN basada en túneles del modelo de tubo, en lugar de usar una conectividad sitio-a-sitio basada en un túnel sencillo.

Por el contrario, debemos acentuar que si tenemos un mapeo uno-a-uno entre el campo DSCP del usuario y el campo DSCP del encabezado exterior en el punto de ingreso, tal mapeo puede cambiar en el egreso. Lo más importante es que la información del encabezado IP interior, como la caída precedente AF marcada en el ingreso, no cambie en los nodos intermedios. Esta última propiedad es muy importante, por ejemplo, cuando la información de la caída de procedencia necesita ser preservada desde el ingreso hasta el egreso del túnel.

La figura 2.12 proporciona una sinopsis de lo que se presentó en los párrafos anteriores. El modelo "tubo" se aplica especialmente a túneles IP, donde por muchas razones es deseable no copiar el campo DSCP oculto del encabezado IP. Por ejemplo, si un atacante conoce que el tráfico de una misión crítica para una red particular fue marcado con un valor dado del campo DSCP, copiando el campo DSCP oculto del encabezado del paquete IP en el encabezado externo, el atacante podría descubrir que algunos paquetes deben ser colectados para un análisis de las transacciones de la misión crítica. El modelo de tubo es además usado cuando información como la caída de procedencia AF no debe ser perdida (la caída de procedencia AF podría perderse en ciertas situaciones, como cuando un dominio intermedio convierte todo el tráfico a EF). En algunos casos el punto de salida del túnel debe aplicar algún condicionamiento al tráfico antes de pasar por el túnel, como cuando la remarcación es requerida antes de pasar los paquetes sobre un túnel del modelo de tubo, ya que, por ejemplo, el dominio destino no tiene capacidad *DiffServ* y sólo acepta paquetes marcados de acuerdo al modelo IP de precedencia.

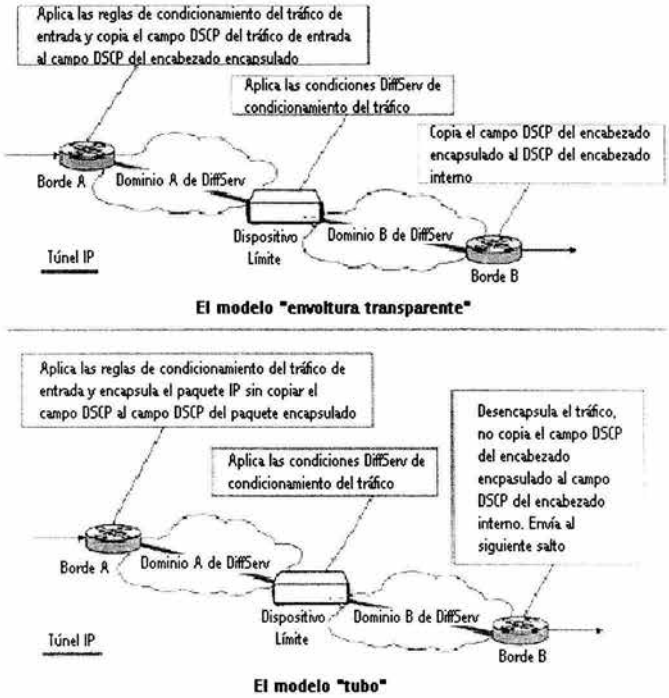


Figura 2.12 Los modelos de "envoltura transparente" y de "tubo"

2.2.3 QoS y MPLS

La diferenciación QoS en una red MPLS puede obtenerse de dos maneras. Usando el campo experimental (EXP) en el encabezado de encapsulación de la pila de etiquetas tomando en cuenta la diferenciación de hasta ocho clases de tráfico dentro de una LSP. En este enfoque E-LSP, el par valor de EXP-valor de la etiqueta para los paquetes entrantes en la interfaz de entrada de la LSR determina el funcionamiento por salto. El otro enfoque está basado simplemente en la asociación de un PHB a un valor de la etiqueta MPLS. Este modo es conocido como L-LSP. No hay diferencia en el nivel de QoS que puede ser desarrollado usando estos dos enfoques diferentes. Sin embargo, la habilidad para usar el campo EXP para la clasificación de paquetes requiere la implementación de un nodo especial.

2.3 Autenticación, Autorización y Contabilidad

La entrega de cualquier tipo de servicio a los clientes por parte de los proveedores de servicio normalmente requiere tres componentes fundamentales para que el proveedor de servicio pueda llevar la factura por el uso del servicio y negar el servicio a clientes no deseados. Estos componentes son Autenticación, Autorización, y Contabilidad (AAA, *Authentication, Authorization, and Accounting*):

- *Autenticación* es definida como la capacidad o acción del proveedor de servicio para solicitar al usuario de un servicio o recurso pruebe su autenticidad.
- *Autorización* es la acción de un proveedor de servicio para verificar que un usuario cuya identidad es autenticada tiene verdaderamente derecho de acceso al servicio. Sin embargo, para servicios basados en acceso anónimo, puede ser suficiente que un usuario

someta algunas credenciales a confianza. Un ejemplo pueden ser los servicios basados en el acceso por prueba, donde un usuario anónimo obtiene acceso al servicio simplemente sometiendo al proveedor de servicio una prueba (por ejemplo, alguna forma de dinero electrónico o créditos).

- *Contabilidad* es la colección de datos de uso que pueden ser procesados por el proveedor de servicio para emitir facturas o para limitar el uso del servicio mismo. Por ejemplo, en tiempos de dificultades o por política general, una compañía puede decidir poner un tapón en el tiempo en que un empleado permanece conectado utilizando la red corporativa basado en acceso remoto. Un proveedor de servicio puede negar la autorización a un usuario de prepago porque, basado en la información de contabilidad, ha excedido el límite del crédito.

2.3.1 Autenticación y Autorización del Usuario

El proceso de autenticación y autorización del usuario consiste de dos pasos:

1. Reunir material de autenticación o autorización del usuario (proceso *front-end*).
2. Verificar el material (referido como proceso *back-end*). Normalmente, el proceso *back-end* es la parte de funciones AAA del proveedor de servicio.
   El mecanismo *front-end* es dependiente de la tecnología, y el proceso *back-end* tiende a ser independiente de la tecnología.

Ejemplos típicos de mecanismos *front-end* para la colección de material AAA del usuario incluyen la fase de autenticación PPP CHAP (*Challenge Handshake Authentication Protocol*) y PAP (*Password Authentication Protocol*), la información de *login* y la contraseña que se envían por una aplicación cliente de Telnet hacia un servidor Telnet en el inico de una sesión Telnet, una página Web protegida con TLS donde el usuario necesita introducir sus datos e interfaces basadas en tarjetas inteligentes con el protocolo EAP (*Extensible Authentication Protocol*) transfieren información de autenticación a un servidor que interpreta la información de la tarjeta inteligente. Además, hay maneras para medir parámetros biométricos y, por ejemplo, identificar individuos escaneando sus retinas o sus huellas dactilares. En redes celulares, durante el procedimiento de enlace de la estación móvil (esto es cuando el usuario registra con la red su paradero y la red comienza la gestión de la movilidad de la estación móvil) la red reúne los datos de autenticación del usuario que compara con los datos recuperados de la base de datos HLR (*Home Local Register*). Estos pueden venir del ingreso directo del usuario, como en las redes AMPS y CDMA, o de una tarjeta con chip conocida como Módulo de Identidad del Sucriptor (SIM, *Subscriber Identity Module*) en GSM, o USIM en UMTS.

Ejemplos de procesos *back-end* incluyen un archivo de contraseñas localmente almacenado en el dispositivo terminal donde los datos de autenticación están coleccionados o la búsqueda de una base de datos remota para las decisiones de autorización y autenticación. En la industria inalámbrica, por ejemplo, la proposición seleccionada para la autenticación de los suscriptores es descargar del nodo servidor toda la información necesaria para comprobar los datos de autenticación colectados de las estaciones móviles. Una vez que este proceso es completado, la estación móvil es entonces autorizada para usar los servicios de la red inalámbrica de datos. El acceso a las redes de paquetes de datos vía una red inalámbrica requiere un nivel adicional de autenticación.

2.3.2 Colección de los Datos de Contabilidad

Existen dos enfoques para la reunión de los datos de contabilidad. Un enfoque es almacenar datos localmente en el nodo de servicio, como un servidor NAS, o una aplicación de terminal. Los inconvenientes de este enfoque incluyen problemas de seguridad, de destino compartido (si el nodo falla, los datos de la contabilidad pueden perderse), y muy a menudo un procedimiento demasiado complejo para reunir los datos de contabilidad si el usuario es móvil y puede acceder a múltiples nodos de servicio. El enfoque preferido está basado en el envío de los datos de

contabilidad a un *gateway* o un servidor y entonces permitir al sistema de facturación accesar a un punto centralizado de contacto para recuperar los datos de contabilidad. Sin duda, esta funcionalidad centralizada de colección de los datos de contabilidad requiere plataformas altamente confiables, protección de la integridad de los datos, y mecanismos de recuperación de desastres, pero todos estos requerimientos tienen que ser satisfechos solo una vez, mientras que los nodos de servicio locales no tienen que soportar tal funcionalidad tan compleja y especializada.

Examinemos cómo es el proceso de contabilidad en los sistemas inalámbricos (figura 2.13). En los sistemas GPRS, los datos de contabilidad son transferidos a una función centralizada CGF (*Charging Gateway Function*) en base a los formatos CDR (*Charging Data Record*) especificados en ASN-1 usando el protocolo GTP. Además en GPRS, en algunos casos, como en el acceso a una red corporativa o ISP, la corporación y el ISP pueden colectar los datos de contabilidad usando RADIUS en lugar de o simultáneamente con CGF, y el portador inalámbrico puede decidir apagar el protocolo GTP o mantenerlo activo, dependiendo si tarifas planas o cuentas basadas en el uso son entregadas a los suscriptores o si los datos son reunidos para análisis. En CDMA2000, los datos de contabilidad son colectados usando RADIUS, compartiendo el mismo método utilizado en la industria de las redes de datos.

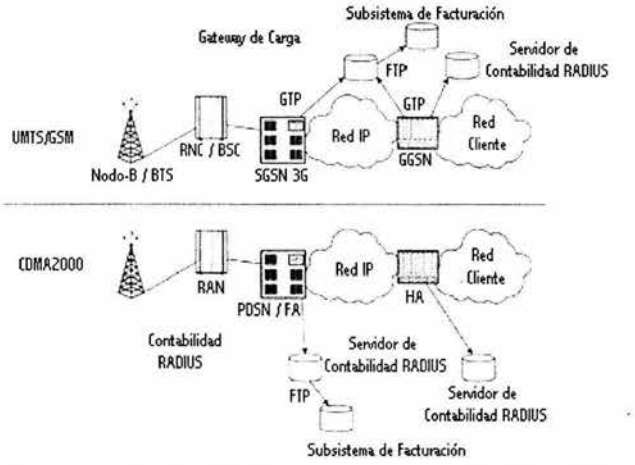


Figura 2.13 Arquitectura para la colección de datos de contabilidad en UMTS/GPRS y CDMA2000

2.3.3 AAA y Servicios de Acceso a la Red: RADIUS

En el acceso por marcación (*dial-up*) así como en otras aplicaciones de servicio de acceso a la red, ha sido reconocido que almecenar archivos en cada servidor de la red de acceso es impráctico y resulta en dolores de cabeza para la seguridad y la administración. Consecuentemente, el IETF eligió un enfoque basado en un protocolo cliente/servidor para presentar funciones de AAA. El estándar define un protocolo base para la autenticación y la autorización (RADIUS) y su extensión para la contabilidad (*RADIUS Accounting*). El servidor de acceso a la red reúne los datos de autenticación utilizando uno de los protocolos descritos en las siguientes secciones, y entonces pregunta a un servidor RADIUS enviándole un mensaje de solicitud de acceso para obtener una decisión sobre si se admite al usuario en la red. Si el usuario es admitido, el servidor RADIUS regresa un mensaje de aceptación de acceso; si no, regresa un mensaje de rechazo de acceso. Dentro del mensaje de aceptación de acceso, el servidor RADIUS puede incluir atributos para la configuración del servicio de acceso a la red entregado al usuario, tales como la dirección IP del usuario, la duración permitida de la sesión, y la información de la dirección IP y de la contraseña necesarias para pasar las tramas PPP por un túnel hacia un LNS usando L2TP.

2.3.3.1 Métodos de Autenticación para el Acceso a la Red

En la industria de las redes de datos, las funciones AAA han estado basadas en el uso de PPP, además de que la mayoría de los métodos de autenticación de acceso a la red han sido desarrollados para soportar autenticación PPP. La fase de autenticación toma lugar después de que la fase de configuración del enlace PPP ha sido completada y antes de que la fase de configuración de la red comience, así que si la fase de autenticación no es exitosa, no se lleva a cabo la fase de configuración de la red, el enlace se cae, y el acceso a la red es negado. En los párrafos siguientes, consideramos tres de los métodos más populares: PAP, CHAP, y EAP.

El protocolo de autenticación de contraseña (PAP) es un protocolo simple que permite a un punto final PPP –normalmente una terminal- entregar el nombre de usuario y la contraseña a su par – normalmente un servidor NAS- de modo que el par puede checar su validez y permitir o negar la continuación de la sesión PPP y subsecuentemente el acceso a la red. Este protocolo tiene una debilidad; un atacante puede guardar el valor del nombre de usuario y la contraseña enviados al descubierto mediante PAP y montar ataques basados en *playback* sobre el servidor NAS.

En respuesta, el IETF definió una forma para proteger de ataques el proceso de autenticación vía un protocolo nombrado CHAP (*Challenge Handshake Authentication Protocol*). En este protocolo, un punto final PPP puede periodicamente exigir a un par usando una cadena de bits aleatoria, llamada *challenge,* y el nodo par debe responder con una respuesta basada en un secreto compartido con el *challenger endpoint,* usando el valor del *challenge* de acuerdo a una función de MD-5 [RFC1321]. El punto final compara entonces el valor del MD-5 contenido en la respuesta con un valor esperado. Si los resultados concuerdan, entonces la sesión PPP puede continuar; de otra manera el enlace es desconectado.

La flexibilidad en el protocolo de autenticación mientras que la fase de autenticación está ocurriendo permite a los protocolos de autenticación evolucionar sin una sustitución de software en los puntos extremos PPP. Sin duda, la selección del protocolo de autenticación típicamente ocurre en el tiempo de configuración del enlace PPP, y los puntos extremos del enlace PPP necesitan tener la implementación en hardware de todos los protocolos de autenticación necesarios y la capacidad de negociarlos en la fase de establecimiento del enlace.

El protocolo de autenticación extensible (EAP) ha sido definido de modo que la selección del protocolo de autenticación puede ser aplazada hasta la fase de autenticación y de modo que un servidor *back-end* puede ser utilizado para implementar los algoritmos de autenticación, en vez de requerir los puntos extremos para implementarlos. Sin duda, un punto final PPP puede ser agnóstico para el mecanismo de autenticación y simplemente intercambiar mensajes EAP hacia servidores de autenticación externos que implementan los mecanismos de autenticación. Esto permite, por ejemplo, mejorar la calidad de la autenticación de los clientes en las terminales de los usuarios y en los servidores en la red del operador sin impactar la infraestructura. Esto puede hacer posible una migración más suave del acceso basado en contraseña hacia el acceso basado en tarjetas inteligentes y no requiere duras citas para la migración de todos los nodos. Por ejemplo, un NAS puede encaminar tramas EAP hacia diferentes servidores de autenticación dependiendo del valor del protocolo de autenticación seleccionado.

El método de autenticación basado en el nombre de usuario y contraseña, no ha sido muy popular con los administradores de red porque el mantenimiento de las contraseñas significa mucha carga para el *staff* de soporte. En despliegues de red demasiado grandes, los cambios frecuentes de contraseñas son contraproductivos, ya que esto normalmente empuja a los usuarios a escoger contraseñas simples que pueden ser algoritmicamente cambiadas (por ejemplo, adjuntando dos dígitos) en el extremo de un prefijo de contraseña que no cambia. Por consiguiente, los métodos de autenticación de tres factores se están haciendo muy populares, ya que no requieren del usuario para administrar una contraseña. De hecho, el usuario requerirá recordar su identidad (nombre de usuario) y un PIN (*Personal Identity Number*) secreto que normalmente no requiere ser cambiado cada vez. El usuario entonces lee algunos dígitos de una tarjeta de señal segura y los

introduce en un área apropiada en la ventana de inscripción, o un lector del chip de la tarjeta anexa automáticamente esos dígitos para permitir la generación de una contraseña una sola vez.

2.3.4 AAA y *Roaming*: El Identificador de Acceso a la Red

Cuando un suscriptor desea utilizar el mismo servicio que en la red local –esto es, la red en la que la relación cliente-vendedor toma lugar- cuando vaga hacia redes de diferentes proveedores de servicio (conocidas como redes visitadas o exteriores), la red visitada y la red local deben ser capaces de intercambiar información AAA. La forma en que esto ha sido manejado en la industria es de que el servidor AAA de la red visitada dialogue con el servidor AAA de la red local en una configuración conocida como *proxy* RADIUS. En esta configuración, el servidor AAA de la red visitada actúa como un cliente AAA del servidor AAA de la red local. Esto requiere que la red visitada sea capaz de encaminar los mensajes AAA hacia el servidor AAA local conveniente. El IETF ha presentado el método definiendo un identificador de usuario compuesto del nombre de usuario y del dominio. El formato del identificador es *usuario@dominio*, y se conoce como un identificador de acceso a la red (NAI, *Network Access Identifier*).

Cuando un identificador de usuario con formato NAI es recibido en un mensaje AAA, el servidor AAA de la red visitada puede interpretar la parte de dominio del NAI y encaminarla al servidor AAA de la red local. Este modelo implica que exista una relación de confianza entre la red visitada y la red local, lo cual requiere la instalación de seguridad entre el servidor AAA de la red visitada y el servidor AAA de la red local. Esto no es muy escalable, ya que tiene una complejidad de n2 –esto es, cada proveedor de servicio necesita instalar seguridad con todos los proveedores de servicio-. Esto ha sido manejado permitiendo a terceros actuar como un intermediario o corredor. En este arreglo, el corredor es la entidad con la cual cada proveedor de servicio establece una relación, y esto reduce la complejidad hasta ser lineal. En otras palabras, el proveedor necesita un arreglo simple de seguridad, y la complejidad es descargada al corredor, el cual se convierte en una entidad especializada para manejar los acuerdos y en este proceso debe ofrecer el establecimiento de los servicios. Para mejorar la seguridad, el corredor debe simplemente actuar como un redirector de las transacciones AAA, así que el servidor AAA de la red visitada y el servidor AAA de la red local podrían ser puestos en comunicación directa después de la consulta inicial dirigida al servidor AAA del corredor resultando en la redirección de la transacción hacia el servidor AAA local. Esta característica no es parte de las capacidades de RADIUS y está permitida en el protocolo AAA de siguiente generación, DIAMETER. La figura 2.14 ilustra los dos modelos diferentes.

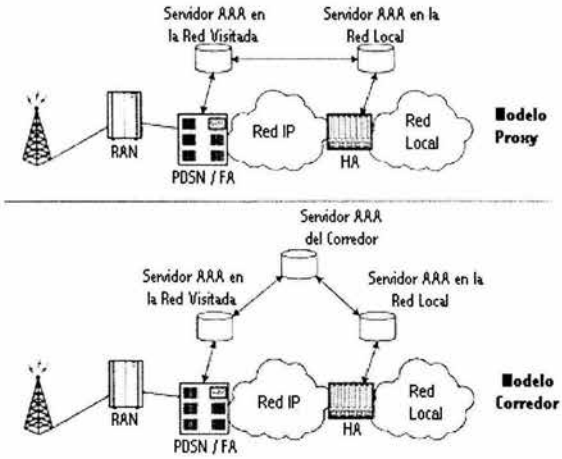


Figura 2.14 Ejemplos de la arquitectura de AAA en los modelos proxy y corredor: CDMA2000

2.3.5 Evolución de AAA: DIAMETER

El protocolo DIAMETER ha sido seleccionado para resolver los problemas relacionados al hecho de que RADIUS es un protocolo cliente/servidor, definiendo una relación par-a-par entre las entidades pares de DIAMETER. Éste permite cosas como procedimientos iniciados en el servidor AAA. Además añade mejoras en la comunicación servidor-servidor, permitiendo mejor funcionamiento en grandes despliegues basados en *proxy*, donde la comunicación servidor-servidor puede conducir cientos de transacciones por segundo. Estas mejoras se extienden sobre el nivel de transporte, con la introducción del protocolo SCTP (*Stream Control Transmission Protocol*); el nivel del modelo de datos, con jerarquías, los modelos de datos orientados a objetos opuesto a RADIUS, y el nivel de seguridad, con la adición de integridad. Además, DIAMETER permite a los corredores AAA actuar como agentes redirectores, haciendo así, directa la comunicación entre el servidor AAA visitado y el servidor AAA local y mitigando la posibilidad de ataques.

La industria inalámbrica está considerando ahora a DIAMETER para muchos otros usos, como para la interacción con un servidor HSS (*Home Subscriber Server*) por servidores SIP en redes inalámbricas. El trabajo sobre DIAMETER está aún en proceso y se requerirá de algún tiempo para ser estabilizado y ser desarrollado comercialmente.

2.4 Servicios de Red

La operación de un proveedor de servicio o empresa de redes, que incluye VPNs, vincula algunos desafíos de configuración y administración que son resueltos con una serie de herramientas, protocolos, y dispositivos. Esta sección proporciona una visión del escenario de los problemas operacionales y la forma en que estos son resueltos.

2.4.1 Administración de Direcciones

Una tarea que puede realmente agobiar a un administrador IT es la asignación de direcciones IP a las terminales. Esto es desafiante porque en la asignación de direcciones existen restricciones relacionadas a la topología, y estas restricciones se convierten en un reto cuando los usuarios se hacen móviles y no permanecen estacionarios dentro de la misma red. Además, el administrador IT debe ser cuidadoso con los conflictos entre los esquemas de direccionamiento público y privado y

del uso de direcciones IP públicas en general. Así un administrador debe ser capaz de evitar los conflictos y además conservar las direcciones IP en grandes despliegues.

Otro problema que frecuentemente afecta a los administradores de red: las redes que no intercambian información de ruteo, tales como una red pública o una red privada, o un par de redes privadas que posiblemente utilizan traslape de espacios de direcciones privadas, algunas ocasiones necesitan intercambiar tráfico. Esto es típico de las redes privadas de las empresas que proporcionan acceso a Internet u otras redes privadas que pertenecen a compañías de negocios o a compañías que han sido recientemente adquiridas. Este problema común es resuelto utilizando Traducción de Dirección de Red (NAT, *Network Address Translation*).

Sin duda, como el número de terminales IP en una red se incrementa hasta cientos de terminales, la complejidad de administrar manualmente el asignamiento dinámico de direcciones IP llega a ser tan alta que ninguna persona puede dedicarse a esta tarea. Esta situación fue la razón para la definición del protocolo de configuración dinámica de terminales (DHCP, *Dynamic Host Configuration Protocol*), el cual es comúnmente utilizado en redes de negocios y campus para asignar direcciones IP a las terminales y configurarlas con otra información necesaria para utilizar los servicios de la red IP. Otra alternativa popular para DHCP es el asignamiento dinámico de direcciones basado en PPP. En este método, el servidor NAS administra los *pools* locales de direcciones IP y las asigna a las terminales durante el establecimiento de la sesión PPP, o el servidor NAS dialoga con un servidor DHCP actuando como un cliente DHCP en nombre de la terminal. Esto posibilita que la infraestructura AAA reparta las direcciones IP al NAS.

2.4.1.1 El Protocolo DHCP

El protocolo DHCP es un protocolo cliente/servidor que permite la configuración IP de las terminales con una dirección IP y otra información como la dirección IP del servidor DNS y la dirección IP del *gateway por default*. El protocolo permite la configuración IP de una terminal sin la necesidad de tener algún conocimiento previo de la red donde está localizada. Como se ilustra en la figura 2.15 el cliente DHCP de la terminal simplemente envía algunos paquetes DHCP de *broadcast* en un intento por comunicarse con algún servidor DHCP sobre el enlace donde el nodo está conectado (mensajes *DHCP DISCOVER*). Los servidores responden con un mensaje *DHCP OFFER*, que contiene un identificador de cada servidor. El cliente recibe los ofrecimientos y selecciona uno de ellos. Entonces responde con un mensaje *DHCP REQUEST* de *broadcast* que contiene también el identificador del servidor. Los servidores que no son identificados por el identificador abandonan la transacción, mientras que el servidor que fue identificado envía un mensaje *DHCP ACK* al cliente aceptando la dirección IP, o envía un mensaje *DHCP NACK*, el cual le notifica al cliente que la información de configuración está fuera de fecha y entonces un nuevo intento de configuración debe ser iniciado. Esto es útil para implementar la característica de *tiempo de arrendamiento*, así como para notificar a los clientes de alguna inconsistencia de la información de configuración. Un cliente DHCP debe liberar una dirección IP que no está en uso por mucho tiempo por medio de un mensaje *DHCP RELEASE* enviado al servidor DHCP.

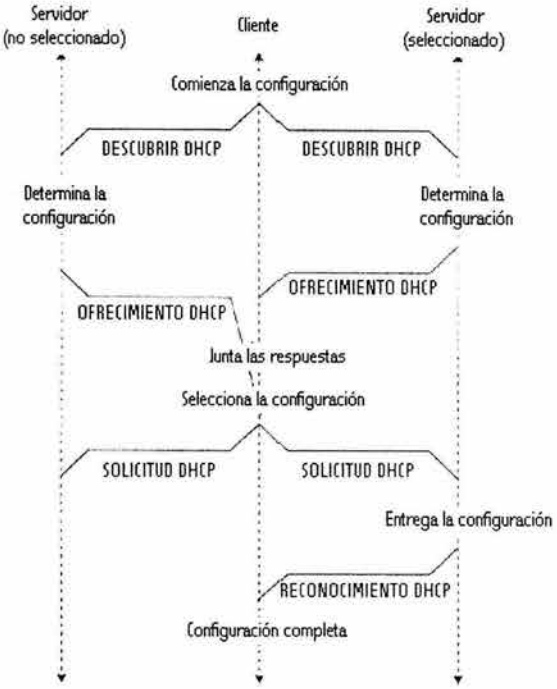


Figura 2.15 Asignación de la dirección IP en base al protocolo DHCP

Además, DHCP puede ser usado para configurar las terminales con información genérica vía el mensaje *DHCP INFORM* que el cliente envía al servidor para obtener información adicional de configuración. El servidor DHCP responde al mensaje *INFORM* vía un mensaje *DHCP ACK* que contiene la información de configuración con las opciones DHCP solicitadas en el mensaje *DHCP INFORM*. El mensaje *INFORM* puede ser *unicast* hacia el servidor directamente cuando su dirección es conocida (como en el caso de cuando la terminal previamente obtuvo la dirección IP vía DHCP). De otra manera, una terminal puede mandar por *broadcast* este mensaje buscando que algún servidor DHCP responda, lo cual normalmente sucedería en sistemas alámbricos cuando la dirección IP fue asignada por otros medios o cuando una terminal basada en PPP requiere información de configuración que el protocolo de control de red (NCP, *Network Control Protocol*) no puede entregar.

2.4.2 Nombramiento de Terminales

Uno de los problemas que usualmente afectaba a los administradores de redes era la necesidad de identificar una terminal IP mediante un identificador que pudiera ser fácilmente utilizado por un humano. De hecho, el escribir la dirección IP de una terminal es una tarea más difícil que escribir una etiqueta alfanumérica entendible, la cual puede estar semánticamente asociada con algo. Además, una etiqueta mnemónica es mucho más amigable y como los humanos son los usuarios de las aplicaciones que necesitan un identificador de terminal como entrada, esto hace que se requiera aún más el uso de las etiquetas para identificar las terminales. Sin embargo, esto acarrea el problema de cómo gestionar el mapeo entre las etiquetas y las direcciones IP, las cuales son necesarias para direccionar a las terminales usando paquetes IP. Esto condujo a la definición y desarrollo de un sistema distribuido de bases de datos llamado DNS (*Domain Name System*) que permite una infraestructura global de resolución para el nombramiento de las terminales IP.

2.4.2.1 Sistema de Nombre de Dominios (DNS)

El Sistema de Nombre de Dominios es un sistema distribuido de bases de datos que permite resoluciones globales de los nombres de terminales para las direcciones IP. Como se ilustra en la figura 2.16, el nombre de una terminal está organizado de acuerdo a una sintaxis, que define el nombre de la terminal para estar compuesto de etiquetas estructuradas, hechas de cadenas alfanuméricas separadas por un punto. Esta notación es conocida como *nombre de dominio completamente calificado* (FQDN, *Fully Qualified Domain Name*) y es de la forma etiqueta1.etiqueta2. ... etiqueta(T-1).etiquetaT. La etiqueta T es llamada dominio de nivel superior (TLD, *Top Level Domain*), y éste puede ser un código de país (por ejemplo, us, fr, uk, it) o uno de los dominios TLD estándares permitidos para Internet –tradicionalmente, com, mil, gov, org, net, int. La etiqueta (T-1) es definida como un dominio, e identifica únicamente a un nombre de espacio administrativamente independiente para el cual el dueño del dominio tiene los derechos para definir el mapeo nombre de terminal-dirección IP definiendo una etiqueta adicional. Una entidad administradora de un dominio puede definir el dominio para estar compuesto sólo por un nombre único –por ejemplo, bigco.com- que trazaría el plan para una o más direcciones IP. Alternativamente, el dominio puede ser hecho por cientos de nombres de terminales que se obtiene añadiendo etiquetas adicionales separadas por punto a las dos etiquetas que identifican el nombre del dominio.

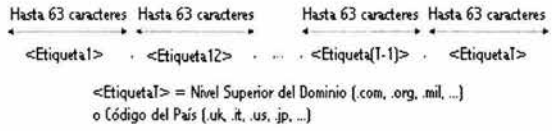


Figura 2.16 Ejemplo de la estructura para el nombramiento de la terminal

Esta notación tiene sus raíces en la operación de la base de datos distribuida DNS. En realidad el DNS está hecho de una zona raíz, la cual está compuesta de 12 servidores que almacenan las direcciones IP de los servidores que pueden resolver el nombramiento de las terminales pertenecientes a todos y cada uno de los dominios DNS. Cuando una terminal intenta resolver un nombre de terminal para una dirección IP, como se ilustra en la figura 2.17 , en primer lugar busca en una memoria interna opcional. Probablemente, esto no brinde resultados, y entonces es ejecutada una consulta hacia un servidor configurado para la red local. Esta consulta puede fallar, y en la mayoría de los casos esto sucede, ya que en el servidor se encuentran sólo aquellos nombres asociados a las direcciones IP administradas por el operador de la red local, por ejemplo, cierto ISP. Cuando esto sucede, el cliente DNS de la terminal consulta al servidor TLD, el cual apunta a la dirección del servidor que puede resolverlo. El cliente entonces puede consultar esta dirección y obtener de ésta la información deseada. Normalmente, es regresada una dirección IP sencilla, pero también pueden ser regresadas múltiples direcciones IP. La terminal que obtiene una lista de direcciones IP puede usar cualquiera de ellas para comunicarse con el servidor deseado. Estas direcciones IP múltiples pueden ser asociadas a las interfaces IP de una máquina o de múltiples computadoras.

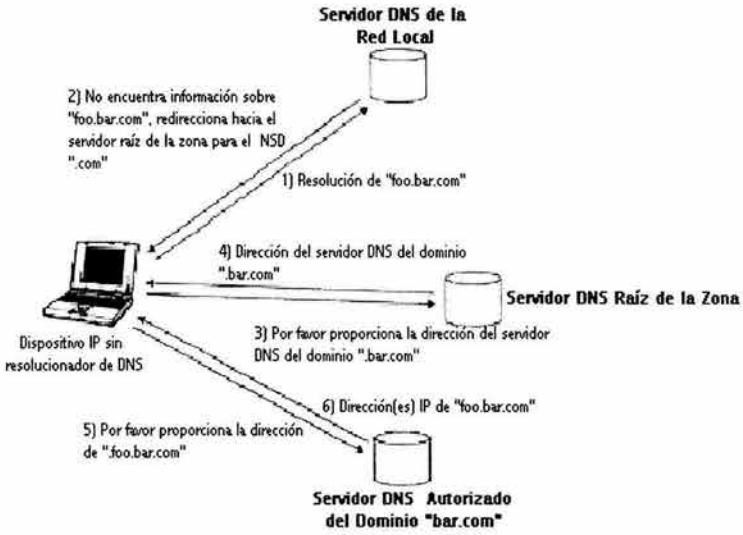


Figura 2.17 Pregunta a un DNS para la resolución del nombramiento de una terminal

Es posible además preguntar al DNS para informarse sobre cúal es el nombre de una terminal asociada a una dirección IP. Esta funcionalidad es muy útil porque una terminal puede ser capaz de verificar el nombre de terminal de un corresponsal, por ejemplo, para checar que realmente pertenece a un dominio que tiene derechos de acceso a algunos recursos. Sin embargo, esta característica no es muy usada, principalmente porque no todos los dominios están configurados para proporcionar este servicio.

Hemos mencionado que una organización que opera una red privada puede definir su propio DNS privado y su propia zona raíz de servidores que atienden a los TLDs propietarios. Este es de hecho el propósito seguido por la asociación GSM cuando definieron el dominio TLD .gprs para ser usado en los sistemas GPRS para construir FQDNs que se utilizan para identificar las direcciones IP de los puntos de terminación de los túneles GPRS en el nodo GGSN. Estos puntos de terminación son conocidos como puntos de acceso, y por consiguiente los identificadores son conocidos como nombres de los puntos de acceso o APNs (*access point names*). La siguiente es la sintaxis de un APN:

APN =-<APN Network Identifier>. <APN Operator Identifier>

<APN Network Identifier> = Any valid DNS name

< APN Operator Identifier> = -<mnc<MNC>.mcc<MCC>.gprs
or -<wireless operator domain name>.gprs

<MNC> = Mobile Network code belonging to the operator

<MCC>= Mobile Country code of the Country where the operator is based

2.4.2.2 Traducción de Direcciones de Red (NAT)

La traducción de direcciones de red (NAT, *Network Address Translation*) es un mecanismo que permite a las redes pertenecer a dos reinos independientes de ruteo y direccionamiento –esto es, redes que pueden usar diferentes esquemas de direccionamiento que no son mutuamente

alcanzables basados en encaminamiento IP de extremo-a-extremo- para intercambiar tráfico. Por ejemplo, las dos redes pueden ser una red corporativa que usa un esquema de direccionamiento privado y una red ISP que usa direcciones públicas, o una corporación y un negocio con redes asociadas ambas usando traslape del espacio de direcciones privadas.

NAT proporciona un mapa transparente de direcciones IP de diferentes grupos para el usuario final. Por ejemplo, el proveedor de servicio puede mapear sus direcciones IP privadas sobre direcciones IP públicamente encaminables cuando el cliente necesite conectarse a Internet. Las tecnologías como NAT son necesarias cuando direcciones IP privadas internas no puedan ser usadas fuera de las redes privadas en un espacio de direccionamiento público por razones de seguridad o compatibilidad. La motivación detrás del uso de NAT es una mejor utilización de las direcciones IP públicas.

Existen dos variaciones del NAT tradicional:

- Traducción de dirección de red IP, además llamado NAT Básico o Estático.
- Traducción del puerto de dirección de red (NAPT, *Network Address Port Translation*), también referida como Traducción de Dirección del Puerto (PAT, *Port Address Translation*).

NAPT puede mapear múltiples direcciones IP para una dirección IP sencilla pero con diferentes números de puerto TCP. Además, un método llamado *NAT Protocol Translation* (NAT-PT) ha sido propuesto para la traducción de direcciones entre IPv4 e IPv6.

NAT trabaja modificando las direcciones de los paquetes IP de tal manera que el dispositivo haga la reescritura NAT de las direcciones de los encabezados para pasar los paquetes de acuerdo a las reglas específicas de traducción de direcciones de la red. Los paquetes son entonces encaminados según la nueva información del encabezado. Esta restricción de acceso a usuarios remotos se ha convertido en un mayor problema con las implementaciones de VPN. La razón está en la incompatibilidad de NAT e IPSec. Una de las funciones de IPSec es el soporte de la integridad de los datos del usuario. Esto significa que IPSec previene cualquier modificación de los paquetes. Ya que la principal función de NAT es cambiar las direcciones destino de los paquetes IP, un proceso NAT desde el punto de vista del *gateway* y del cliente de IPSec será visto como una violación de la integridad y seguridad de los datos del usuario. Esto puede potencialmente romper un túnel, lo cual puede tener consecuencias devastadoras para los servicios VPN. Como resultado, cuando un túnel IPSec es establecido sobre una red que implementa NAT, el paquete de autenticación IPSec fallará. También, IKE sufre de la presencia de NAT, ya que en una negociación IKE, las partes intercambian sus direcciones IP.

Ahora vamos a considerar cómo los diferentes modos de IPSec pueden coexistir con NAT. En los modos IPSec de transporte y de túnel, el encabezado AH autentica el paquete IP entero, incluyendo el encabezado. Cuando un dispositivo NAT cambia la dirección del paquete IP, la nueva suma de comprobación no será válida y el paquete será descartado en el destino. Esto hace a IPSec AH y NAT incompatibles. Contrario al encabezado AH, el encabezado ESP en el modo de transporte proteje solo el encabezado TCP/UDP del paquete y no sus direcciones fuente y destino. Así, en este modo la integridad de extremo-a-extremo de todos los paquetes TCP/UDP que pasan a través de NAT no será violada.

Una forma de resolver este problema de incompatibilidad en general está basado en la asunción de que un dispositivo NAT que está custodiado por una asociación de seguridad de extremo-a-extremo o un túnel de extremo-a-extremo serán remplazados por una serie de dos o más túneles concatenados o encadenados en el dispositivo NAT. Otro enfoque que ha sido recientemente propuesto al IETF es llamado NAT Transversal o NAT-T. NAT Transversal no viola la arquitectura básica de IPSec, y es completamente compatible con dispositivos IPSec estándares. El único requerimiento para soportar NAT-T es la implementación de una serie de capacidades, las cuales deben ser soportadas por los dispositivos que representan los puntos finales del túnel y no afecta a ningún dispositivo sobre la trayectoria de los datos. Si durante la fase de establecimiento del túnel

IPSec es detectado por los puntos finales del túnel que NAT-T es soportado y requerido, el tráfico de cada asociación de seguridad IPSec negociada será encapsulado en paquetes UDP que contienen la información que ayudará a restaurar el paquete cambiado por NAT a su forma original en el punto final del túnel. El tráfico IPSec entre los puntos finales del túnel es encapsulado en UDP usando el puerto IKE (UDP puerto 500). Como resultado, los paquetes encapsulados siguen la misma ruta que los paqutes IKE, lo cual asegura que la modificación de los paquetes hecha por NAT es similar a la modificación hecha por IKE. La longitud del encabezado IP original y el tipo de protocolo son almacenados en el encabezado de NAT-T.

NAT-T ha sido propuesto al IETF por *SSH Communications* y una coalición de *Cisco Systems, F-Secure, Microsoft, y Nortel Networks*. NAT-T permite establecer VPNs extremo-a-extremo aún cuando el proveedor de servicio usa esquemas de direccionamiento privados. El control del equipo puede presentar un problema, como no hay forma de que sea cierto que los dueños de los puntos extremos de la conexión IPSec tengan algún control sobre el equipo entre los puntos extremos. NAT-T presenta una forma más fácil y mucho más elegante de evitar el problema, ya que no requiere cambios de los dispositivos NAT.

CAPÍTULO 3

INTERFACES DE RADIO EN LOS SISTEMAS INALÁMBRICOS

Cuando tratamos con datos inalámbricos, es importante tener un buen entendimiento de los aspectos del acceso de radio y de la infraestructura de la red central. La tecnología de radio acceso (conocida como interfaz de aire) define la tecnología que los dispositivos de datos deben usar para la interfaz con un sistema inalámbrico particular, y las capacidades asociadas a la transmisión de datos. La red central define los protocolos usados por el sistema inalámbrico para interactuar con la estación móvil para su autenticación, configuración, soporte de la movilidad, y administración de la sesión.

Este capítulo proporciona una breve descripción de los estándares inalámbricos de primera, segunda y tercera generación para el acceso vía radio.

3.1 Tres Generaciones Inalámbricas

Las tecnologías celulares están divididas en tres generaciones: primera, segunda y tercera, abreviadas como 1G, 2G, y 3G respectivamente. En el pasado, varios cuerpos de estandarización y consorcios internacionales definieron estos términos muy vagamente. En respuesta a esta situación, publicaciones y académicos han renombrado algunas de las tecnologías en los límites de la definición "G", añadiendo un punto decimal a su designación, tal como 2.5G por ejemplo.

La tabla 3.1 sintetiza las características básicas, nomenclatura, y propiedades de los sistemas celulares.

Tabla 3.1: Propiedades de los Sistemas Celulares

GENERACIONES	1G	2G	2.5 G	3G
Sistemas	NMT,TACS , AMPS	TDMA IS-136, GSM, CDMA IS-95, HSCSD, CDPD	GPRS, CDMA2000-1X, EDGE	CDMA2000-3X, CDMA2000-1X EV-DO UMTS, Enhanced EDGE
Tecnología voz/datos	Circuito de voz, circuito de datos por marcación (dial-up)	Circuito de voz, circuito de datos por marcación (dial-up)	Circuito de voz, circuito/paquete de datos (Internet, servicios IP)	Circuito/paquete de voz, circuito de datos y paquetes de datos de alta velocidad (multimedia, serviciosIP)
Tasa de datos teórica	2.4-9.6 Kbps	9.6 -19.2 Kbps, 28.8 Kbps	9.6-144 Kbps; 70-473 Kbps	144 Kbps -2 Mbps; 144 Kbps-2 Mbps; 256 Kbps -2.4 Mbps
Rendimiento promedio esperado	2–9 Kbps	9-19 Kbps	9–300 Kbps;	60-1000 Mbps
Tecnología de radio acceso	FDMA	TDMA, CDMA	TDMA, CDMA	TDMA, CDMA, W-CDMA, TD-SCDMA

Los sistemas celulares inalámbricos de primera generación proporcionan transmisión analógica de voz basada en el Acceso Múltiple por División de Frecuencia (FDMA) con redes centrales basadas en multiplexaje por división de tiempo (TDM). Ejemplos de sistemas 1G incluyen AMPS (*Advanced Mobile Pone System*), usado en los Estados Unidos, y el sistema NMT (*Nordic Mobile Telephone*), el cual es aún desplegado en muchos países de Europa Occidental. Típicamente, las tecnologías 1G fueron desplegadas dentro de un distrito o un grupo de ciudades y no fueron pensadas para uso internacional.

En contraste con la primera generación, las tecnologías 2G fueron diseñadas para una implementación internacional. Gran énfasis fue puesto en la compatibilidad, en la habilidad sofisticada de *roaming*, y el uso de la codificación digital para transmisión de la voz sobre el aire. Ejemplos populares de sistemas 2G son GSM (*Global System for Mobile Communications*) y cdmaOne (basado en el estándar IS95 de la TIA).

Un sistema celular puede ser clasificado como un sistema 3G si cumple con un número de requerimientos establecidos por la ITU:

- Debe operar en una de las frecuencias del espectro asignadas para los servicios 3G.
- Debe proporcionar al usuario un arreglo de nuevos servicios de datos, incluyendo multimedia, independientemente de la tecnología de la interfaz de aire.
- Debe soportar transmisiones móviles de datos a 144 Kbps para usuarios de alta movilidad (velocidad vehicular),a 384 Kbps para peatones, y transmisiones estacionarias de datos de hasta 2 Mbps (al menos en teoría).
- Debe permitir servicios de paquetes de datos.
- Debe cumplir el principio de independencia de la red central de la interfaz de acceso de radio.

La figura 3.1 resume esta discusión ilustrando los principales sistemas celulares y sus rutas de migración.

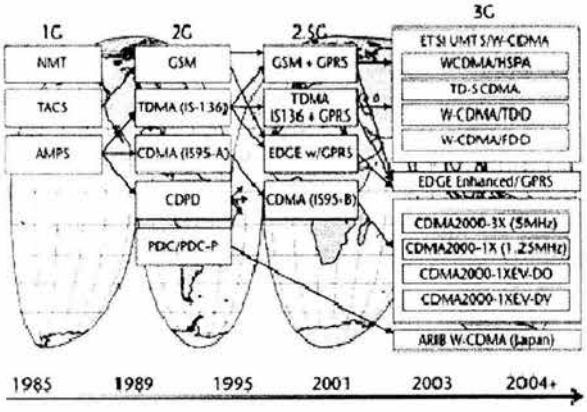


Figura 3.1 Rutas de migración de los sistemas celulares

3.2 Sistemas Celulares 1G

Todos estos sistemas soportan servicios de datos por circuitos y pueden ser utilizados para varias formas de MVPN, sin ninguna dificultad. Esta sección proporciona una revisión de las interfaces de aire utilizadas por los sistemas 1G más ampliamente desarrollados.

3.2.1 AMPS

Todos los sistemas celulares 1G dependen de la modulación de frecuencia analógica para la transmisión de voz y datos y de la señalización en banda para mover la información de control entre las terminales y el resto de la red durante la llamada. El sistema AMPS es un buen ejemplo de la tecnología analógica de primera generación más usada en los Estados Unidos. AMPS está basado en la radio transmisión de FM usando el principio de Acceso Múltiple por División de Frecuencia (FDMA) donde a cada usuario le es asignada su frecuencia para separar los canales dentro del espectro asignado (ver figura 3.2). FDMA está basado en canales de banda estrecha, cada uno capaz de soportar un circuito de teléfono que es asignado a un usuario particular para la duración de la llamada. La asignación de frecuencia es controlada por el sistema, y la transmisión es usualmente continua tanto para la dirección ascendente (*uplink*), como para la dirección descendente (*downlink*). El espectro en tales sistemas es asignado al usuario para la duración de la llamada, la cual está siendo usada para enviar voz o datos.

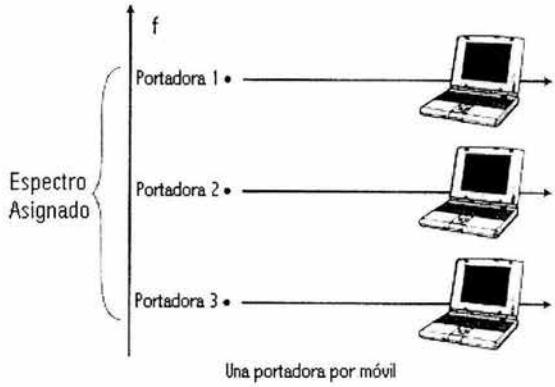


Figura 3.2 Principios del Acceso Múltiple por División de Frecuencia (FDMA)

Así como en otras tecnologías 1G, en AMPS un circuito –representado por una porción del espectro- es asignado al usuario y debe permanecer disponible para éste, similar al par de cobre telefónico usado para las comunicaciones de voz. Similar a la conexión analógica alámbrica, un módem es usado para el acceso a los datos. Los protocolos de corrección de errores usados por los módems inalámbricos tienden a ser más robustos que sus contrapartes alámbricos, debido a la necesidad de tratar con desafíos mayores del ambiente físico con niveles de interferencia y de relaciones señal-ruido más altos que en un par de cobre o una fibra óptica. La tasa de datos más alta para una llamada de un módem AMPS bajo buenas condiciones es de hasta 14.4 Kbps, y tan baja como 4.8 Kbps bajo condiciones malas. Para establecer una conexión AMPS de datos puede tomar en cualquier parte hasta 20 segundos o más.

3.2.2 El Sistema Nórdico deTelefonía Móvil (NMT) y el Sistema de Comunicación de Acceso Total (TACS)

El sistema NMT fue originalmente introducido en 1981 en cuatro países del Norte de Europa – Dinamarca, Finlandia, Noruega, y Suecia- en la banda de fecuencia de 450 MHz. El sistema TACS fue desarrollado tres años más tarde en el Reino Unido y después se expandió a otros países de Europa, como Italia. Ambos sistemas están basados en la tecnología analógica de radio acceso FDMA.

Inicialmente, NMT fue optimizado para ser usado en ambientes rurales de los países Escandinavos. Se asignó una frecuencia de 450 MHz para la instalación de células grandes por

tener mejores características de propagación en frecuencias altas. Como los negocios y las condiciones ambientales cambiaron, NMT fue modificado para operar en el rango de 800 MHz, tomando en cuenta el tamaño y la potencia de los teléfonos. En contraste, TACS fue diseñado para una mayor capacidad de cobertura. Los sistemas TACS operan en las frecuencias de 800 y 900 MHz, lo cual requiere un número mayor de células pero permiten transmisores más pequeños y de menor potencia. Este sistema es muy eficiente y económico para países como el Reino Unido, con alta densidad de población y un gran número de áreas urbanas.

3.3 Sistemas Celulares 2G

Los sistemas celulares digitales de segunda generación constituyen la mayoría de la infraestructura de comunicación celular implementada hoy en día. Los sistemas 2G como GSM, apuntaron hacia un cambio en la forma de uso de las comunicaciones móviles. En parte ayudaron a la transición de un teléfono móvil para convertirse de un objeto de lujo a una necesidad y también ayudaron a que los costos de suscripción bajaran debido a la utilización más eficiente de la interfaz de aire y al volumen desarrollado de teléfonos y componentes de la infraestructura.

Importantes regiones geográficas adoptaron diferentes sistemas 2G, esto es TDMA y CDMA en Norte América, GSM en Europa, y PDC (*Personal Digital Celular*) en Japón. La figura 3.3 describe el número de suscriptores en todo el mundo para los sistemas 2G más importantes. Ésta efectivamente muestra cómo el sistema GSM ha tenido éxito y porque está siendo adoptado en otras áreas geográficas (como Norte América, China, la región Asia-Pacífico, y más recientemente, Sur América). CDMA, que se originó en Norte América, ha proliferado en Sur América y más tarde en la región Asia-Pacífico. TDMA permanece ampliamente desplegado en regiones de Norte y Sur América, pero se espera decline porque la decisión tomada por algunos portadores norteamericanos es convertir sus redes TDMA a GSM.

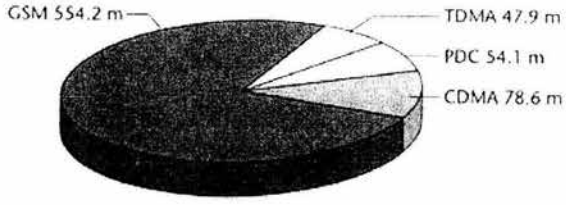


Figura 3.3 Número de suscriptores en todo el mundo para los sistemas 2G más importantes (2002).

3.3.1 TDMA Norteamericano (IS-136)

Este sistema de segunda generación, extensamente desplegado en los Estados Unidos, Canadá, y Sur América, es conocido con muchos nombres, incluyendo TDMA Norteamericano, IS-136, y D-AMPS (*Digital AMPS*).

TDMA ha sido usado en Norteamérica desde 1992 y fue la primer tecnología digital en ser desarrollada comercialmente. Como su nombre lo indica, está basado en el acceso múltiple por división de tiempo. En TDMA los recursos son compartidos por tiempo, combinado con multiplexaje por división de frecuencia (esto es, cuando múltiples frecuencias son utilizadas). Como resultado, TDMA ofrece múltiples canales digitales que usan diferentes ranuras de tiempo sobre una frecuencia portadora compartida. A cada estación móvil le es asignada una frecuencia específica y una ranura de tiempo durante la cual puede comunicarse con la estación base, como se muestra en la figura 3.4.

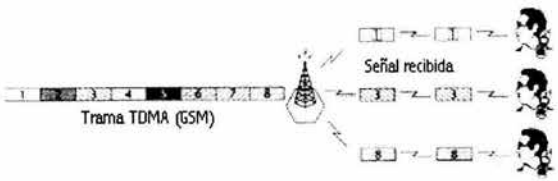


Figura 3.4 Acceso Múltiple por División de Tiempo

El transmisor TDMA está activo durante la ranura de tiempo asignada e inactivo durante otras ranuras de tiempo. El sistema TDMA Norteamericano soporta tres ranuras de tiempo, de 30 KHz cada una, divididas en tres o seis canales para maximizar la utilización de la interfaz de aire. Una secuencia de división de tiempo multiplexa las ranuras de tiempo en TDMA formando tramas, las cuales son de 40 ms de longitud. La tasa total de bits del canal de tráfico de TDMA es de 48.6 Kbps. El control elevado y el número de usuarios por canal, decrementa la efectividad de un canal disponible para el tráfico de usuario a 13 Kbps. TDMA es una tecnología de banda dual, lo que significa que puede ser desplegada en las bandas de frecuencia de 800 y 1900 MHz. En regiones donde están desplegados AMPS y TDMA, los teléfonos TDMA están diseñados para operar en modo dual, analógico y digital, para ofrecer a los clientes la capacidad de utilizar la cobertura de la infraestructura analógica existente.

3.3.2 Sistema Global para Comunicaciones Móviles (GSM)

La iniciativa para el sistema celular GSM fue aceptada en 1982 por la CEPT (*Conference of European Posts and Telecommunications Administrations*) y actualmente está regido por el ETSI (*European Telecommunications Standards Institute*), el cual ha delegado las especificaciones GSM de mantenimiento y evolución al proyecto 3GPP. La intención detrás de la introducción de GSM era tener un enfoque común para la creación de sistemas digitales en los países europeos, para permitir *roaming* internacional y mejorar las economías de escala decrementando los costos de los teléfonos y de los componentes de la infraestructura a través de la producción en masa. Esta fue una decisión inteligente, ya que contribuyó al éxito de los proveedores de infraestructura celular y de los fabricantes de equipos europeos.

El estándar GSM, similarmente al estándar TDMA Norte Americano, está basado en el uso de dos tecnologías de multiplexaje simultáneas, TDMA y FDMA. Cada canal de radio frecuencia (RF) soporta ocho ranuras de tiempo agrupadas dentro de tramas TDMA, las cuales a su vez están agrupadas dentro de multitramas consistentes de 26 tramas TDMA que portan a los canales de tráfico y control. Las multitramas están construídas dentro de supertramas e hipertramas. La asignación de las ranuras de tiempo es esencialmente estática, por ejemplo, la octava ranura de tiempo de un canal RF dado es asignada al mismo usuario cada vez que ésta se restablece, no importa si el usuario tiene o no tiene datos para enviar.

El sistema GSM, soporta tres tipos de servicios: servicios portadores, tele-servicios, y servicios suplementarios. Los servicios portadores de GSM toman en cuenta que la transferencia da datos sea transparente para el usuario y definen los atributos de acceso, los atributos de transferencia de información, y los atributos generales con roles específicos. Los atributos de acceso definen las propiedades y parámetros de los canales de acceso tales como la tasa de bits; los atributos de transferencia definen el modo de transferencia de datos (bidireccional, unidireccional), el tipo de información (voz o datos), y el modo de establecimiento de llamada; los atributos generales definen servicios específicos de red tales como QoS y opciones de interconexión. Los tele-servicios están basados en el fundamento de los servicios portadores y gobiernan las comunicaciones usuario-usuario para aplicaciones de voz o datos. Ejemplos de tele-servicios incluyen Fax de Grupo 3, telefonía, servicio de mensajes cortos (SMS), y comunicaciones de circuitos de datos IP y X.25. Los servicios suplementarios proporcionan características adicionales de valor agregado tales como llamada en espera, envío de llamadas, sin llamada y llamadas en conferencia.

3.3.3 HSCSD (*High-Speed Circuit-Switched Data*)

HSCSD es una opción en GSM que permite combinar mútiples ranuras de tiempo GSM (canales de tráfico) cada uno con capacidad de una tasa de bits de 14.4 Kbps. La tasa de bits resultante disponible para un usuario único puede alcanzar hasta 56 Kbps.

Los portadores inalámbricos pueden llevar a cabo la migración hacia HSCSD actualizando el software de la Central Móvil de Conmutación GSM (MSC, *Mobile Switching Center*) y de la Estación Base Transmisora/Receptora (BTS, *Base Transceiver Station*). Los portadores inalámbricos además tienen que distribuir teléfonos capaces de recibir transmisiones HSCSD o actualizar los productos para las estaciones móviles GSM basadas en PCMCIA (*Personal Computer Memory Card International Association*) y tarjetas CompactFlash (CF) (como las que produce *Nokia*). HSCSD puede ser soportado dentro de la infraestructura para la gestión de la movilidad de GSM, la cual además permite servicio de *roaming* y otros servicios familiares de GSM a tasas de transmisión más altas.

3.3.4 CdmaOne

Acceso Múltiple por División de Código (CDMA) IS-95 –o *cdmaOne*- es una de las tecnologías 2G más populares que está siendo utilizada en América, Asia, y el Este de Europa. CDMA está basada en una técnica en la cual a cada suscriptor le es asignado un código único, conocido como código pseudoaleatorio que es usado por el sistema para distinguir a un usuario del resto de los otros usuarios que están transmitiendo simultáneamente en la misma banda de frecuencia. CDMA pertenece a la clase de sistemas llamados *Sistemas de Espectro Expandido*, y más específicamente a la familia de Espectro Expandido por Secuencia Directa (DSSS, *Direct Sequence Spread Spectrum*). Los canales físicos en CDMA están definidos en términos de la radio frecuencia de la portadora y de un código –esto es, una secuencia de bits. La señal digital resultante de la codificación de la voz o de los datos, después de la aplicación del *framing* apropiado (o las capas de radio enlace), es digitalmente invertida antes de que module a la frecuencia portadora. Esto se realiza añadiendo digitalmente la señal al código pseudoaletorio que es usado para distinguir al usuario. El espectro entero de la portadora está disponible para cada usuario, de ahí el nombre de *espectro expandido*.

El receptor, que tiene un decodificador de señal pseudoaleatoria, reproduce la señal original demodulando la de RF y agregándole (base 2) la misma señal pseudoaleatoria usada por el transmisor, obteniendo así la señal original. CDMA es un sistema de interferencia limitada, lo que significa que en cualquier tiempo un usuario que no está transmitiendo no interfiere con otros usuarios que comparten el mismo espectro, el ancho de banda efectivo, y por lo tanto la relación señal-ruido, disponible para los otros usuarios incrementará en algún grado. Las propiedades de CDMA son las siguientes:

- Múltiples canales de voz están disponibles para cada radio canal.
- Para prevenir la interferencia, los llamadores son asignados a diferentes canales de radio frecuencia (o si comparten un radio canal, se les asigna diferentes códigos pseudoaleatorios).
- El mismo radio canal pueder ser utilizado en células adjuntas.
- El número de llamadas dentro de un sector está "suavemente" limitado.
- El ancho de banda usado influye en el número de usuarios simultáneos.

Para visualizar mejor el concepto de CDMA, imagine un cuarto lleno con parejas de personas hablando una a la otra, cada pareja en su propio lenguaje. Cada persona sólo podría ser capaz de entender a su compañero pero no al resto de las conversaciones en el cuarto. Como el número de pares de personas con lenguaje único incrementa, el nivel de ruido subirá al máximo, después del cual las conversaciones ya no serían posibles.

La tecnología celular CDMA tiene además la capacidad de *handoff* suave –esto es, el sistema especifica un receptor (receptor RAKE) capaz de recibir hasta tres señales relacionadas al mismo canal, por efectos de multitrayectorias o porque múltiples fuentes transmiten la misma señal. El sistema permite a la estación móvil enviar y recibir simultáneamente con tres estaciones base. Esto permite la anulación de los efectos de *ping-pong* y además mejora el funcionamiento contra las multitrayectorias o radio condiciones adversas.

CDMA fue desarrollado originalmente bajo el nombre comercial cdmaOne basado en TIA [IS-95], un estándar para la compatibilidad estación móvil-estación base para sistemas de espectro expandido de banda ancha. Este es un esquema CDMA de secuencia directa en el cual los usuarios son diferenciados por códigos únicos conocidos por el transmisor y el receptor. La versión IS-95A del estándar permite servicios de datos por conmutación de circuitos de hasta 14.4 Kbps. La siguiente generación de IS-95, llamada IS-95B, requiere cambios de software y hardware en los elementos del sistema CDMA y en las estaciones móviles pero soportará paquetes de datos con una tasa de transferencia que va de 64 a 115 Kbps. Esto se lleva a cabo usando el canal de avance y técnicas de agregación de código y otras modificaciones a IS-95A. En IS-95B, pueden ser agregados hasta 8 canales CDMA de tráfico para uso de un solo suscriptor.

3.4 Sistemas Celulares 3G

En esta sección proporcionamos una inspección de las interfaces de radio y propiedades de los principales sistemas 3G.

3.4.1 CDMA2000

CDMA2000, a menudo llamado CDMA3G, es la siguiente generación de los sistemas celulares originales CDMA IS-95 e IS-95B. Este ha sido desplegado en América, así como en algunas regiones de Asia y el Este de Europa. La Tecnología de Radio Transmisión (RTT) de CDMA2000 incluye mejoramientos que efectivamente doblan la eficiencia espectral de CDMA IS-95, así como el número de llamadas de voz simultáneas que el sistema puede manejar. CDMA2000 utiliza tasas de transmisión que son múltiplos de 1.2288 Mbps, lo que significa que los sistemas celulares basados en CDMA2000 son compatibles con los sistemas CDMA IS-95 y las terminales móviles de CDMA2000 pueden ser compatibles con los sistemas legados. CDMA2000 puede soportar múltiples anchos de banda de la portadora y planes de banda de frecuencia incluyendo PCS e IMT2000. La capacidad de desplegar RTT de CDMA2000 para 1.25 MHZ es especialmente importante en Norte América, donde se permite a los portadores CDMA reusar su espectro existente para ofrecer el servicio CDMA2000 con tan solo actualizar el equipo sin la necesidad de comprar nuevo espectro. Esta versión de CDMA2000 ha sido nombrada CDMA2000 fase uno, o CDMA2000-1x RTT. La otra versión de la tecnología CDMA2000, llamada CDMA2000-3x, representa la evolución lógica de CDMA2000-1x, emplea 5 MHz de ancho de banda.

CDMA2000-1x proporcionará a los suscriptores la habilidad para transferir y recibir paquetes a tasas de transferencia netas de 153.6 kbps o una tasa de transferencia efectiva de hasta 144 Kbps. CDMA2000-1x, al igual que su antecesor soporta voz y datos. La capa física de CDMA2000-1x incorpora un número de mejoras que proporcionan tasas de transferencia más altas y mejor eficiencia espectral que los sistemas CDMA de la segunda generación. Una capacidad en el modo explosión (*burst*) es definida para permitir mejor administración de la interferencia y capacidad de utilización. Un paquete de datos móvil activo de alta velocidad siempre tiene un canal de tráfico usando un código fundamental. Este canal es llamado el canal fundamental (FCH). Una llamada activa de HSPD (*High Speed Packet Data*) con la necesidad de un ancho de banda mayor ya sea en la dirección hacia delante o de reversa le podría ser asignado un canal adicional para la duración de una ráfaga de datos, la cual es del orden de segundos. El canal adicional durante este estado es llamado el canal suplementario (SCH), el cual permite un amplio rango de tasas de datos; tasas netas de 9.6 a 307.2 Kbps son soportadas sobre cada canal suplementario. Aún cuando el estándar CDMA-1x soporta tasas de transferencia netas sobre el canal SCH de hasta 307.2 Kbps, se ha estimado que la máxima tasa de transferencia efectiva que puede ser soportada

sobre una amplia área de cobertura –con una portadora de 1.25 MHz- será alrededor de 150 Kbps. Usualmente un canal SCH es asignado para servicio de datos. Un canal SCH con una tasa de datos de 19.2 Kbps o mayor es equivalente a múltiples llamadas de voz tomando en consideración la capacidad de la interfaz de aire.

3.4.1.1 CDMA2000-1xEV

Para satisfacer los requerimientos de alta velocidad del mercado inalámbrico de datos, la comunidad de estándares de CDMA ha desarrollado una versión optimizada de CDMA2000 llamada CDMA2000-1xEv-DO (donde DO significa *Data Only*). CDMA2000-1xEV-DO soporta para el enlace descendente tasas de transferencia de datos de hasta 2457.6 Kbps y para el enlace ascendente soporta tasas de hasta 153.6 Kbps. Note que mientras los sistemas CDMA2000 han sido diseñados para proporcionar la misma capacidad tanto al enlace ascendente como al enlace descendente, la versión 1xEV-DO de CDMA2000 ha sido diseñada para adaptarse a las necesidades asimétricas de alta velocidad para los datos de usuario, los cuales requieren más ancho de banda en la dirección descendente para bajar información de Internet y recibir el flujo de tráfico. Los paquetes de datos son solo un tipo de tráfico soportado por esta tecnología.

1xEV-DO proporcionará a los usuarios conectividad "*always-on*" para paquetes de datos, a diferencia de los ofrecimientos actuales de DSL y cable módem. Una red 1xEV-DO puede ser implementada como complementaria a una red CDMA2000-1x regular, ya que la mayoría de los componentes de hardware así como el espectro pueden ser compartidos entre las dos redes. Cuando se planea un sistema combinado, se debe asignar una frecuencia portadora dedicada separada de 1.25 MHz para el tráfico 1xEV. Mientras dos sistemas puedan coexistir en una red de portadoras, requerirán teléfonos diferentes o dos funcionalidades diferentes soportadas en un solo teléfono.

3.4.1.2 CDMA2000-3x

CDMA2000-3x (o CDMA 3G-3xRTT) utiliza 5 MHz de ancho de banda, y por consiguiente está clasificado junto con UMTS en la familia W-CDMA (*Wideband CDMA*) de las tecnologías de radio transmisión. Entrega tasas de datos de hasta 144 Kbps para aplicaciones móviles y tanto como 2 Mbps para aplicaciones estacionarias. CDMA2000-3x introducirá las más altas tasas de transferencia para transmisión de datos, QoS más sofisticados y capacidades multimedia avanzadas. Dependerá de la capa de enlace de datos basada en ATM entre las estaciones base y las Centrales Móviles de Conmutación para acomodar las velocidades más altas y un modelo de llamadas avanzado.

La tabla 3.2 muestra una comparación entre las tecnologías CDMA.

Tabla 3.2: Comparación de las tecnologías CDMA2000

	LLAMADAS POR RADIO CANAL	ANCHO DE BANDA DEL RADIO CANAL	TASA DE DATOS PICO (TEÓRICA)
CdmaOne IS-95 (A/B)	13-28	1.25 MHz	9.6/14.4/19.2 Kbps
CDMA2000-1x 1XEV-DO	140-200	1.25 MHz	144–153.6 Kbps 144 kbps–2.4 Mbps
CDMA2000-3X	180–300	5 MHz	385 Kbps–2.4 Mbps
W-CDMA	140–200	5 MHz	144 Kbps-peatón 384 Kbps-vehicular

Tabla 3.2: Comparación de las tecnologías CDMA2000

	LLAMADAS POR RADIO CANAL	ANCHO DE BANDA DEL RADIO CANAL	TASA DE DATOS PICO (TEÓRICA)
			2.4 Mbps-estacionario

3.4.2 Sistema Universal para Telecomunicaciones Móviles (UMTS)

UMTS es un sistema celular inalámbrico de tercera generación que cumple con todas las definiciones de un sistema 3G. UMTS fue diseñado para ser una evolución del sistema GSM/GPRS. Como resultado, UMTS hereda la mayoría de la arquitectura de la red central de GSM/GPRS, y está garantizado el servicio de *roaming* entre UMTS y GSM, y la transmisión intersistemas con teléfonos que trabajan en modo dual capaces de soportar UMTS y GSM. El sistema UMTS está definido por el proyecto 3GPPP en tres liberaciones: R99, R4, y R5. El sistema UMTS comparte la red central con el sistema GSM, y de R99 las especificaciones GSM y UMTS son las mismas. R99, sin embargo, introduce una nueva interfaz de radio estándar basada en la tecnología W-CDMA, así como también un nuevo método de interconexión de la red central a la red de radio acceso (RAN).

3.4.2.1 Estandarización UMTS

UMTS ha sido especificado por la Unión Internacional de Telecomunicaciones (ITU) en el contexto de la iniciativa del Sistema Internacional de Telecomunicaciones Móviles (IMT-2000). El proyecto 3GPP fue formado en 1998 para coordinar un esfuerzo global de una gran variedad de cuerpos regionales de estandarización para definir las especificaciones para el sistema UMTS. Entre los cuerpos involucrados en la especificación se incluyen a la ARIB (*Association of Radio Industries and Businesses*) de Japón, el TTC (*Telecommunication Technology Committee*) de Asia, T1P1 de la TIA (Norte América), y el ETSI (*European Telecommunications Standards Institute*) de Europa. El ETSI además encargó al 3GPP las especificaciones para el mantenimiento y evolución de GSM. Esto fue el resultado lógico derivado del uso de la red central de GSM como la base para el desarrollo de las especificaciones de la red central de UMTS y manteniendo la interoperabilidad entre los sistemas GSM y UMTS. Además los operadores de red y los fabricantes de equipo de red se juntaron para formar el grupo OHG (*Operators Harmonization Group*), el cual fomenta la interoperabilidad mutua y el *roaming* entre los estándares CDMA2000 y W-CDMA.

UMTS soporta el concepto de VHE (*Virtual Home Environment*), el cual permite a los suscriptores el acceso a los mismos servicios desde cualquier lugar en el mundo donde es soportado UMTS. Los suscriptores que usan los sistemas con VHE, son capaces de utilizar los mismos servicios como si estuviesen en la red local mientras andan en cualquier otra red pública móvil (PLMN, *Public Land Mobile Network*). Los servicios dependen de las capacidades de las redes visitadas y de los acuerdos de servicio entre varios operadores. Al igual que su predecesor, el sistema UMTS ofrece servicios basados en circuitos y paquetes. Las secciones de las redes centrales que soportan estos servicios son llamadas dominio UMTS CS y dominio UMTS PS respectivamente. Finalmente, UMTS ofrece una red central que es independiente de la red RAN. Esto se realiza ocultando los aspectos de movilidad a nivel celular que son utilizados para afectar la central en GSM dentro de la RAN. En UMTS, por ejemplo, la central no está enterada de la localización del usuario.

3.4.2.2 Interfaz de Radio de UMTS

La red UMTS está dividida lógicamente en una red de radio acceso terrestre UMTS (UTRAN, *UMTS Terrestrial Radio Access Network*) y una red central (CN), conectadas vía una interfaz abierta (la interfaz Iu) como se muestra en la figura 3.5. Cuando se utiliza para comunicarse con el

dominio CS, la interfaz Iu es llamada Iu-CS, y cuando es utilizada para comunicarse con el dominio PS, la interfaz es llamada Iu-PS.

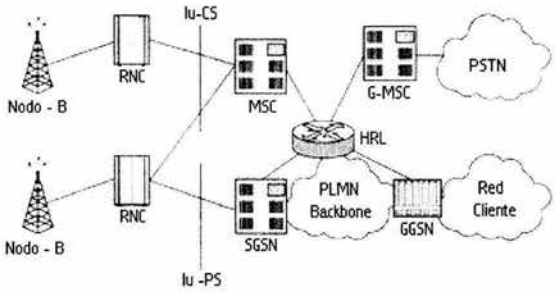


Figura 3.5 Arquitectura de UMTS de 3GPP

Desde una perspectiva de servicios de datos, GPRS y el dominio PS de UMTS son similares – ambos permiten a los proveedores de servicio inalámbrico ofrecer servicio bidireccional de paquetes de datos. GSM y el dominio CS de UMTS permiten soportar circuitos de datos y servicios de voz. Los sistemas UMTS permiten las tasas de transferencia más altas y el soporte de servicios multimedia sobre los portadores CS, que GSM no permitía.

En el nivel alto, UTRAN consiste del radio controlador de la red (RNC) y del nodo B. RNC es funcionalmente similar al controlador de la estación base (BSC) en las redes GSM, aunque con mayor inteligencia y un número de nuevas responsabilidades debido al principio fundamental de independencia de la red central de la RAN, lo cual requiere que la RAN cubra muchos aspectos de la movilidad de los usuarios que originalmente manejaba la red central. El RNC gestiona las funciones de los recursos de radio, tales como establecimiento y liberación de la llamada, control de potencia, y *handover* suave. Un RNC además manda la relocalización de una estación móvil a otro RNC, cuando es óptimo para la estación móvil que sea servido por un nuevo RNC. Dos interfaces de radio están especificadas para UMTS: una está basada en una operación de duplexaje por división de frecuencia (FDD) que usa la tecnología de radio FDD/W-CDMA, y la otra está basada en una operación de duplexaje por división de tiempo (TDD) que usa la tecnología de radio TDD/W-CDMA.

Las licencias de UMTS asignan ciertas bandas de frecuencia a los operadores. Un tipo de asignación es conocida como *espectro emparejado*. El espectro emparejado utiliza dos bandas de frecuencia separadas, una para el tráfico ascendente y otra para el tráfico descendente. Este método de asignación es usado para la operación FDD. El otro tipo de asignación, es usado para TDD, es llamado *espectro disparejo*. Aquí las estaciones móviles envían y reciben información en la misma banda de frecuencia. Debido a que TDD requiere un control muy fino del tiempo para enviar y recibir paquetes, éste es más apropiado para aplicaciones en distancias cortas, como en el interior de las picocélulas instaladas en lugares de alta concentración de usuarios como aeropuertos, oficinas, lugares de negocios.

UMTS soporta velocidades de transmisión a través de la interfaz de aire más altas que GSM. UMTS define tres categorías de movilidad con su correspondiente tasa de bits:

- *Movilidad alta*, como en las comunicaciones desde un automóvil, tasas de transmisión de hasta 144 Kbps.
- *Movilida baja*, como en la comunicación mientras una persona está caminando por la calle, con tasas de transmisión de hasta 384 Kbps.

- *Movilidad interior*, en las cuales no hay realmente una verdadera movilidad y constituyen las comunicaciones estacionarias, con tasas de transmisión de hasta 2 Mbps.

Las tasas de transferencia actuales dependen de la capacidad de la interfaz de aire y de las condiciones ambientales en un momento dado.

3.4.3 EDGE (*Enchased Data Rates for Global Evolution*)

EDGE fue concebida en 1997 sólo como una evolución de GSM, pero más tarde fue adoptada por el sistema TDMA Norte Americano. La adaptación de EDGE como una posible evolución de la tecnología de la interfaz de aire para TDMA Norte Americano tomó lugar en 1998 cuando el principal foro de la industria para la tecnología TDMA, el UWCC (*Universal Wireless Communications Consortium*), adoptó ésta como la base para el estándar 136-HS para proporcionar servicios a 384 Kbps.

EDGE reusa el espectro de GSM y TDMA y la estructura de ranuras de tiempo, y está basado en modernos y altamente eficientes esquemas de modulación. La tecnología de radio de EDGE transmite sobre un control fundamental de calidad del enlace, un concepto que permite la adaptación de la protección de los datos a la calidad del canal, entonces alcanza la tasa de bits óptima para una variedad de radio ambientes. Los esquemas de modulación de EDGE permiten tasas de bits totales desde 22.8 hasta 69.2 Kbps por ranura de tiempo, respectivamente. Un máximo de 8 canales combinados en el sistema EDGE con una tasa de transferencia efectiva estimada de 48 Kbps por canal producirá tanto como 384 Kbps (teóricamente hasta 473.6 Kbps), lo cual está en línea con los requerimientos de 3G para paquetes de datos inalámbricos. Básicamente, EDGE solo introduce nuevas técnicas de modulación, nueva codificación de canal, ajustes a los protocolos de enlace, y otros realces a los sistemas GSM y TDMA sin afectar sus redes centrales.

3.4.3.1 Clasificación de EDGE

Como se muestra en la figura 3.6, existen diferentes clases de sistemas EDGE.

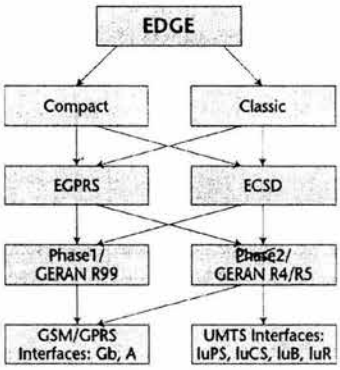


Figura 3.6 Taxonomía de EDGE

Primero están las versiones *EDGE Compact* y *EDGE Classic*. *EDGE Compact* diseñado para TDMA IS-136 utiliza 200 kHz para el canal de control. Utiliza estaciones base sincronizadas para mantener un despliegue mínimo del espectro de 1 MHz dentro de un patrón de reuso de la primer frecuencia. *EDGE Classic* emplea la tradicional estructura GSM de 200 kHz para el canal de control con un patrón de reuso de frecuencia de 4/12 en la primer frecuencia.

Segundo, existe una distinción entre los sistemas EDGE desplegados para conmutación por paquetes llamado *Enhanced GPRS* (EGPRS) y conmutación por circuito llamado *Enhanced CSD* o *Enhanced HSCSD* (ECSD o E-HSCSD).

Finalmente, existen dos fases de EDGE. La Fase 1, también referida como GERAN R99, y la Fase 2, conocida con el nombre de GERAN R4/R5. La fase 1 de EDGE define la nueva interfaz de aire con capacidad de paquetes de datos de hasta 384 Kbps y requiere de células más pequeñas comparadas con las de GSM. Define además servicios de conmutación de paquetes y conmutación de circuitos sencillos y multiranuras. La fase 2 de EDGE define la alineación con UMTS bajo el concepto conocido como GERAN (*GSM/EDGE Radio Access Network*). De hecho, la fase 2 de EDGE, o GERAN R4/R5, extenderá todos los servicios sobre la red central de UMTS.

Los objetivos eventuales de la especificación GERAN incluyen el proporcionar clases de servicios de datos similares a UMTS y la capacidad para la interfaz y *handover* con UMTS CN sobre la interfaz Iu. Mientras que GERAN R4 introduce sólo mejoras menores al actual estándar EDGE, la mayoría sobre la interfaz de aire, y retiene la interfaz Gb para conexiones a GPRS, mayores mejoras a los paquetes son esperados con la llegada de GERAN R5, que introducirá el marco UMTS QoS, soporte para la interfaz Iu y la arquitectura del protocolo.

3.4.3.2 El Futuro de EDGE

Diseñado como un mejoramiento a GSM y a TDMA, EDGE coexistirá eficientemente con las actuales infraestructuras celulares basadas en el multiplexaje por división de tiempo y potencialmente proporcionará una trayectoria alternativa de migración hacia UMTS. EDGE es atractivo para aquellos operadores inalámbricos que fueron incapaces de obtener licencias 3G – por ejemplo, en algunos países de Europa Occidental. Estos operadores esperan con la combinación de EDGE y GSM proporcionar servicios 3G y *roaming* global, a la vez que no requiere la adquisición de nuevo espectro para el uso de un sistema 3G basada en W-CDMA. La migración hacia EDGE en los mercados Norte Americanos es aún más probable, porque el espectro para UMTS no está disponible en esta parte del mundo.

3.5 WLAN (*Wireless LAN*)

WLAN se ha convertido en la tecnología de acceso inalámbrico de más rápido crecimiento. WLAN –combinado con sistemas 2.5G y 3G- puede potencialmente llevar las comunicaciones inalámbricas de datos a un nuevo nivel que no sería posible con un sistema 3G solo. Por ejemplo, un número de hoteles en muchas partes del mundo, como el oeste de Europa y Norte América, están ofreciendo a sus clientes la capacidad de usar servicios WLAN. Estos negocios se asocian con un operador celular o un proveedor ISP, los cuales les administran los servicios.

3.5.1 Tecnologías WLAN

WLAN es una versión de los estándares LAN alámbricos (802.3 o Ethernet son dos ejemplos muy populares) definida por el IEEE con el nombre 802.11b. WLAN depende de la tecnología de RF y transmite datos sobre el aire mucho mejor que una conexión alámbrica requerida por las otras tecnologías LAN.

Una conexión WLAN exitosa requiere un dispositivo cliente, una tarjeta de red inalámbrica (NIC) instalada en el dispositivo móvil del usuario (por ejemplo una *laptop* o un PDA), y un punto de acceso (AP), el dispositivo que termina la interfaz de aire de RF y ejecuta funciones de ruteo. Una topología WLAN típica es mostrada en la figura 3.7.

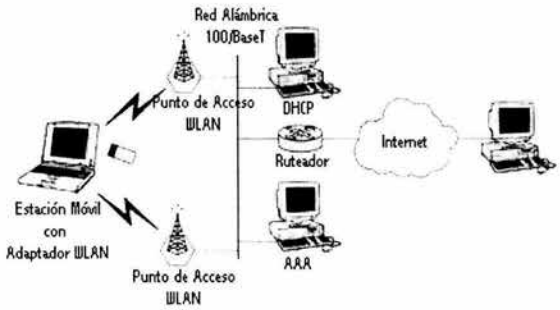


Figura 3.7 Topología típica de una WLAN

Las WLANs pueden alcanzar distancias de hasta 500 metros al aire libre sin la presencia de obstáculos. WLAN está basada en el uso de la banda sin licencia ISM (*Industrial, Scientific, and Medical*), de 2.4 a 2.5 MHz, la cual ofrece claras ventajas económicas para el despliegue comercial de WLAN. La frecuencia de 2.4 MHz es usada para teléfonos inalámbricos y dispositivos *Bluetooth*.

Las redes definidas por los estándares 802.11 son capaces de operar usando dos tipos de transmisión: Espectro Expandido por Salto de Frecuencia (FHSS) y Espectro Expandido por Secuencia Directa (DSSS). Las tecnologías FHSS y DSSS de la interfaz de radio son mutuamente exclusivas. FHSS es la más simple de implementar pero está limitada a 2 Mbps por regulaciones de la FCC (en los Estados Unidos, donde fue desarrollada). Para la banda sin licencia, DSSS es más compleja pero ofrece más alta tolerancia a la interferencia y las tasas de transmisión llegan a 11 Mbps, las cuales son las más altas posibles para el estándar 802.11b. Por ello la versión DSSS es la más popular, y rápidamente se está convirtiendo en el estándar de facto.

Una de las mayores limitaciones para un despliegue más extenso de las WLANs para uso público y corporativo ha sido la falta de seguridad o una forma estándar para lograr acceso seguro y confidencialidad de los datos. Típicamente, los despliegues de WLANs públicas están basados en la autenticación de los usuarios en un portal, posiblemente después de que ocurre una redirección TCP cuando el usuario intenta acceder a cualquier página Web. Después de la autenticación, el punto de conexión del usuario hacia Internet permitirá al usuario acceder hasta que nueva autenticación sea solicitada o una cuenta necesite ser *encabezada*.

CAPÍTULO 4

SERVICIOS DE DATOS EN SISTEMAS INALÁMBRICOS

4.1 Circuitos vs Paquetes

Con el servicio inalámbrico de datos por conmutación de circuitos, son asignados circuitos dedicados a los suscriptores no importando si los usan o no. En teoría, esto proporciona un ancho de banda más efectivo ya que se dedica un canal completo a cada usuario. El servicio de datos es proporcionado vía un modelo de *dial-up* inalámbrico similar al acceso remoto de *dial-up* alámbrico. El usuario marca un número telefónico asociado con el servidor de acceso a la red (NAS) usado para un servicio inalámbrico específico de datos. Una vez que la conexión física -esto es, el circuito- está establecido entre la estación móvil y el servidor, es utilizado el protocolo PPP para proporcionar servicio de la capa de enlace de extremo-a-extremo. La terminación de la sesión PPP de usuario puede realizarse usando técnicas simples de *dial-up* basadas en apagar el banco de módems o los servidores de acceso remoto (RAS), que abarcan funcionalidades de interconexión IWF (*Interworking Function*). La función IWF normalmente es requerida para terminar los protocolos de acceso inalámbrico (RLP, *Radio Link Protocol*) e interactuar con la Red de Teléfono Pública (PSTN) cuando es necesario. En algunos casos la IWF puede transmitir PPP a una red privada que usa L2TP.

En contraste, las tecnologías inalámbricas de datos por conmutación de paquetes están basadas en una red de acceso inalámbrico que soporta multiplexaje estadístico de las sesiones de usuario sobre la interfaz de radio. Los recursos de la red de paquetes de datos son utilizados sólo durante la transferencia de datos e inhabilitados durante los periodos ociosos, resultando en un sistema más eficiente en el cual cualquier fuente de tráfico puede usar los recursos que no son utilizados por otros. El multiplexaje estadístico es una propiedad importante de todos los sistemas de paquetes de datos. El multiplexaje estadístico hace a los sistemas de paquetes de datos más eficientes que los sistemas basados en circuitos, ya que garantiza a cada usuario una separación, un canal dedicado, que no se utiliza completamente con patrones de ráfagas de transmisiones de datos. Sin embargo, esto significa que los usuarios de redes de medios compartidos deben contender por el ancho de banda disponible, algunas veces resultando en congestiones, retardos, y baja efectividad para el usuario.

El acceso por contención a los recursos compartidos es un problema típico no solo para ambientes celulares sino también para las WLANs. En los sistemas celulares que soportan acceso en modo de paquetes, para hacer eficiente el uso de los recursos, los portadores de radio acceso son asignados solo temporalmente a un usuario específico. Después de un periodo de inactividad, la estación móvil entra en un modo de operación ocioso (por ejemplo, en GPRS) o inactivo (CDMA2000). Este modelo permite a la estación móvil estar constantemente alcanzable para enviarle información de señalización y datos a su dirección de la capa de red utilizando procedimientos de actualización de localización y *paging*, mientras los recursos no dedicados están activos para permitirle a la estación móvil enviar y recibir datos. Cuando necesita recibir datos, la estación móvil es llamada, "despierta", y emite una petición para instalar el radio portador que le permita la recepción de los datos. La estación móvil emite la misma petición cuando necesita enviar datos o cuando no ha podido instalar el radio portador.

El soporte de la movilidad de los paquetes de datos de usuario está basado en varios mecanismos de *tunneling* como IP Móvil (adoptado por CDMA2000) y GTP (adoptado por GSM y UMTS). Este modelo común de *tunneling* de paquetes de datos es mostrado en la figura 4.1. Los túneles descritos en la figura por líneas de cuadros (para túneles discontinuos) y por líneas sólidas (para túneles activos) son establecidos dinámicamente entre los puntos temporales de enlace de la estación móvil hacia la red inalámbrica y un túnel de "punto de anclaje" o red local que también actúa como un *gateway* hacia la red de datos móvil desde la cual el usuario está recibiendo

servicio de acceso. Como las estaciones móviles cambian dinámicamente su localización dentro de la red, los túneles son establecidos dinámicamente entre la estación móvil y la red de acceso inalámbrico visitada.

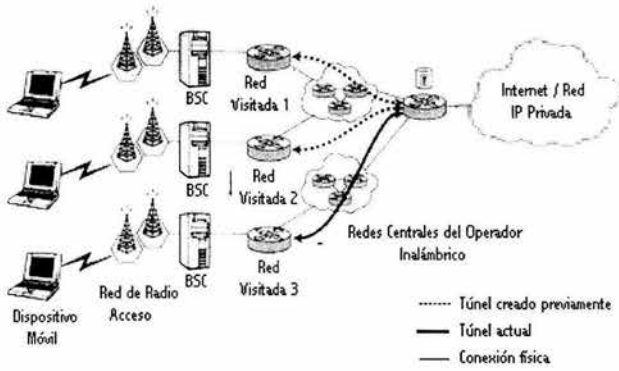


Figura 4.1 Mecanismo de túneles para paquetes de datos inalámbricos.

Todas las características familiares del acceso alámbrico de *dial-up* son presentadas en los circuitos de datos inalámbricos: secuencia *login*-contraseña, capacidad de acceso a la red corporativa simplemente marcando números telefónicos específicos, procedimientos de configuración de identidad en los dispositivos cliente de los usuarios como las *laptops*.

Las tecnologías inalámbricas de paquetes de datos no requieren marcar un número para alcanzar un servidor NAS específico en una red corporativa o una red ISP. Con esto, los usuarios disfrutan la conectividad *permanente* o la conectividad *bajo demanda* a Internet o a su red corporativa. Sin embargo, en la mayoría de los casos, se requiere predefinir las relaciones entre la corporación y el portador inalámbrico.

4.2 Servicios de Datos en los Sistemas 1G, 2G y 3G

Esta sección nos da una descripción detallada de cómo los servicios de datos inalámbricos son proporcionados en los ambientes celulares más populares.

4.2.1 Circuitos de Datos en los Sistemas 1G

Las tecnologías inalámbricas 1G como TACS, NMT y AMPS están basadas en la multiplexación por división de frecuencia. Una señal de voz es transmitida directamente a una parte del espectro que está dedicado al usuario. La misma parte del espectro puede ser utilizada para modular las señales de datos usando un módem inalámbrico. Los protocolos de corrección de errores usados por los módems inalámbricos tienden a ser más robustos por la necesidad de tratar con un ambiente físico más desafiante con interferencias y relaciones señal-ruido más altas.

La tasa de transferencia para un módem AMPS bajo buenas condiciones es tan alta como 14.4 Kbps y bajo condiciones malas es tan baja como 4.8 Kbps. Puede haber una tardanza de 20 segundos o más para establecer una conexión. Como resultado, la experiencia para el usuario no es muy satisfactoria, y combinado con la mala relación funcionamiento-precio, ha hecho a los servicios CSD sobre los sistemas celulares de primera generación una fuente insignificante de ingresos para los portadores. Esto explica parcialmente el estancamiento de los servicios de datos durante los 90´s.

4.2.2 Conmutación de Circuitos de Datos en los Sistemas 2G y 3G

Los sistemas de segunda y tercera generación están basados en la transmisión digital de la voz sobre recursos de radio dedicados. Estos sistemas están basados en el uso de canales digitales, y por lo tanto no son necesarias la modulación y la demodulación para transmitir datos desde las estaciones móviles hacia la red central. Estos sistemas han sido aumentados con capacidades para servicios de conmutación de circuitos de datos, y como resultado, pueden ofrecer un servicio de datos transparente utilizando mecanismos ARQ (*Automatic Repeat Request*), los cuales involucran la retransmisión de las partes perdidas de los datos transmitidos sobre el canal digital. Además, estos canales necesitan estar terminados en algún lugar de la red inalámbrica para proporcionar acceso directo a la red de datos o para interactuar con las líneas ISDN o PSTN para proporcionar conectividad extremo-a-extremo hacia una función IWF en la red central del portador inalámbrico.

4.2.2.1 Conmutación de Circuitos de Datos en CDMA y TDMA

Como se muestra en la figura 4.2, este servicio requiere un circuito fijo –en este caso, una conexión *dial-up* con un módem CDMA- para ser establecido entre el móvil y el destino de la llamada. El sistema debe transportar los datos en una forma digital hacia una función IWF, la cual puede generar los tonos del módem para la comunicación directa a la red PSTN.

Para este efecto, una llamada de datos se origina en la IWF dentro de la red del proveedor de servicio, la cual marca al número destino de la estación móvil. La IWF convierte los datos (CDMA o TDMA) codificados al formato de un módem analógico normal y pasa la llamada sobre la red PSTN. Técnicas adicionales de compresión a menudo permiten a los usuarios alcanzar tasas de datos de hasta 19.2 Kbps. La secuencia de llamada para una conexión CDMA de circuitos de datos incluye los siguientes pasos, los cuales son ilustrados en la figura 4.2:

1. La conexión del circuito es establecida por la estación móvil.
2. La llamada de datos es dirigida por el controlador de la estación móvil hacia la IWF.
3. La llamada saliente es puesta por el módem IWF sobre el bus IWF de paquetes interno hacia un *switch* TDM.
4. El *switch* TDM conecta la llamada a la red PSTN.
5. La llamada es terminada por el módem en el lugar de destino de la llamada.

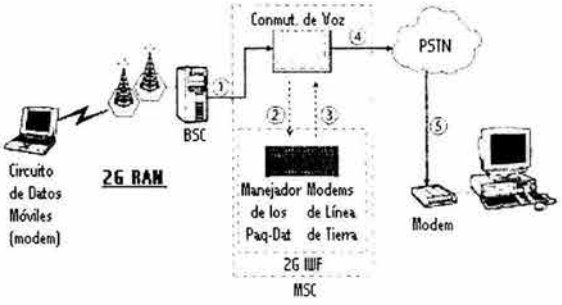


Figura 4.2 Arquitectura de la conmutación de circuitos en CDMA.

Uno de los engrandecimientos comerciales más popular de cdmaOne es QNC (*Quick Net Connect*). Esta tecnología, originalmente diseñada por *3COM, Qualcomm, y Unwired Planet*, permite a los portadores proporcionar a los usuarios acceso directo a Internet y a redes IP privadas, desviándose de la red PSTN y evitando la necesidad de usar procedimientos *dial-out* del módem. En QNC la IWF encamina los datos desde la red CDMA inalámbrica hacia Internet o

Intranet usando PPTP o L2TP. Esto evita el uso de los recursos de la red PSTN, tiempo de instalación, y tiempo de preparación del módem, resultando en una conexión extremo-a-extremo más rápida y más confiable.

4.2.2.2 Conmutación de Circuitos de Datos en GSM y UMTS

GSM fue definido originalmente para ofrecer servicios digitales de voz. Aunque inicialmente el sistema GSM no abarcó acceso de datos, como el acceso a redes de computadoras se convirtió en un nuevo servicio de gran importancia para los clientes, y para los operadores representó una nueva fuente de ingresos, fueron definidas nuevas capacidades del sistema. En este tiempo también fueron definidos los servicios CSD orientados a conexión así como los servicios de datos sin conexión tales como SMS y USSD (*Unstructured Supplementary Services Data* –los cuales son algunas veces utilizados para interactuar con *gateways* WAP, *Wireless Application Protocol*).

En GSM, la llamada de datos la mayoría de las veces es iniciada por el suscriptor GSM, quien establece una conexión *dial-up* llamando a un número de acceso de datos deseado proporcionado por el proveedor ISP o una red privada. La llamada de datos originada por la estación móvil es terminada en una IWF, la cual convierte los datos de entrada a un formato de módem analógico regular y conduce un procedimiento *dial-up* para establecer un enlace sobre la red PSTN hacia el punto final del destino de la llamada, esto es, un servidor de acceso remoto (RAS). PPP normalmente proporciona el servicio extremo-a-extremo de la capa de enlace entre la estación móvil y el RAS.

Los datos recibidos por la función IWF se convierten a tonos FSK analógicos característicos de los módems analógicos. El resultado de la llamada de datos de extremo-a-extremo puede ser visto como dos llamadas independientes: la trayectoria de los datos móviles y la trayectoria de la red PSTN. La trayectoria de los datos móviles se refiere a la conexión entre el móvil y la IWF. La trayectoria de la red PSTN se refiere a la conexión entre la IWF y el RAS en el destino de la llamada.

Una alternativa a esta arquitectura es la característica de Acceso Directo a Internet, que es similar a QNC de CDMA. Con esta característica el enlace PPP que se origina en el móvil es terminado en la IWF y entonces los paquetes IP son encaminados directamente hacia Internet. Por el otro lado, el usuario móvil está limitado al acceso a Internet y a otros servicios de datos proporcionados sólo por el portador inalámbrico. Este inconveniente, sin embargo, puede ser evitado transmitiendo las tramas PPP recibidas por la IWF sobre L2TP, permitiendo entonces al portador inalámbrico proporcionar servicio de acceso a redes remotas, utilizando L2TP basado en VPN.

Las tasas de transferencia que se ofrecen a los usuarios por conmutación de circuitos en GSM son de 9.6 Kbps o 14.4 Kbps. Normalmente depende de las condiciones del canal de radio y del protocolo de compresión negociado en la instalación de la sesión PPP.

Con respecto a CSD no existe diferencia en la arquitectura entre UMTS y GSM, solo que UMTS proporciona servicios CSD con tasas de transferencia más altas. GSM definió HSCSD (*High-Speed Circuit-Switched Data*). HSCSD permite el uso de múltiples canales de tráfico *full-rate* (TCH/F es un canal de 16 Kbps) para lograr tasas de datos mayores. La estación móvil HSCSD puede solicitar portadores asimétricos.

Una estación móvil puede solicitar transferencia transparente de los datos sobre los circuitos de la red inalámbrica. En este caso las redes GSM/UMTS proporcionan al usuario un canal que entrega los bits desde la estación móvil hacia la red externa, y viceversa. Este tipo de servicio normalmente no es apropiado para la transferencia de datos de aplicaciones basadas en TCP/IP debido a que la relativamente alta tasa de error afectaría la comunicación hasta el punto de que sería muy lenta y en ocasiones, puede no haber comunicación. En lugar de esto, este servicio puede ser utilizado para la entrega sin restricciones de cadenas de bits.

4.2.2.3 Capacidades del Servicio CSD de GSM/UMTS

GSM y el dominio UMTS CS ofrecen una serie de servicios portadores básicos:

UDI. Este servicio proporciona transferencia de información digital sin restricciones.

3.1 kHZ. Servicio usado para elegir una función de interacción de audio de 3.1 kHZ en el controlador de la estación móvil (MSC), esta categoría de servicio es utilizada cuando interactúa con el servicio de audio de 3.1 kHz de ISDN o PSTN e incluye la capacidad para seleccionar un módem en la función de interacción. "*External to the PLMN*" indica que el servicio de audio de 3.1 kHz sólo es usado fuera de PLMN, en la ISDN/PSTN. La conexión dentro de PLMN, el punto de acceso del usuario hacia la IWF, es una conexión digital sin restricciones.

PAD. Este servicio proporciona acceso a un PAD (para PSPDN basados en X.25).

Paquete. Este servicio proporciona interacción directa hacia una red de paquetes o una red ISDN (normalmente X.25, X.31).

Voz y datos alternados. Este servicio hace posible la alternación entre voz y datos durante la duración de la llamada.

Voz seguida de datos. Con esta característica, es posible comenzar una llamada en el modo de voz y luego conmutar al modo de datos, pero no viceversa.

Los servicios portadores 3.1 kHz y UDI están muy relacionados. De hecho, el término 3.1 kHz no aplica a PLMN, más bien representa los recursos PSTN usados para proporcionar conectividad de extremo-a-extremo (el espectro requerido para transmitir una conversación de voz) que un módem en una IWF puede usar para conectarse a la red de datos accedida por los suscriptores PLMN. Típicamente UDI y 3.1 kHz usan el mismo portador físico desde la estación móvil hasta la IWF, y diferentes portadores después de la IWF hacia la red externa (hacia la PLMN). UDI es normalmente utilizado para soportar conectividad del tipo ISDN, mientras que 3.1 kHz es utilizado para conectividad analógica hacia redes externas. Típicamente, las adaptaciones de terminales V.110 y V.120 son usadas para conectividad ISDN. Utilizando UDI con V.110 o V.120 es posible también proporcionar acceso digital directo a redes de datos, logrando instalación de la conexión más rápida.

Los servicios UDI y 3.1 kHz están caracterizados por un parámetro QoS muy importante: los tipos transparente o no transparente del servicio portador. Un servicio es transparente si la red se comporta como un tubo de bits, totalmente inconsciente de qué protocolo de usuario es transmitido. En el modo no transparente la estación base y la IWF son el punto de terminación del protocolo de radio enlace (RLP). Este protocolo proporciona una serie de servicios al protocolo de usuario. El protocolo de usuario (PPP para servicios comunes de acceso a red) es encapsulado en tramas RLP. Estas tramas están numeradas y son más pequeñas que el protocolo de usuario, así que el tamaño de la unidad de retransmisión es normalmente entre uno o dos órdenes de magnitud más pequeña que el paquete original del protocolo de usuario.

Esto permite la retransmisión de unos pocos bytes sobre el aire cuando una parte de los datos de del usuario fueron corrompidos debido a las malas condiciones de radio. Las tramas numeradas pueden retransmitirse –vía ARQ- y también la secuencia de números puede ser utilizada para implementar mecanismos de control de flujo, así que cuando hay exceso de tráfico entrante que la interfaz de radio no puede manejar, el RLP envía señales de contrapresión a la funcionalidad de retransmisión (en el lado terminal y en la IWF), de modo que el flujo de tráfico de usuario pueda pasar apropiadamente. El RLP mejora la calidad del enlace desde un punto de vista de la tasa de error (BER); esto es, proporciona algún grado de independencia del BER de las radio condiciones de desvanecimiento.

4.3 Paquetes de Datos en CDMA2000

En esta sección se describe la arquitectura central para paquetes de datos asociada con la interfaz de radio CDMA2000. Esta arquitectura es descrita en las recomendaciones 3GGP2 y en los estándares TIA como [IS835] y [TS115]. Esta arquitectura permite a los proveedores de servicio celular inalámbrico de CDMA2000 ofrecer servicios bidireccionales de paquetes de datos usando el protocolo IP. Para proporcionar esta funcionalidad, CDMA2000 utiliza dos métodos de acceso: IP Simple e IP Móvil.

En IP Simple, el proveedor de servicio debe asignar al usuario una dirección IP dinámica. Esta dirección permanece constante mientras el usuario mantiene la conexión con la misma red IP dentro de un dominio del portador inalámbrico –esto es, mientras que el usuario no salga del área de cobertura del mismo nodo PDSN (*Packet Data Serving Node*). Sin embargo, una nueva dirección IP debe ser obtenida cuando el usuario se mueve hacia un área geográfica conectada a una red IP diferente –esto es, dentro del área de cobertura de otro PDSN. El servicio de IP Simple no incluye ningún esquema de *tunneling* y soporta movilidad sólo dentro de los límites de cierta área geográfica.

En IP Móvil, la estación móvil está enlazada al nodo PDSN, que soporta funcionalidad FA, y su HA le asigna una dirección IP. IP Móvil permite a la estación móvil mantener su dirección IP por la duración de la sesión mientras se está desplazando en la red CDMA2000 u otros sistemas que soportan IP Móvil.

Para las estaciones móviles compatibles con un estándar TIA/EIA [IS2000] enlazadas a una red CDMA2000-1x, están disponibles tasas de datos que pueden variar entre la tasa fundamental de 9.6 Kbps y cualquiera de las siguientes tasas ráfaga: 19.2 Kbps, 38.4 Kbps, 76.8 Kbps, 153.6 Kbps.

Estas ráfagas de más alta velocidad son asignadas por la infraestructura en base a las necesidades del usuario y la disponibilidad de los recursos (ancho de banda del enlace por aire y elementos de la infraestructura). Las ráfagas son asignadas a un móvil dado por una duración de tiempo de 1 a 2 segundos. Los recursos y la situación del móvil son entonces revaluados. La asignación de ráfagas es ejecutada independientemente de los canales de avance y de reversa.

4.3.1 Arquitectura de CDMA2000 para Paquetes de Datos

La arquitectura del sistema de datos de CDMA2000 está basada en los siguientes componentes (como se muestra en la figura 4.3):

- Una estación móvil en forma de un teléfono, un PDA, o una tarjeta PCMCIA en una computadora portátil que soportan al cliente IP Simple o IP Móvil, o ambos.
- Red de Radio Acceso (RAN) CDMA2000-1x.
- Función de Control de Paquetes (PCF).
- Nodo de Servicio de Paquetes de Datos (PDSN) que soporta funcionalidad FA en caso de IP Móvil.
- Servidores AAA locales y exteriores.
- Agente Local (para el método de acceso de IP Móvil).

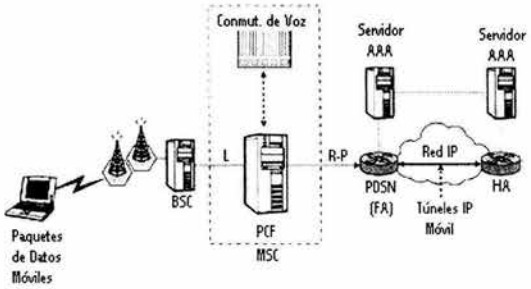


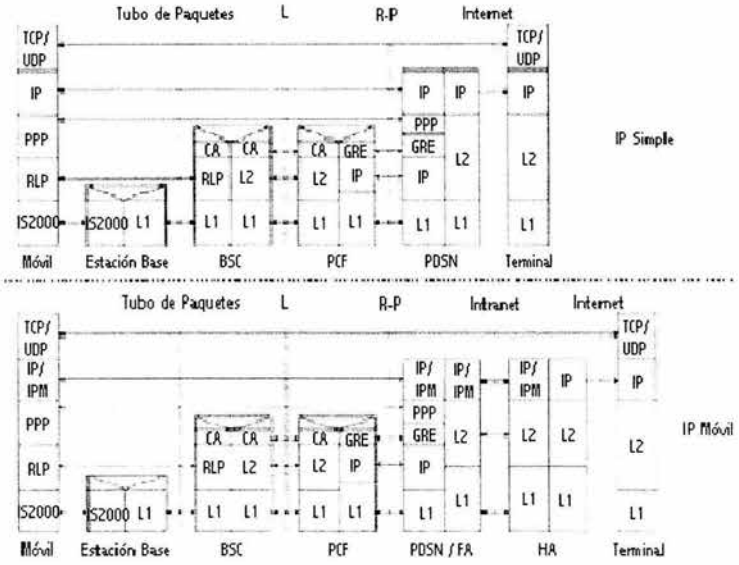
Figura 4.3 Ejemplo de la arquitectura de conmutación de paquetes de CDMA2000

Cuando la estación móvil se conecta a la estación base de CDMA2000, primero establece una conexión hacia un nodo PDSN. En el caso de IP Móvil, la estación móvil es conectada a su HA de servicio por un túnel entre el nodo PDSN/FA y el HA establecido utilizando IP Móvil. La dirección IP de la estación móvil es asignada del espacio de direcciones de su red local, proporcionada estática o dinámicamente por el HA en el comienzo de la sesión. Un alto nivel de autenticación y autorización de IP Móvil son ejecutadas por el nodo PDSN y el HA en la infraestructura AAA.

En el caso de IP Simple, la dirección debe ser asignada a la estación móvil por el nodo PDSN y no puede ser proporcionada estáticamente en la estación móvil. La autenticación para este método de acceso está basada sólo en el nodo PDSN.

La conexión entre la estación móvil y su nodo PDSN de servicio requiere una segunda capa de conectividad para establecer una conexión IP exitosa. La conectividad es proporcionada por el protocolo PPP y soporta IPCP, LCP, PAP y CHAP. El protocolo PPP es iniciado por la estación móvil durante la negociación de la conexión y es terminado por el nodo PDSN. Entre la radio red de CDMA2000 y el nodo PDSN, el tráfico PPP es encapsulado dentro de la interfaz R-P (*Radio-Packet*).

En la figura 4.4 se muestran ejemplos del *stack* de protocolos CDMA2000 para los casos de IP Simple e IP Móvil.



CA - Capa de Adaptación usada para tapar la información mientras un enlace inactivo es reconectado
L1 - Capa física
L2 - Capa de enlace

Figura 4.4 Ejemplos de las pilas de protocolos del servicio de datos de CDMA2000

La función PCF mostrada en esta figura es el elemento de la red de radio acceso de CDMA2000 responsable de la instalación y procesamiento de la interfaz R-P. PCF es implementada como un componente del controlador de la estación móvil CDMA2000. Una vez que las conexiones de la capa de enlace son establecidas, la función PCF simplemente transmite las tramas PPP entre el dispositivo móvil y el nodo PDSN. Otra importante función de PCF es proporcionar el soporte de micro-movilidad, lo cual se realiza permitiendo a la estación móvil cambiar la función PCF mientras se mantiene anclado en el mismo PDSN y almacena los datos de usuario mientras un radio enlace inactivo es reconectado.

El papel más importante del nodo PDSN en la arquitectura de CDMA2000 es terminar las sesiones PPP originadas en la estación móvil y proporcionar funcionalidad FA, en caso de que se requiera servicio de IP Móvil, o entregar los paquetes IP al siguiente salto cuando se usa IP Simple. Finalmente, el nodo PDSN es responsable del establecimiento, mantenimiento y terminación de la conexión de la capa de enlace basada en PPP hacia la estación móvil.

Para el servicio básico de Internet utilizando el método de acceso de IP Simple, el nodo PDSN asigna una dirección dinámica al móvil, termina el enlace PPP del usuario, y envía los paquetes directamente hacia Internet vía el *gateway por default* de la red IP central del proveedor de servicio. Los paquetes de la estación móvil pueden ser verificados para asegurar que el móvil está usando la dirección IP fuente asignada por el nodo PDSN.

Para el método de acceso de IP Móvil, el nodo PDSN establece la conectividad del protocolo IP Móvil hacia la red local de la estación móvil representada por el HA, el cual es responsable de la asignación de la dirección IP. El nodo PDSN debe soportar una funcionalidad de cliente AAA para ayudar a la autenticación parcial del móvil por el servidor AAA local. Por [IS835], el nodo PDSN es también requerido para soportar el encabezado de compresión TCP/IP *Van Jacobson* y tres

algoritmos de compresión PPP: *Stac LZS, MPPC, y Deflate* –este último es el más usado en las estaciones móviles basadas en Linux y UNIX.

La interfaz R-P que conecta a la función PCF y al nodo PDSN –también definida por TIA/EIA como A10/A11- es una interfaz abierta basada en el protocolo de *tunneling* GRE y es usada para conectar la radio red y el nodo PDSN. El protocolo de la interfaz R-P es similar a IP Móvil donde la función PCF actúa como el FA y el nodo PDSN actúa como el HA (la interfaz R-P utiliza túneles GRE para el tráfico y mensajes de IP Móvil como RRQ/RRP para señalización). Aparte de soportar la interfaz R-P, los dispositivos móviles basados en IP pueden cruzar los límites del controlador de la estación móvil sin impactar la continuidad de las sesiones del usuario. En otras palabras, si el usuario se mueve a otra área de cobertura de un controlador, la sesión del usuario no se desconecta y el usuario no es forzado a reconectarse vía un nuevo controlador y obtener una dirección IP nueva. Esto se realiza ejecutando *transferencias PCF* mientras se mantiene a los dispositivos móviles anclados en el mismo PDSN. Sin embargo, esto requiere que todos las funciones PCF en servicio tengan conexiones de red hacia el mismo *pool* de PDSNs.

4.3.2 Perspectiva de la Estación Móvil

La estación móvil CDMA2000 puede autenticarse con la base de datos HLR del proveedor de servicio para el acceso inalámbrico y autenticarse con el nodo PDSN y el HA, usando los métodos de acceso de IP Simple o IP Móvil, para el acceso a la red de datos. Se requiere que las estaciones móviles soporten un protocolo PPP estándar y que sean capaces de soportar autenticación basada en CHAP durante la fase de autenticación PPP para el servicio de IP Simple. Para el servicio de IP Móvil, el dispositivo móvil debe soportar el cliente IP Móvil. En este modo, la estación móvil se comunica con su HA vía el nodo PDSN de servicio en la red visitada. Si el móvil soporta uno o más de los algoritmos de compresión PPP opcionales como MPPC o Stac LZS, entonces la compresión PPP puede ser negociada durante la fase de conexión con el nodo PDSN, optimizando así el uso de los recursos de la radio red y engrandeciendo la experiencia del usuario mediante una tasa de transferencia efectiva más alta.

4.3.2.1 Letargo

Se espera que la estación móvil soporte el "letargo" del enlace por aire, lo cual permite al móvil o al controlador de la estación móvil descansar la conexión activa del enlace por aire después de un periodo de inactividad y liberar la interfaz de aire y los recursos de la estación base. Si la estación móvil o la función PCF asociada tienen paquetes para enviar mientras están inactivos, la conexión es reactivada y la transmisión continua. Las estaciones móviles inactivas son definidas como las estaciones que no tienen una conexión activa de la capa de enlace hacia la función PCF. Todas las estaciones móviles –activas o inactivas- registradas que utilizan el método de acceso de IP Móvil tienen una entrada en la lista de visitantes del nodo PDSN y un lazo con el HA correspondiente.

El nodo PDSN que atiende a los usuarios en la red exterior sirve como el ruteador por *default* para todos los usuarios móviles registrados, activos o inactivos. Para el modo de IP Móvil el nodo PDSN/FA guarda el tiempo restante del *registro de tiempo de vida* de cada estación móvil en su tabla de ruteo y la estación móvil es responsable de renovar su tiempo de vida con el HA. Si el móvil no se ha registrado antes de que expire su registro de tiempo de vida, el nodo PDSN cerrará el enlace con la función PCF para este móvil y termina la sesión. Una vez que el registro de tiempo de vida de la estación móvil ha expirado, el nodo PDSN/FA detendrá los paquetes encaminados hacia ésta.

Para recibir y enviar paquetes, las estaciones inactivas deben hacer la transición hacia el estado activo. Dado que cualquier estación móvil en cualquier momento puede estar en estado activo o inactivo, el nodo PDSN generalmente no requiere una indicación del estado de los enlaces PPP hacia las estaciones móviles. El tráfico puede llegar sobre el enlace inactivo en cualquier tiempo, forzando a la estación móvil asociada a la transición al estado activo. Para el estado activo, los enlaces PPP transportan tráfico, el nodo PDSN termina la sesión PPP con la estación móvil y

retransmite el tráfico IP encapsulado hacia el móvil desde el HA o desde el móvil hacia el HA vía un túnel de reversa. Existe un túnel separado para cada HA único para todos los usuarios registrados.

4.3.2.2 Tipos de Estación Móvil

Hay dos tipos básicos de configuración de la estación móvil –el modelo de retransmisión y el modelo de red. En el modelo de retransmisión, la terminal móvil CDMA2000 está conectada a otro dispositivo terminal de datos portátil como una *laptop*, un dispositivo informático de bolsillo, o alguna otra terminal de datos. El teléfono del modelo de retransmisión no termina alguna de las capas del protocolo excepto para la capa física de CDMA2000 (interfaz de radio) y las capas RLP. El dispositivo terminal enlazado debe terminar todos los otros protocolos de las capas más altas (PPP, IP, TCP/UDP, etc.).

Las estaciones móviles del modelo de red, además de la interfaz de radio, terminan todos los protocolos necesarios y no requieren algún dispositivo terminal de datos adicional. El teléfono móvil por sí mismo proporciona entrada a todo usuario y despliega las capacidades para hacer uso de la red de paquetes de datos. Ejemplos de este tipo de teléfono incluyen el teléfono "inteligente" o el teléfono "*micro-browser*". Estos dispositivos normalmente incluyen algún navegador Web o alguna aplicación de servicio de información, así como una pantalla para ver la información obtenida desde el servidor de Internet. Tal tipo de terminales puede ofrecer la capacidad para conectar una l*aptop* a una red de datos vía una conexión PPP terminada en la misma terminal.

4.3.3 Niveles de Movilidad de CDMA2000

La arquitectura de paquetes de datos de CDMA2000 define tres niveles de movilidad para la estación móvil, según se ilustra en la figura 4.5.

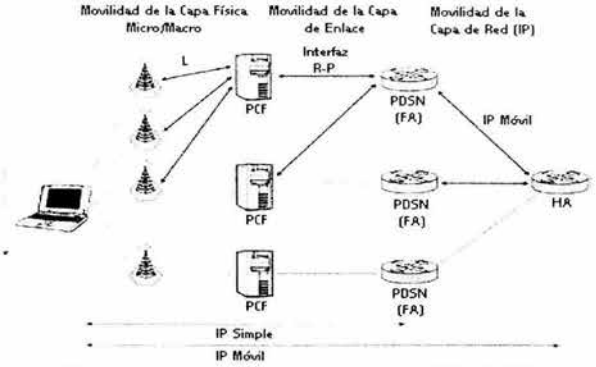


Figura 4.5 Jerarquías de movilidad de CDMA2000

Un nivel está representado en la capa física por el *handoff* suave o semisuave de BTS-a-BTS, mientras la estación móvil está anclada en la misma PCF. Esto se realiza por el radio acceso de CDMA2000 y es invisible para la función PCF y el nodo PDSN.

El segundo nivel de movilidad está representado por la interfaz R-P sobre la capa de enlace, que permite un *handoff* transparente de PCF-a-PCF mientras mantiene la sesión en el mismo PDSN. En este caso, las dos opciones previamente descritas entran en juego: activo e inactivo. En el estado activo, cuando el usuario cruza el límite de la PCF, el *handoff* es transparente para la estación móvil. La estación móvil participa en un *handoff* semisuave hacia el nuevo controlador de la estación base (BSC), mientras la sesión de datos de la capa de enlace permanece en la PCF

original por la duración de la llamada y el móvil se encuentra en estado activo. En otras palabras, cuando la estación móvil está en estado activo, no ocurrirá un cambio de PCF.

Cuando un móvil cruza el límite de cobertura de una PCF mientras está inactivo, el móvil tendrá una reactivación en un nuevo BSC para establecer una nueva conexión a una PCF. La nueva PCF intenta asignar al móvil su PDSN actual. Si la nueva PCF se ha conectado a este PDSN, la sesión PPP previamente establecida entre la estación móvil y el PDSN no será afectada.

El tercer nivel de movilidad, la capa de red, es el *handoff* inter-PDSN, basado en el uso del protocolo IP Móvil. Asumamos que la estación móvil se ha registrado con el HA y el nodo PDSN (la estación móvil ha sido autenticada por cada uno) para establecer el túnel de IP Móvil sobre el cual el tráfico es distribuido. Cuando el móvil vaga hacia una localización que es atendida por una PCF conectada a un PDSN diferente, el móvil recibe una indicación de que debe registrarse con este nuevo PDSN. Este registro actualiza la tabla de movilidad en el HA, de modo que todo el tráfico subsecuente es encaminado hacia el nuevo PDSN para este móvil. En este caso el enlace PPP del móvil es impactado por este cambio mientras que la capa IP permanece intacta.

Note que el último tipo de *handoff* no está disponible en el modo de IP Simple; IP Simple proporciona sólo movilidad parcial, vía los otros dos niveles, a la estación móvil. Una de las funciones de la interfaz R-P es traer el servicio de IP Simple casi igual en funcionalidad al servicio de IP Móvil. Por ejemplo, maneja las situaciones donde la estación móvil cambia su punto de enlace hacia la red de modo que frecuentemente el establecimiento del túnel IP Móvil introduce significante elevación en la red en términos del incremento de los mensajes de señalización. Otro problema es el estado latente del establecimiento de cada canal nuevo, lo cual introduce retrasos o interrupciones durante los cuales los datos de usuario no están disponibles. Este retardo es inherente al viaje redondo en el que incurre IP Móvil mientras la petición de registro es enviada al HA y la respuesta es enviada de regreso al nodo PDSN.

4.3.4 AAA Móvil en CDMA2000

CDMA2000, al igual que la mayoría de los sistemas celulares, soporta el concepto de redes locales y redes visitadas. Un suscriptor de CDMA2000 tiene una cuenta establecida con un portador inalámbrico, el cual proporciona al usuario servicios inalámbricos de voz y datos. Este mismo portador inalámbrico puede proporcionar al suscriptor móvil una red local. La red local tiene información del perfil del usuario e información de autenticación. Cuando el usuario anda dentro del territorio de un portador inalámbrico diferente –esto es, una red visitada- este portador debe obtener la información de autenticación y el perfil de servicio para este usuario particular de la red local del usuario. El perfil de servicio indica qué recursos de radio son autorizados al usuario, tales como ancho de banda máximo o prioridad de acceso. En CDMA2000 los perfiles de los usuarios son guardados en una base de datos HLR (*Home Location Register*) localizada en la red local y son temporalmente recuperados en una base de datos VLR (*Visitor Location Register*) localizada en la red exterior.

Procedimientos similares tienen lugar para autenticar el acceso del usuario a redes de datos. La arquitectura de paquetes de datos de CDMA2000, descrita en la figura 4.6, está basada en el concepto de redes de datos local y exterior representadas por el HA y el PDSN y los servidores AAA local y exterior –por ejemplo, RADIUS o DIAMETER.

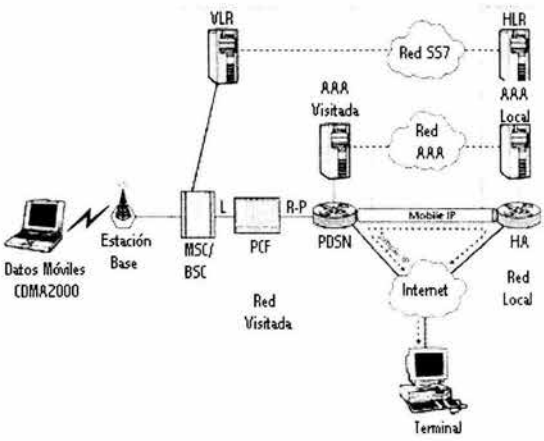


Figura 4.6 Típica red central de CDMA2000 con subsistemas AAA

Las estaciones móviles que solicitan servicio de datos en los sistemas CDMA2000 son autenticadas dos veces: en la capa física y en la capa de enlace. La autenticación en la capa física es ejecutada por la infraestructura HLR y VLR del sistema celular inalámbrico. Está basada en un identificador internacional de la estación móvil (IMSI, *International Mobile Station Identifier*). En la capa de enlace CDMA2000, la autenticación de la estación móvil es conducida por la infraestructura de servidores y clientes AAA. Está basada en el identificador de acceso a la red (NAI) –esto es, un identificador de usuario de la forma usuario@dominio_local, el cual permite a la red visitada identificar el servidor AAA de la red local mediante la etiqueta "dominio-local" de la dirección IP local. NAI permite la distribución de información específica de seguridad de IP Móvil para soportar la autenticación en el nodo PDSN/HA durante el registro del móvil, asignación del HA, y *handoff* inter-PDSN.

Note que la red de datos AAA autentica al usuario, contrario a la autenticación de la capa física, la cual autentica al móvil. Por lo tanto, los usuarios que desean acceder a redes de datos públicas o privadas tienen que realizar una secuencia *login*-contraseña, además la autenticación del dispositivo móvil toma lugar en la fase de registro.

El subsistema de datos de CDMA2000 proporciona dos mecanismos de autenticación del usuario cuando son solicitados los métodos de acceso de IP Simple o IP Móvil. Para el método de acceso de IP Simple, la autenticación está basada en el protocolo CHAP, el cual es una parte de la negociación PPP. En CHAP, el nodo PDSN exige a la estación móvil con un valor aleatorio al cual debe responder con una firma basada en MD-5, un nombre de usuario, y una contraseña. El PDSN pasa el par demanda/respuesta al servidor AAA local para la autenticación del usuario.

Para IP Móvil, el nodo PDSN manda una demanda similar dentro de un mensaje de anuncio del agente a la estación móvil. La estación móvil debe responder a la demanda con una firma y el NAI es verificado por la red local, pero esta vez la respuesta es enviada con la petición de registro de IP Móvil antes del establecimiento de la sesión PPP. En ambos casos los datos de contabilidad son colectados en el nodo PDSN y transferidos al servidor AAA. El nodo PDSN colecta las estadísticas de datos usados para cada usuario, combina éstas con los registros de contabilidad de radio acceso enviadas por la PCF, y los envía al servidor AAA local.

Para el *roaming* de usuarios, el servidor AAA puede ser configurado para mandar una copia de todos los registros de contabilidad de RADIUS hacia el servidor AAA local además de guardar una copia en el servidor AAA de la red visitada.

Cuando ocurre un *handoff* entre dos PDSNs, un mensaje de *Alto a Contabilidad* es enviado al servidor AAA desde el nodo PDSN liberado, un mensaje de *Inicio de Contabilidad* es enviado al servidor AAA desde el nuevo nodo PDSN que se conecta. El mensaje de Alto a Contabilidad puede llegar algún tiempo después del mensaje de Inicio de Contabilidad (el PDSN liberado puede no estar enterado de que el móvil se ha movido, pero debe esperar un mensaje de Registro de Tiempo de Vida o PPP Inactiva para terminar la sesión). Esto significa que el servidor debe aceptar múltiples secuencias alto/inicio de diferentes PDSNs. Cuando un contador PPP de inactividad o un tiempo de vida de IP Móvil expira, o el móvil termina la sesión, el enlace R-P es liberado y un mensaje de Alto a Contabilidad es enviado al servidor AAA.

4.4 Paquetes de Datos en GSM y UMTS: GPRS y Dominio UMTS PS

En esta sección describimos los sistemas GPRS y dominio UMTS PS, y los servicios ofrecidos a las estaciones móviles. Vemos las posibles maneras en que un móvil puede acceder a redes de paquetes de datos, así como cuáles son los protocolos que pueden ser utilizados y de que forma toma lugar la autenticación.

4.4.1 Elementos de GPRS

El sistema GPRS es una extensión del sistema GSM para paquetes de datos, el cual fue originalmente diseñado para servicios de circuito. GPRS permite soportar transmisiones de datos basados en paquetes sobre la interfaz de radio y la movilidad de los paquetes de datos dentro de la red central. El despliegue de GPRS impone la actualización del software de los subsistemas de la estación base (BSS), los cuales permiten la multiplexación de los servicios de datos sobre las ranuras que no son ocupadas por los servicios de voz, control de flujo, y los mecanismos de retransmisión necesarios para entregar servicios de datos sobre la tecnología de radio transmisión de GSM. Esto requiere también la actualización del software de la base de datos HLR y la instalación de nuevos nodos en la red central: SGSN (*Serving GPRS Support Node*) y GGSN (*Gateway GPRS Support Node*). DNS, sistema de administración de direcciones, funciones AAA, facturación, y red inteligente son los componentes adicionales que forman parte de los servicios avanzados de GPRS.

La arquitectura de GPRS es descrita en la figura 4.7:

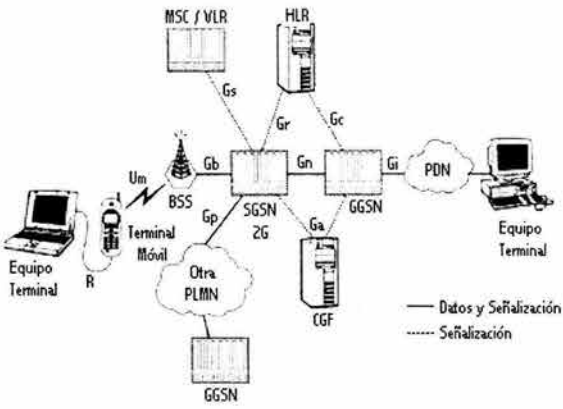


Figura 4.7 Arquitectura de GPRS

El nodo SGSN en GPRS, ofrece servicios de compresión en la capa de red, segmentación y funcionalidad de reensamble, *framing* lógico en la capa de enlace y multiplexación, cifrado, así

como señalización y administración de la movilidad de la estación móvil (dentro del BSS, entre SGSNs), y la gestión del establecimiento de túneles GTP hacia nodos GGSN. El nodo SGSN también interactúa con la base HLR y la red inteligente, el controlador de la estación móvil, y el Centro de Servicio de SMS (SMS-SC).

El nodo GGSN "ancla" la sesión de comunicaciones de datos y proporciona acceso a redes de paquetes de datos soportando la terminación de túneles GTP desde el SGSN al cual la estación móvil está enlazado. Los nodos GGSN también son utilizados en redes IP para proporcionar una base y un *gateway* para servicios avanzados de paquetes de datos tales como navegador Web, WAP, redes privadas remotas, incluyendo redes usadas para proporcionar soporte de movilidad para usuarios intra-PLMN, *roaming* (red *GPRS Roaming Exchange* o GRX).

4.4.2 Elementos de UMTS

UMTS ofrece servicios de paquetes de datos sobre su dominio PS. Su arquitectura se muestra en la figura 4.8, es similar a la arquitectura de GPRS. Los mismos nodos de red están involucrados en la red central, aunque el protocolo GTP utilizado en UMTS (GTPv1) no es compatible con las versiones del protocolo GTP usadas para GPRS (GTPv0). Existen otras diferencias en las capacidades de servicio –por ejemplo, UMTS soporta su propio marco de QoS con más capacidades multimedia. Además, el nodo SGSN de UMTS, no termina los protocolos de la capa de enlace, no proporciona compresión en la capa de red o cifrado. En lugar de eso, simplemente retransmite los paquetes entre GGSNs y los Controladores de la Radio Red (RNCs) sobre túneles GTP. En UMTS, la función del RNC es manejar la movilidad de las estaciones móviles entre los nodos B (estaciones base de UMTS).

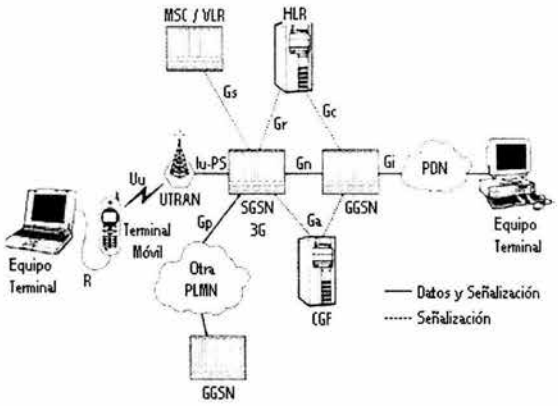


Figura 4.8 Arquitectura de UMTS

4.4.3 Arquitectura de GPRS y del Dominio UMTS PS

El sistema GPRS define principalmente dos componentes: el Subsistema de la Estación Base (BSS) y la *backbone* PLMN. El BSS de GPRS es el BSS de GSM aumentado con una Unidad de Control de Paquetes (PCU, *Packet Control Unit*) que es usada para soportar los servicios de paquetes. La *backbone* PLMN incluye dos nodos nuevos: el nodo SGSN y el nodo GGSN. El GGSN y el SGSN están conectados vía una red IP e interactúan vía la interfaz Gn, basados en el protocolo GTP.

Cuando un usuario vaga, se enlaza hacia un nodo SGSN en la red visitada y hacia un nodo GGSN en la red local o en la red visitada. Si el nodo GGSN está en la red local, la red IP utilizada para

conectar el SGSN visitado y el GGSN local es nombrada *Inter-PLMN Backbone Network*. La red *backbone Inter-PLMN* es usualmente ofrecida por los proveedores de servicio de red bajo el nombre de *GPRS Roaming Exchange* (GRX). El SGSN en la red visitada y el GGSN en la red local interactúan sobre la red GRX vía una interfaz, llamada Gp, la cual es completamente idéntica a la interfaz Gn.

Las especificaciones de GPRS definen nuevas capas del protocolo en el BSS –el Control del Radio Enlace (RLC, *Radio Link Control*) y el Control de Acceso al Medio (MAC, *Medium Access Control*)- que permiten el uso de la estructura de las tramas de GSM para GPRS. El sistema GSM permite usar de una hasta ocho ranuras de tiempo en ambas direcciones (ascendente y descendente). Las especificaciones estándar definen la manera de adaptar diferentes protocolos de red al servicio lógico de enlace ofrecido por este sistema –*Sub-Network Dependent Convergence Protocol* (SNDCP)- mediante la transmisión de tramas de Control Lógico del Enlace (LLC, *Logical Link Control*) entre la estación móvil y el SGSN. Esta funcionalidad es proporcionada por la PCU.

La red RAN de GSM, aumentada con la funcionalidad de la PCU, está conectada a la central de GPRS vía la interfaz Gb, la cual define un servicio de red basado en *Frame-Relay* en lo alto del protocolo del subsistema de la estación base de GPRS (BSSGP) (figura 4.9). BSSGP es usado para soportar canales lógicos en lo alto del servicio de *Frame Relay*. Estos canales lógicos son utilizados para implementar un protocolo LLC para encaminar las tramas entre el BSS y la central, así que el BSC + PCU puede encaminar las tramas LLC hacia la célula correcta. En la dirección ascendente, el protocolo BSSGP transporta la información de identificación de la célula, y cualquier trama LLC transportada en el protocolo BSSGP puede ofrecer información de localización. Típicamente, una estación móvil actualiza su localización (actualización de la célula) cuando está dentro de una sesión activa (enviando y recibiendo datos) mediante el envío de una trama LLC.

SNDCP, LLC, y BSSGP –así como el servicio de red basado en *Frame Relay*- están terminados en el nodo SGSN. Ya que tanto el tráfico de usuario como la información de control son transportados sobre estos protocolos, y los servicios de la capa de enlace hacia el móvil son terminados en el SGSN, un SGSN es particularmente complejo. Esta complejidad potencialmente trae severas limitaciones sobre su escalabilidad. Para manejar está situación, durante el desarrollo de los estándares de UMTS, se tomó la decisión de no terminar los servicios de la capa de enlace en el SGSN, reduciendo así la complejidad de este elemento y permitiendo la escalabilidad para soportar muchos más suscriptores y un área de cobertura más amplia. La escalabilidad de un SGSN para cubrir un área más amplia es importante para minimizar la señalización de administración de la movilidad asociada al proceso de *handoff*. En UMTS, el proyecto 3GPP definió una interfaz entre la red RAN y la red central del dominio PS, nombrada interfaz Iu-PS. Esta interfaz está basada en IP sobre transporte ATM para el plano de usuario y el protocolo RANAP (*Radio Access Network Application Part*) para el plano de control. RANAP es una aplicación SCCP (*Signaling Connection Control Part*) de usuario. SCCP es transportado sobre una banda ancha SS7 o un transporte IP basado en los protocolos SIGTRAN –a saber, M3UA y SCCP.

Los paquetes de usuario son transferidos sobre la interfaz Iu-PS usando transporte GTP/UDP/IP, y entonces son retransmitidos por el RNC hacia la estación móvil usando protocolos de radio enlace (PDCP/RLC/MAC). La funcionalidad del protocolo PDCP (*Packed Data Convergence Protocol*) en UMTS es similar a SNDCP en GPRS. También soporta protocolos de compresión de encabezado que son particularmente utilizados para la reducción de la saturación para aplicaciones de tiempo real –en particular, para aplicaciones de Voz sobre IP. Las capas RLC y MAC son usadas para implementar la capa de radio enlace. Éstas implementan los canales lógicos de la capa de enlace sobre la interfaz de radio W-CDMA de la capa física. La figura 4.9 sintetiza la discusión de los *stacks* de protocolos.

La terminal móvil comunica información de control hacia la red central de UMTS o GPRS que usa un protocolo de capa 3 de la interfaz de radio (RIL3). Este incluye administración de la movilidad y administración de la sesión en GPRS (o paquetes en UMTS). En GPRS, RIL3 es transportado sobre el canal LLC NULL y es manejado por el SGSN en la red central. En UMTS, este protocolo

es transportado usando el procedimiento de transferencia directa sobre el protocolo RANAP. El SGSN elabora la información de control desde la terminal, y como consecuencia, puede interactuar con otras entidades dentro de la red. Por ejemplo, puede iniciar diálogos MAP con el registro HLR para procedimientos de seguridad, recuperación de información del suscriptor, o propósitos de actualizar la localización.

Las sesiones de paquetes de datos en GPRS y UMTS son establecidas instalando y manteniendo túneles GTP hacia los nodos GGSN. Un túnel GTP es una encapsulación de los paquetes de usuario entre el GGSN y el SGSN en GTP/UDP/IP.

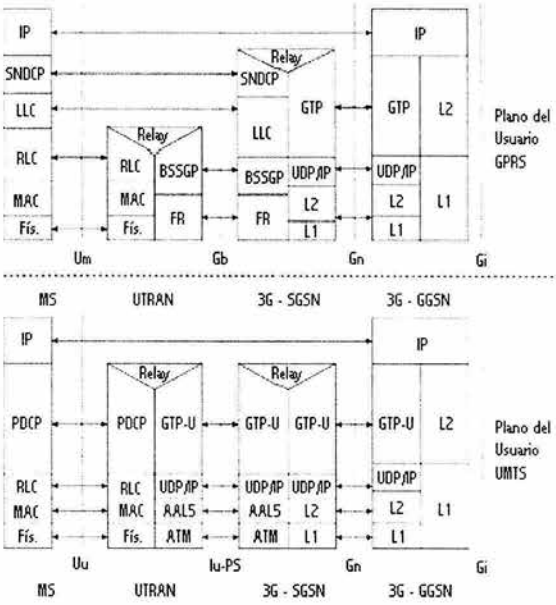


Figura 4.9 Plano del usuario y plano de control de GPRS

Otra función del nodo SGSN es colectar los datos de carga y la comunicación hacia una función CGF (*Charging Gateway Function*) sobre la interfaz Ga (ver figura 4.7). La interfaz Ga está basada en el protocolo GTP. El nodo SGSN también puede soportar servicios SMS vía la interfaz Gd hacia el SMS-GMSC e interactuar con el MSC/VLR vía la interfaz Gs para coordinar el *paging* y la actualización de la localización.

4.4.4 Capacidades del Servicio de GPRS y del Dominio UMTS PS

Los sistemas GPRS y UMTS PS son multi-protocolos y neutrales hacia la naturaleza de la capa de red o capas de enlace del tráfico de usuario. Los protocolos de usuario son también llamados PDPs (*Packet Data Protocols*). El tipo de protocolo es identificado con el término "tipo PDP".

Los sistemas GPRS y UMTS PS ofrecen un canal de transporte *informal* desde el GGSN hacia la estación móvil. Este canal está caracterizado por un número de parámetros QoS, los cuales son diferentes para las liberaciones antes de R99 y las liberaciones de R99 hacia delante. En R99 y liberaciones posteriores, es posible diferenciar el manejo de paquetes pertenecientes a la misma sesión de usuario. Esto se realiza estableciendo múltiples portadores de diferente clase de tráfico y perfil QoS, asociados con la misma sesión, y enviando los paquetes hacia los portadores

apropiados basados en las mismas reglas de clasificación establecidas en el GGSN y en la estación móvil.

4.4.5 Terminales de GPRS y de UMTS PS

Existen tres clases diferentes de estaciones móviles de GPRS:

Clase A. Esta clase permite el soporte concurrente de servicios GSM y GPRS.
Clase B. En esta clase, la estación móvil monitorea los canales de *paging* de GSM y de GPRS, pero solo puede soportar un servicio a la vez.
Clase C. En esta clase, la estación móvil solo soporta servicio GPRS (como un dispositivo de datos).

Las terminales clase A requieren dos transmisores-receptores GSM separados operando en diferentes frecuencias, con servicios de paquetes y circuitos independientes. Debido a la complejidad de estas terminales, en R99, los operadores y los fabricantes trabajaron en la definición de terminales que soporten el Modo Dual de Transferencia (DTM). Desde una perspectiva de servicio, este enfoque ofrece la coexistencia de servicios de voz simultáneos de GPRS y GSM como en una terminal Clase A, pero desde una perspectiva de *paging* son más similares a un dispositivo Clase B y requieren un transmisor-receptor. Esto es posible mediante una actualización del BSS para encaminar los mensajes de *paging* sobre el mismo canal usado por GPRS, cuando la estación móvil está enlazada. Note que esto permite que la coordinación del *paging* suceda en el BSS, al igual que en los sistemas UMTS.

Una terminal móvil con capacidad de acceso a GPRS o UMTS PS puede ser:

- Un dispositivo integrado que ofrece recursos informáticos y acceso inalámbrico de datos en una unidad física.
- Un dispositivo compuesto de dos elementos: uno dedicado al acceso inalámbrico y el otro un dispositivo con capacidad para aplicaciones de datos.

La última configuración es similar a las *laptops* de hoy, las cuales están equipadas con tarjetas módem PCMCIA o una conexión serial a un módem. De hecho, los estándares 3GPP definen la existencia de dos componentes lógicos de la estación móvil: el equipo terminal (TE) y la terminación móvil (MT). El TE es la parte con capacidad computacional y la MT es la parte dedicada al soporte de las capacidades de acceso inalámbrico de datos. Cuando el TE y la MT están implementadas como entidades físicas separadas, pueden ser conectadas por múltiples tecnologías (serial, infrarrojo, *Bluetooth*, etc.) con la capa de enlace basada en el protocolo PPP, u otra interfaz propietaria. Las figuras 4.7 y 4.8 muestran los dos componentes separados por la interfaz R.

Cuando la interfaz PPP es usada entre el TE y la MT, el tipo PDP IP puede ser usado, pero el material de autenticación y configuración no es transportado entre el GGSN y la MT utilizando PPP. Más bien, es encapsulado en un elemento de información de opciones de configuración del protocolo (PCOIE, *Protocol Configuration Options Information Element*), transparente retransmitido entre RIL3 y GTP por el nodo SGSN. De esta manera, PPP existe entre el TE y la MT, pero no entre la MT y el nodo GGSN. Este modo de acceso es llamado *acceso IP no transparente*. Las terminales móviles también vienen con el modo dual GPRS/GSM y capacidad UMTS.

CAPÍTULO 5

FUNDAMENTOS DE MVPN

5.1 Definición de VPN

VPN (*Virtual Private Netrwork*) combina dos conceptos: red virtual y red privada. En una red virtual, nodos remotos y geográficamente distribuidos pueden interactuar uno con el otro de la misma manera que lo hacen en una red donde todos los nodos están colocados. La topología de la red virtual es independiente de la topología física de las instalaciones usadas para soportarla. Un usuario casual de la red virtual, no está enterado de la instalación física de la red. Una red virtual es también manejada como una simple entidad administrativa.

Las redes privadas son usualmente definidas como instalaciones de red no compartidas que combinan terminales y clientes que pertenecen a la misma entidad administrativa. Un buen ejemplo de una red privada es una Intranet corporativa, la cual puede ser usada sólo por un cierto número de individuos autorizados que pertenecen a esa corporación en particular. Las redes privadas virtuales, son entonces, la emulación de redes de datos privadas seguras sobre instalaciones públicas de telecomunicaciones compartidas inseguras.

Las propiedades de una VPN incluyen mecanismos para la protección de los datos y el establecimiento de relaciones de confianza entre las terminales en las redes virtuales y la incorporación de varios métodos para hacer cumplir y mantener los acuerdos del nivel de servicio (SLAs) y la calidad del servicio (QoS) para todas las entidades que forman una VPN.

5.2 Bloques de una VPN

Las tecnologías sobre las cuales se construye una VPN, incluyen:

- Control del Acceso
- Autenticación
- Seguridad
- *Tunneling*
- Acuerdos del nivel de servicio

5.2.1 Control del Acceso

El control del acceso en las redes de datos es definido como una serie de políticas y tecnologías que gobiernan el acceso a los recursos de las redes privadas. Los mecanismos de control del acceso operan independientemente de la autenticación y la seguridad y básicamente definen qué recursos están disponibles para un usuario particular después de que ha sido autenticado. En el mundo de VPN las entidades físicas, como terminales remotas, *firewalls*, y *gateways* VPN involucradas en las sesiones de comunicación, son responsables usualmente del estado de la conexión VPN.

Ejemplos de decisiones incluyen:

- Iniciar
- Permitir
- Continuar
- Rechazar
- Terminar

El principal propósito de cualquier VPN es permitir el acceso selectivo y seguro a los recursos de redes remotas. Con seguridad y autenticación pero sin control del acceso, la VPN solo está protegiendo la integridad y confidencialidad del tráfico transmitido, y previniendo de usuarios desconocidos en la red, pero no protege los recursos de la red. El control del acceso usualmente depende de la información acerca de la entidad que solicita conexión, tal como la identidad o credenciales –así como de las reglas que definen las decisiones de control del acceso. Por ejemplo, algunas VPNs pueden estar gobernadas por un servidor centralizado u otro dispositivo VPN de control localizado en la central de datos del proveedor de servicio, o pueden ser administradas localmente por un *gateway* VPN en las redes privadas involucradas en la comunicación VPN.

La serie de reglas y acciones que define los derechos de acceso a los recursos de red es llamada *política de control del acceso*. La política de control del acceso permite la ejecución de la meta de un negocio. Por ejemplo, la política "Permiso de uso" puede ser implementada usando autenticación del usuario basada en RADIUS e incrementando un contador de tiempo cada vez que un usuario obtiene acceso. En teoría, un mensaje *RADIUS DISCONNECT* puede ser usado para interrumpir la sesión del usuario cuando son sobrepasadas 60 horas, pero algunas veces la política se puede hacer cumplir solamente en el tiempo de entrada al sistema, o quizás poniendo un límite de la duración de la sesión que pondría un límite superior de uso que excede el máximo de tiempo permitido. Políticas similares puede ser implementadas remplazando el límite de tiempo con un límite de crédito que puede estar asociado a una cuenta de prepago.

5.2.1.1 Política de Aprovisionamiento y Ejecución

Los ejemplos de mecanismos de política de aprovisionamiento y ejecución incluyen LDAP (*Lightweith Directory Access Control Protocol*), un estándar para interrogar a un directorio. Las definiciones de servicio y las instrucciones específicas de acceso son almacenadas en bases de datos centralizadas, a las que pueden acceder el equipo responsable de las decisiones de control del acceso, como ruteadores IP, *gateways* VPN, o aplicaciones de red inteligente. Las principales ventajas de estos métodos son la simplicidad y la facilidad de administración y aprovisionamiento. Con LDAP, por ejemplo, los cambios en las políticas pueden ser realizados por el proveedor de servicio y el administrador IT de la corporación sólo accediendo a un servidor que aloja una base de datos particular en vez de reaprovisionar la información almacenada localmente en muchos elementos de la red.

El uso de RADIUS une el proceso de autenticación del usuario con el control del acceso y la selección de la política de servicio. Una vez que la política de acceso es elegida, su ejecución toma lugar en el dispositivo preguntando a un depósito de la política que utiliza LDAP. En años recientes, otro protocolo llamado COPS (*Common Open Policy Service*) ha sido propuesto para implementar políticas de decisión y aprovisionamiento para muchos dispositivos simples.

5.2.1.2 Portal Cautivo

La función de control del acceso puede ser ejecutada en el punto de terminación de los protocolos de acceso aceptando el ingreso a la red solo después de que la fase de autenticación del protocolo de acceso ha sido completada exitosamente. De otra manera, es posible ejecutar el control del acceso vía un *enfoque de portal cautivo*. Este método es comúnmente utilizado en redes de acceso basadas en WLAN y en redes de acceso de banda ancha. Éste forza a los usuarios a que se autentiquen llenando una forma en una página Web, la cual es el único lugar al que pueden acceder después de obtener conectividad IP. Esto puede ser realizado mediante una funcionalidad TCP de redirección en los puertos 80, 8000, y 8080, los cuales son utilizados típicamente por http.

La funcionalidad TCP de redirección –implementada en un dispositivo de red o un ruteador ordinario, tiene lugar en el borde de una VPN (o cualquier red IP)- inspecciona todos los paquetes IP hasta la capa de transporte. Si el protocolo es TCP y el número de puerto es reconocido para HTPP, la dirección destino y el encabezado HTPP son modificados para solicitar la página Web

que corresponde a la credencial del portal de la página de entrada. Alternativamente, cuando el dispositivo de red no es construido para operar en la capa de aplicación, el mismo portal puede tener la inteligencia para responder siempre a las solicitudes HTPP que entran desde direcciones IP no registradas enviando vía HTPP la señal de la página Web. Una vez que las credenciales de usuario son colectadas y el usuario está autenticado, el dispositivo de red, informado por el portal, levanta la funcionalidad TCP de redirección y permite libremente el flujo del tráfico de usuario, quizá hasta que algún otro evento –como la inactividad del contador de usuario, el límite del tiempo de uso o el límite de volumen es excedido, un intervalo es requerido antes de nueva autenticación, o alguna redirección hacia alguna página- no modifique este estado.

Algunos proveedores de servicio aún no usan los portales cautivos basados en redirección TCP, quizá porque el equipo que tienen solo inspecciona los paquetes hasta la capa de red y puede estar configurado solo para permitir el acceso a ciertos destinos. En vez de eso, proporcionan acceso a los usuarios si deliberadamente apuntan sus navegadores hacia un URL impreso en una tarjeta de suscripción o una tarjeta de prepago que les proporcionan. Una vez que pasan la fase de autenticación, la red permite al usuario, identificado por su dirección IP, acceder a todos los destinos.

5.2.2 Autenticación

Una de las más importantes funciones que VPN soporta es la autenticación. En VPN, cada entidad involucrada en la comunicación debe ser capaz de identificarse con las otras partes involucradas y viceversa. La autenticación es el proceso que permite a las entidades que se comunican verificar sus identidades. Uno de los mecanismos más populares ampliamente utilizado en las redes de hoy en día es llamado PKI (ver capítulo 2). Éste es conocido como *autenticación basada en certificados*, y las partes involucradas en la comunicación autentican a cada una de las otras mediante el intercambio de sus certificados.

El proceso de autenticación involucra también proporcionar información de autenticación secreta, como una contraseña o un par demanda/respuesta de CHAP, hacia un autenticador, como un servidor de acceso a la red, que por su parte puede buscar un archivo local o preguntar a un servidor RADIUS. A este respecto la operación de VPN abarca dos tipos de autenticación: cliente-*gateway* y *gateway-gateway*. Un ejemplo de autenticación cliente-*gateway* en el ambiente de paquetes de datos de GPRS es la autenticación de usuarios basada en RADIUS que acceden al nodo GGSN. El otro caso es común cuando se instala una conectividad sitio-a-sitio, o cuando redes virtuales *dial-up* están usando un túnel L2TP la autenticación es requerida entre el concentrador de acceso L2TP (LAC) y el servidor de red L2TP (LNS).

5.2.3 Seguridad

La VPN puede estar segura mediante el despliegue de uno de los mecanismos de encriptación disponibles combinado con los sistemas de distribución de claves. Sin embargo, esta seguridad no está limitada a la encriptación del tráfico. Esto también involucra complejos procedimientos por parte del operador y sus proveedores, y cuando la VPN está basada en red, debe existir una relación de confianza entre el proveedor de servicio y el cliente VPN que requiere del despliegue de apropiados mecanismos de seguridad. Por ejemplo, el servidor AAA puede estar accesible sólo mediante mensajes de seguridad de RADIUS vía IPSec. También, el servidor AAA puede pertenecer a una red que no esté incluida en la VPN, para permitir el aislamiento del tráfico AAA del tráfico de usuario.

5.2.4 *Tunneling* Como la Base de VPN

Tunneling es sin duda la tecnología más importante sobre la cual se construyen las IP VPNs. *Tunneling* involucra la encapsulación de ciertos paquetes de datos dentro de otros paquetes de acuerdo a una serie de reglas implementadas en ambos extremos del túnel. Como resultado, el

contenido de los paquetes encapsulados se hace invisible para la red pública sobre la cual son transmitidos estos paquetes.

El concepto de *tunneling* aplicado a una red privada virtual es ilustrado en la figura 5.1. Aquí los paquetes enviados desde la terminal remota A hacia la terminal Z deben atravesar muchos otros *switches* y ruteadores. Si el ruteador C encapsula el paquete que viene de la terminal A y el *gateway* Y lo desencapsula, los otros nodos atravesados por este paquete solo reconocerán el paquete exterior encapsulado y no serán capaces de obtener alguna información acerca de su carga útil o de su punto destino final. De esta forma, la carga útil de los paquetes enviados entre C y Y solo será reconocida por estos dos nodos y las terminales A y Z que representan los puntos origen y destino del tráfico de datos. Esto efectivamente crea un túnel directo por el cual los paquetes son transportados con el nivel de seguridad deseado.

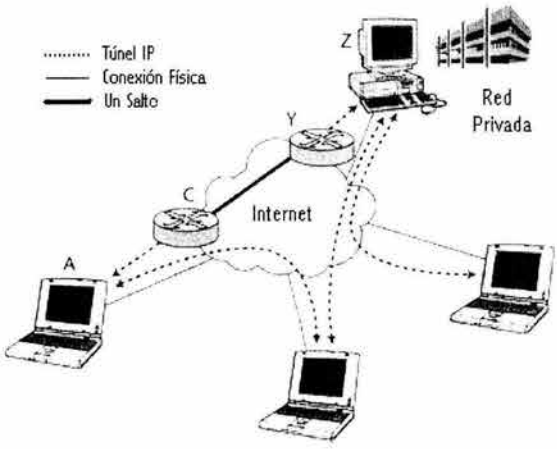


Figura 5.1 Construcción de túneles en una red privada virtual

El túnel puede estar definido por sus puntos finales, las entidades de red donde ocurre la desencapsulación, y el protocolo de encapsulación que es usado. Las técnicas de *tunneling* que soportan VPNs como L2TP o PPTP son usadas para encapsular las tramas de la capa de enlace (PPP). Similarmente, las técnicas de *tunneling* como IPIP y el modo túnel de IPSec son usados para encapsular los paquetes de la capa de red.

En el contexto de VPN, el *tunneling* puede realizar tres tareas:

- Encapsulación
- Transparencia de direccionamiento privado
- Integridad de los datos de extremo-a-extremo y protección de la confidencialidad

La transparencia de la dirección privada permite el uso de direcciones privadas sobre una infraestructura IP públicamente direccionable. Ya que los contenidos del paquete y sus atributos – como direcciones- son entendidos más allá de los puntos finales del túnel, el direccionamiento IP privado puede estar completamente enmascarado para las redes IP públicas que utilizan direcciones válidas (figura 5.2).

Las funciones de integridad y confidencialidad aseguran que una parte no autorizada no pueda alterar los paquetes del usuario durante la transmisión y que los contenidos de los paquetes permanezcan protegidos del acceso no autorizado. Por otra parte, el *tunneling* puede

opcionalmente proteger la integridad del encabezado del paquete IP exterior, proporcionando así autenticación del origen de los datos. Por ejemplo, en IP VPN, es posible utilizar el encabezado AH de IPSec para proteger las direcciones IP de los puntos finales del túnel.

Figura 5.2 Dirección IP privada enmascarada vía *tunneling*

Cuando es aplicada la técnica de *tunneling* para crear una VPN Móvil, estas cuatro funciones (encapsulación, transparencia de direccionamiento privado, integridad de los datos de extremo-a-extremo, y protección de la confidencialidad) deben estar acompañadas por una serie de mecanismos para proporcionar conmutación dinámica del túnel o restablecimiento para soportar la movilidad del usuario VPN. Los sistemas celulares modernos para paquetes de datos, como GPRS o CDMA2000, ya incluyen tales esquemas basados en GTP e IP Móvil, los cuales fueron originalmente diseñados para soportar movilidad. Los túneles móviles basados en estas tecnologías pueden ser concatenados en túneles estáticos en el borde de las redes inalámbricas para proporcionar una variedad de arquitecturas de MVPN.

5.2.4.1 Etiquetado (MPLS) y VPN

MPLS permite el envío de paquetes IP basados en direcciones IP sin destino sobre una *backbone* IP. Una de las aplicaciones de esta propiedad de MPLS es la ingeniería de tráfico –esto es, encaminar paquetes sobre direcciones determinadas por otros criterios y no solo en las rutas más óptimas y quizá basadas en la necesidad de ofrecer algún nivel de QoS, o para seleccionar los enlaces de costo mínimo. Otra aplicación importante de MPLS es la provisión de servicios VPN basados en red entre redes cliente basadas en múltiples sitios, también conocidas como VPNs multisitio. VPN basada en red es un servicio ofrecido por un proveedor de servicio en una forma explícita, vía un ruteador extremo del proveedor (PE) hacia las redes del cliente. Los ruteadores extremos del proveedor normalmente se conectan hacia sitios del cliente vía ruteadores extremos del cliente (CE) vía alguna tecnología de *tunneling*.

El uso de MPLS para ofrecer servicios de VPN está asociado con la habilidad para controlar la instalación de LSPs mediante algún protocolo de asociación descubrimiento/distribución del sitio VPN. Hay principalmente dos escuelas de pensamiento acerca del uso de MPLS para ofrecer VPNs. Una escuela piensa que un ruteador PE totalmente controlado por el proveedor y equipado con múltiples tablas de ruteo tendría que ser usado, a esto se le conoce como enfoque del ruteador monolítico. La otra escuela cree que el ruteador PE debería estar basado en ruteadores virtuales y que los clientes debería tener algún grado de habilidad para manejarlos.

El enfoque del ruteador PE monolítico está basado en la habilidad de que tal ruteador soporte una tabla de ruteo por cada sitio VPN, y cada una de estas tablas de ruteo indicaría al sitio de red del cliente las rutas *intradominio* usando el protocolo IBGP (*Internet Border Gateway Protocol*) y las rutas *interdominio* usando el protocolo BGP (*Border Gateway Protocol*). En el caso de un prefijo de red perteneciente a un sitio que se traslapa con otro prefijo de un sitio diferente anunciados por el mismo ruteador PE, el ruteador estaría acompañado por un ruteador que distinga la forma de la dirección VPN de la familia IPv4. Este ruteador puede estar asociado con dos atributos BGP adicionales –el atributo *VPN Objeto* y el atributo *VPN de Origen*- que ayudarían en la construcción de un filtro que puede ser usado para configurar VPNs sobre PEs. Una etiqueta acompaña la ruta, y el ruteador PE incluye su propia dirección IP así como el BGP del siguiente salto. La etiqueta es utilizada como la etiqueta interior de un *stack* de etiquetas que permite que el paquete IP sea

enviado desde un ruteador PE hacia otro ruteador PE, y para encaminar el paquete hacia el ruteador CE apropiado basado en el valor de la etiqueta.

Con el enfoque de ruteador virtual (VR), el rutedor PE soporta ruteadores basados en software llamados ruteadores virtuales, cada uno cuida de un sitio de red particular. Ya que un ruteador VR es un ruteador regular, los clientes pueden manejarlo y configurarle las clases equivalentes de envío (FECs). Cada PE VR perteneciente a una VPN particular puede descubrir a los otros VRs mediante el uso de OA&M, de métodos basados en directorio, o de un enfoque BGP.

Por ejemplo, es posible prever a un operador GPRS quien no solo maneja el acceso inalámbrico, sino que también hace funcionar su nodo GGSN como el CE de un BGP MPLS, y usa MPLS VPNs para particionar la red en VPNs dedicadas a diferentes servicios. Un operador GPRS puede decidir crear una MPLS VPN para los servicios de paquetes de datos intradominio que es ofrecido a los suscriptores cuando no están vagando y una VPN para suscriptores que vagan (*roaming*).

5.2.5 Acuerdos del Nivel de Servicio

Las entidades involucradas en una red privada virtual, como portadores inalámbricos, proveedores ISP, corporaciones, y usuarios remotos, están unidos por ciertos acuerdos para llevar a cabo los niveles de servicio deseados así como los ingresos deseados por los servicios proporcionados. Tales acuerdos, redactados entre todas las partes interesadas y sus socios, que definen los niveles cuantificables y medibles de servicio son llamados acuerdos del nivel de servicio (SLAs). Los SLAs son especialmente importantes en el contexto de redes virtuales que funcionan sobre una infraestructura compartida o una multitud de infraestructuras compartidas –como es el caso de MVPN. En las redes de datos móviles se requiere más un SLA para soportar todos los servicios y cubrir todas las entidades que están involucradas en tales servicios.

5.2.5.1 Acuerdos del Nivel de Servicio de MVPN

Los SLAs de MVPN son especialmente complejos porque deben incluir tanto al segmento inalámbrico como al segmento alámbrico. A menudo, el funcionamiento del segmento inalámbrico no puede ser adecuadamente realizado debido a la inherente naturaleza impredecible de la interfaz de aire. Adicionalmente, en el ambiente móvil un usuario puede andar hacia una red externa al dominio de administración del proveedor de servicio móvil local, trayendo consigo el problema de garantizar el servicio de extremo-a-extremo. Por lo tanto los proveedores de servicio de MVPN deben incluir en su SLA diferentes garantías de nivel de servicio para los casos cuando el usuario está vagando y cuando el usuario se encuentre en la red local.

La siguiente es una lista de consideraciones que se deben tomar en cuenta cuando se recopila un SLA para un servicio típico de MVPN:

- Disponibilidad del túnel fijo
- Garantías de ancho de banda del túnel fijo
- Estado latente del túnel fijo
- Máxima tasa célula/paquete
- Tasa de paquetes perdidos
- Garantías para la continuidad de la sesión
- Descansos ociosos de las sesiones
- Permitir el *roaming*

5.3 Clasificación de la Tecnología VPN

Hay dos maneras de clasificar la tecnología VPN:

- *Taxonomía de la Arquitectura* trata de cómo es la arquitectura de una VPN y cómo es desplegada.

- *Taxonomía de Tunneling* trata de cómo son implementadas las técnicas de *tunneling*.

La taxonomía de la arquitectura es más utilizada en VPNs de datos alámbricas, mientras que la taxonomía de *tunneling* es aplicada usualmente en sistemas celulares.

5.3.1 Taxonomía de *Tunneling*

Todas las IP VPNs puede ser implementadas utilizando los métodos básicos de *tunneling*:

- Extremo-a-extremo, o voluntario
- Basado en red, u obligatorio
- Túneles encadenados

En base al método de *tunneling* que se utiliza, una VPN puede ser clasificada como voluntaria, obligatoria, o combinada.

5.3.1.1 VPN Voluntaria

Una IP VPN voluntaria proporciona a los usuarios remotos la capacidad de crear un túnel desde sus terminales, como teléfonos móviles o PDAs, hasta cierto punto de terminación, como un *gateway* VPN que se encuentra dentro de la red privada. Las redes privadas usualmente están protegidas por *firewalls* y requieren de mecanismos de seguridad –por ejemplo, autenticación del usuario e integridad de los datos y protección de la confidencialidad- aplicados al tráfico de acceso remoto. Consecuentemente, el equipo del usuario remoto debe soportar los protocolos convenientes para satisfacer estos requerimientos. Por ejemplo, un usuario remoto equipado con un dispositivo como un PDA podría establecer un túnel ESP de IP Sec hacia una red corporativa que utiliza distribución de claves basadas en PKI (también conocido como enfoque de claves asimétricas) o una clave secreta compartida predistribuida (conocido como enfoque de claves simétricas). Todos los datos entre tales estaciones móviles y la red privada son entonces encapsulados en el túnel IPSec de extremo-a-extremo. El túnel de extremo-a-extremo en este ejemplo existe sólo para la duración de la sesión y es rechazado cuando los usuarios remotos no requieren acceso a la red privada, o cuando el usuario debe estar desconectado en base a una serie de eventos predefinidos, tales como duración de la sesión o límites en los derechos de acceso.

Este tipo de servicio VPN es ilustrado en la figura 5.3, en la cual se utiliza acceso *dial-up* móvil sobre una red GSM como un ejemplo. En este escenario, el usuario remoto establece una conexión VPN hacia una red privada después de que un portador inalámbrico le garantiza el acceso a Internet. Note que ambos tipos de acceso (alámbrico e inalámbrico) hacia Internet permiten el *roaming* de usuarios para establecer este tipo de VPN, abriendo "voluntariamente" un canal de comunicación hacia la red privada cuando lo necesitan.

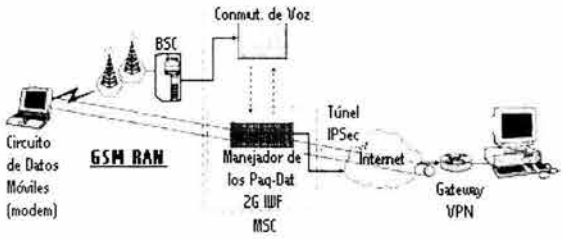


Figura 5.3 VPN voluntaria sobre una red 2G

Una VPN voluntaria acarrea un número significante de ventajas. Para los administradores IT de la red privada y a menudo para los usuarios remotos, esta es la forma más simple de establecer una VPN de acceso remoto. Los usuarios remotos simplemente necesitan acceso a Internet o cualquier otra red IP pública, y un cliente VPN en sus dispositivos móviles o fijos. Todo lo que el departamento IT de la red privada necesita es un *gateway* VPN conectado a Internet y que sea capaz de terminar un tipo de túnel particular, y establecer una serie de políticas y procedimientos de seguridad. El proveedor de servicio que ofrece servicio de acceso a Internet no puede acceder a los datos privados encriptados que están siendo transmitidos entre el usuario remoto y la red privada. Una VPN voluntaria no requiere ninguna relación preestablecida entre las corporaciones y los proveedores de servicio. Por lo tanto, no existen múltiples SLAs y acuerdos legales acerca de la confidencialidad de los datos. Sin embargo, el usuario y la corporación deben estar dispuestos a aceptar un servicio de acceso a la red que puede ser menos predecible y que ofrece una calidad inferior que el servicio proporcionado a las partes que entran en un SLA.

Las VPNs voluntarias requieren que le sean asignadas direcciones IP públicas al equipo de los usuarios remotos. Este requerimiento crea un número de potenciales inconvenientes para el servicio de VPN voluntaria. Debido al número limitado de direcciones IPv4 disponibles para los proveedores de servicio –especialmente para los operadores móviles que ofrecen a sus suscriptores conectividad permanente a Internet- dependen de esquemas de direccionamiento privado para conservar espacio de direcciones IP, combinado con varias técnicas para realizar subredes y traducción de direcciones.

Otra desventaja de una VPN voluntaria aparece en la naturaleza de un túnel de extremo-a-extremo, en el cual el contenido de los paquetes que pasan por el túnel es encapsulado y entonces no está disponible para su inspección en alguno de los nodos sobre el túnel excepto en los puntos finales del túnel. Esto hace que QoS, clase de servicio (CoS), y la mayoría de mecanismos de tráfico esbelto que requieren de la inspección de múltiples campos del paquete sea una tarea imposible.

Cuando en un ambiente inalámbrico celular se implementan MVPNs, el *tunneling* voluntario conduce a una capa extra de encapsulación sobre el último salto del enlace inalámbrico. Esto consume más recursos de radio. Además, no son convenientes complejos algoritmos de encriptación y seguridad para su implementación en pequeños dispositivos inalámbricos, los cuales tienen limitado poder de procesamiento y de batería. Adicionalmente, las condiciones de radio tan cambiantes y el ambiente inalámbrico con pérdidas no son amigables para el establecimiento y preservación de túneles de IPSec. Esto puede conducir a un largo tiempo de instalación, o en casos extremos, al completo fracaso y quizás a la necesidad de moverse hacia una región con mejor cobertura.

Por estas razones, mientras el *tunneling* voluntario proporciona una solución extremo-a-extremo limpia y segura para el acceso a redes privadas, a menudo mayor eficiencia VPN y servicios únicos pueden lograrse con la introducción de otro tipo de VPN.

5.3.1.2 VPN Obligatoria

Un proveedor de servicio puede ofrecer servicio de VPN obligatoria concatenando o encadenando múltiples túneles o proporcionando un túnel sencillo para una parte de la trayectoria de datos entre dos puntos finales. Por ejemplo, una VPN obligatoria puede estar basada en un túnel creado entre una red privada y un proveedor de servicio y no extenderlo hasta alcanzar todo el camino hacia un usuario remoto que está usando el servicio de acceso a la red. Como resultado, con el servicio de VPN obligatoria el usuario remoto no necesita tener alguna implicación en el proceso de establecimiento de la VPN y es "forzado" a usar el servicio disponible cuando requiera el acceso a la red privada.

Este tipo de VPN asume que la infraestructura de red del operador cumple con la inteligencia y funcionalidad necesarias para soportar servicios VPN basados en túneles o series de túneles

proporcionados entre la red privada y la red del proveedor de servicio. La empresa debe preestablecer un SLA detallado con el proveedor de servicio responsable del servicio VPN. El proveedor de servicio a menudo participa en el control de acceso a la red , y la corporación debe confiar al proveedor de servicio para negar el acceso a usuarios no autorizados de acuerdo a la política de acceso a la red definida por el administrador de red. Un posible escenario de una VPN obligatoria implementada en la infraestructura de CDMA2000 –basada en IP Móvil- se ilustra en la figura 5.4. En esta figura los datos de usuario son encapsulados dentro del túnel de IP Móvil entre el nodo PDSN en la red del portador y el HA de la corporación.

Figura 5.4 VPN obligatoria en CDMA2000.

La necesidad de mantener sin protección una parte de la trayectoria privada de datos, de confiar en el proveedor de servicio, y de establecer múltiples SLAs y complejos acuerdos de confidencialidad de los datos son algunos de los inconvenientes de una VPN obligatoria. En el ambiente móvil, los problemas de seguridad llegan a ser más serios, ya que el tráfico de usuario es enviado sobre canales de tráfico potencialmente inseguros. Durante el *roaming* de paquetes de datos, el tráfico sin protección hacia y desde la estación móvil debe atravesar también la red visitada (la cual puede o no tener un SLA establecido con la corporación servida por un portador inalámbrico local) antes de comenzar el túnel hacia la red del portador original. Si existen enlaces inseguros en esta red, especialmente enlaces sin encriptación, esto podría presentar serios problemas de seguridad. Por ejemplo, túneles IPSec *gateway-a-gateway* en los puntos críticos de la red podrían solucionar estos problemas.

Por el lado positivo, una VPN obligatoria utiliza mejor la interfaz de radio evitando la encapsulación sobre el aire, lo cual es especialmente ventajoso para los sistemas inalámbricos celulares, y simplificando el equipo del usuario. Cuando una VPN obligatoria es utilizada, el equipo del usuario final no tiene que soportar algún cliente VPN, o alguna capacidad de *tunneling* o de seguridad. Además, el usuario no está involucrado en la creación de la VPN y solo necesita solicitar el servicio cuando accede a la red del proveedor de servicio.

Otro beneficio de una VPN obligatoria para los proveedores de servicio está en un gran control sobre el usuario. En un modelo obligatorio, el proveedor de servicio usualmente está involucrado en la autenticación del usuario y en la asignación de direcciones IP. Las direcciones IP puede ser asignadas a los usuarios remotos desde el espacio de direcciones privadas de las redes del cliente, ahorrando así el uso de direcciones IP públicamente ruteables del lado del proveedor.

5.3.1.3 VPN de Túneles Encadenados

Una VPN de túneles encadenados consiste de una serie de túneles concatenados que se extienden hasta el equipo del usuario final. Una VPN de túneles encadenados puede venir de muchas maneras diferentes, como se muestra en la figura 5.5, en la cual se ilustran algunas opciones sobre la red GPRS.

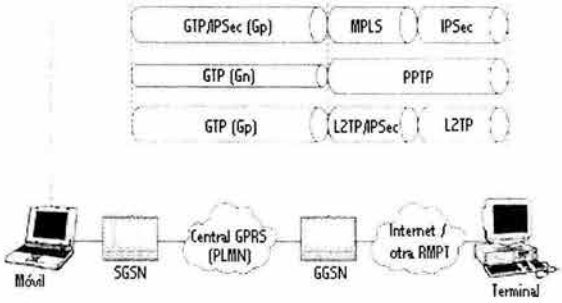


Figura 5.5 VPN de túneles encadenados (en el ambiente GPRS)

De manera similar a una VPN voluntaria, la VPN de túneles encadenados proporciona protección a los datos del usuario de extremo-a-extremo, y el usuario participa en la iniciación del túnel. Como en una VPN obligatoria, el proveedor de servicio está involucrado en el aprovisionamiento y construcción de los túneles VPN concatenados y puede fácilmente aplicar QoS en los puntos de concatenación de los túneles. Esta participación necesita acuerdos SLA y acuerdos para manejar los datos.

5.3.2 Taxonomía de la Arquitectura: VPN Sitio-a-Sitio y VPN de Acceso Remoto

En esta sección vemos la clasificación VPN desde la perspectiva de la arquitectura.
Las arquitecturas VPN pueden ser clasificadas dentro de dos tipos: VPNs sitio-a-sitio, también llamadas LAN-a-LAN o POP-a-POP, y VPNs de acceso remoto.

Una VPN sitio-a-sitio puede incluir variaciones usualmente referidas como VPN Extranet y VPN Intranet, las cuales comparten las mismas propiedades pero están diseñadas para resolver diferentes problemas. Una VPN de acceso remoto incluye métodos de acceso de *dial-up* y paquetes directos. Todos estos tipos de VPNs pueden ser implementados (al menos en teoría) sobre redes inalámbricas móviles.

5.3.2.1 VPN Sitio-a-Sitio

Una VPN sitio-a-sitio es usada para conectar sitios que están geográficamente distribuidos, cada uno con direcciones de red privadas, administrados de tal manera que no se presenten conflictos. En redes tradicionales, las oficinas remotas pueden ser interconectadas por redes de malla parcialmente llenas basadas en líneas arrendadas T1 y E1 o en circuitos de la capa de enlace, como PVCs ATM o Frame Relay dentro de la redes del proveedor de servicio. Otra opción es implementarla basada en la red de ruteo privada o basada en trayectorias de conmutación de etiquetas MPLS. Las redes de ruteo privadas requieren ruteadores capaces de segregar el tráfico de diferentes intranets, basados en múltiples tablas de ruteo.

Resultados similares pueden ser obtenidos proporcionando túneles IP VPN seguros sobre Internet o sobre redes IP del proveedor de servicio. IP VPN proporciona ventajas significativas en cuanto a costos; los costos de la comunicación son reducidos porque el cliente paga sólo por el acceso a la red IP del proveedor de servicio o por el acceso a Internet. Las oficinas remotas son conectadas vía túneles sobre una red IP pública, como Internet o una red IP comercial compartida. Junto con el acceso a la red IP pública, la implementación de VPN requiere *gateways* VPN capaces de soportar suficientes números de sesiones individuales de *tunneling* en cada sitio.

Un proveedor de servicio puede ofrecer conectividad completa hacia todos los sitios corporativos y encaminar los paquetes directamente hacia el sitio más apropiado vía túneles IP, que están conectados hacia un punto de acceso.

5.3.2.1.1 VPN Extranet

Extranet es un concepto relativamente reciente en las redes de datos. Es usualmente utilizado en situaciones cuando una corporación necesita interactuar no solo con sus oficinas remotas sino también con los sitios que pertenecen a sus clientes, proveedores, y otras entidades con las que efectúan transacciones o intercambian información. Estas entidades generalmente son referidas como *redes socio*. Para soportar tales comunicaciones, los túneles VPN pueden ser establecidos entre las redes privadas que pertenecen a las diferentes entidades. Las funciones VPN tales como control del acceso, autenticación, y servicios de seguridad pueden ser empleadas para negar o permitir el acceso a los recursos requeridos. Las amenazas contra la seguridad para la extranet – incluyendo el acceso no autorizado- son mayores que en una Intranet, así que la VPN y la extranet deben ser cuidadosamente diseñadas con múltiples políticas de control del acceso y disposiciones de seguridad únicas entre los miembros de la extranet. Por ejemplo, un proveedor puede tener acceso a la orden del cliente y quizás al sistema de inventario, mientras el cliente desea ser capaz de pedir el material ingresando al sistema de estado de la entrega del proveedor.

La capacidad de las IP VPN para proporcionar dinámicamente túneles y control del acceso dentro de minutos o tal vez segundos y a menudo sin la necesidad de notificar al proveedor de acceso es especialmente utilizada en las extranets. Esta capacidad puede manejar las desventajas de las tecnologías de red, incluyendo los procedimientos de aprovisionamiento largos y complejos. Por ejemplo, el aprovisionamiento de un PVC de Frame Relay requiere entre 5 y 20 días para estar completo. La figura 5.6 muestra a una corporación que establece relaciones dinámicas con sus proveedores y otros socios de negocios.

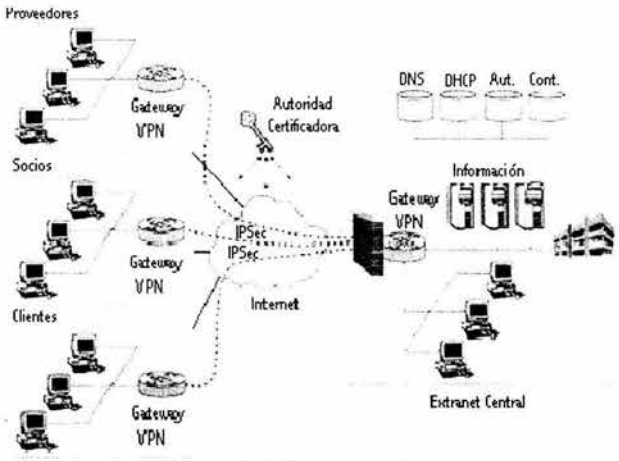


Figura 5.6 VPN extranet dinámica

El uso de IP VPNs que interconectan redes socio vale la pena cuando una cantidad importante de información necesita ser intercambiada entre las redes. Cuando la interacción entre los socios puede ser realizada vía aplicaciones basadas en Web se instalan interfaces Web protegidas con SSL o TLS. Hoy en día las interacciones comerciales están basadas en los portales del cliente o del proveedor.

5.3.2.1.2 VPN Intranet

Una corporación puede decidir instalar una VPN no solo para interconectar los sitios que le pertenecen sino también para definir redes virtuales dentro de su propio dominio de administración.

La mayoría de las veces esto no es requerido, ya que las zonas de seguridad pueden ser definidas por medios que proporcionan *firewalling* y políticas de control del acceso en el nivel de aplicación. Sin embargo, en misiones críticas, es posible que las organizaciones decidan hacer cumplir las medidas de seguridad segregando el tráfico particularmente importante y las zonas de la red vía túneles IPSec-encriptados y hacer cumplir en estas zonas de la red políticas adicionales de autenticación y control del acceso. El papel principal de las VPNs Intranet es establecer y manejar diferentes niveles de acceso interno hacia información específica. En esta capacidad, la VPN Intranet es usada para crear un ambiente similar a la segmentación física de grupos de usuarios en distintas subredes LAN unidas por puentes y ruteadores.

5.3.2.2 VPN de Acceso Remoto

El acceso remoto fue concebido originalmente como una forma de proporcionar a las terminales remotas acceso a los recursos de información y a los servicios de datos localizados en una red privada. El acceso remoto es igualmente utilizado por consumidores y trabajadores remotos u otros usuarios de negocios e institucionales. Las corporaciones y otras entidades han mantenido las instalaciones adecuadas, usualmente consistentes de arreglos de servidores de acceso remoto (RASs) y el equipo de seguridad apropiado, para mantener el nivel conveniente de disponibilidad y confiabilidad del servicio para los usuarios remotos.

5.3.2.2.1 VPN de Acceso Remoto por *Dial-Up*

El acceso remoto por *dial-up* es caro y requiere de significante soporte de los departamentos IT de las corporaciones. A menudo, los usuarios remotos se encuentran muy lejos de la sede de la corporación o de los centros de datos y requieren llamadas de larga distancia, lo cual es especialmente costoso para los llamadores internacionales o teleconmutadores quienes tienden a permanecer conectados por largo tiempo. Las corporaciones que dependían de esta tecnología frecuentemente fueron forzados a crear múltiples centros de datos regionales. El acceso de *dial-up* también requiere equipo RAS caro, el cual es complejo y está lejos de ser exento de averías.

Las VPNs de acceso remoto por *dial-up* pueden estar basadas en el método de *tunneling* voluntario o en el método de *tunneling* obligatorio. En un típico acceso *dial-up* (obligatorio), el usuario marca hacia un POP local de Internet del proveedor de servicio, estableciendo un enlace PPP. Después de que el usuario es autenticado y el enlace PPP es establecido, el proveedor de servicio establece de una manera obligatoria –esto es, de manera transparente para el usuario- un túnel hacia un *gateway* en la red privada, a la que el usuario remoto desea acceder. La red privada ejecuta la autenticación del usuario final y establece la conexión. La arquitectura resultante es ilustrada en la figura 5.7. En contraste, el acceso *dial-up* tradicional involucra una llamada del usuario hacia un banco de módems, un servidor RAS, o un concentrador localizado dentro de un centro de datos de la corporación. La tecnología de *tunneling* elegida para VPN de acceso *dial-up* es L2TP. Para ofrecer esta opción de VPN para los usuarios remotos, las corporaciones deben establecer SLAs detallados (por ejemplo, para configurar una lista de LNSs, aspectos de seguridad, y niveles de QoS), con uno o más proveedores de servicio, los cuales serán responsables de las instalaciones locales para dial-up.

Después de que el operador establece el SLA con una corporación, el tráfico de datos del usuario móvil puede ser pasado por el túnel hacia sus redes privadas utilizando la tecnología L2TP. Los operadores que han seguido el modelo ahora tienen la opción de agregar el tráfico de datos del usuario sobre su red *backbone*.

Una VPN voluntaria es esencialmente una tecnología de acceso independiente, y por lo tanto puede ser fácilmente soportada sobre cualquier conexión *dial-up*, incluyendo la inalámbrica. Todo lo que los usuarios finales tienen que hacer es establecer una conexión *dial-up* hacia el proveedor ISP de su elección y entonces vía un cliente VPN establecer un túnel en la capa de red hacia una red privada particular.

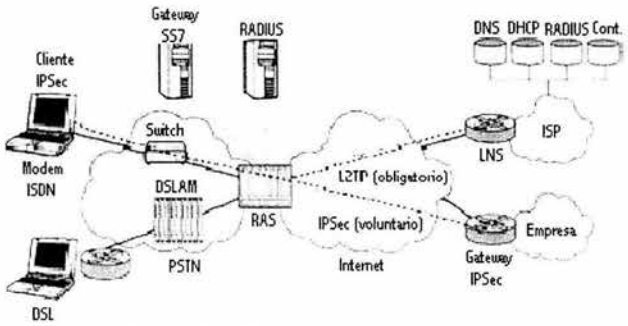


Figura 5.7 Externalización del acceso remoto a la línea terrestre

5.3.2.2.2 VPN de Acceso Directo de Paquetes

Durante la década pasada, nuevas tecnologías de acceso a Internet como la Red Digital de Servicios Integrados (ISDN), la Línea Digital de Suscriptor (DSL), y el cable estuvieron disponibles para los teleconmutadores y otros trabajadores remotos, quienes tradicionalmente dependían del acceso de *dial-up*.

Los sistemas inalámbricos de paquetes de datos por su diseño son más cercanos a los servicios alámbricos de alta velocidad como DSL y el cable módem y ofrecen a los usuarios móviles el mismo nivel de conveniencia, como capacidades automáticas permanentes, opciones de facturación granulares, y desterrando de frecuentes procedimientos de entrada al sistema.

5.4 Moviéndonos Desde lo Alámbrico Hacia lo Inalámbrico y lo Móvil

5.4.1 Inalámbrico vs Móvil

Los términos inalámbrico y móvil a menudo son utilizados incorrectamente para referirse a tipos específicos de redes. Cuando se aplican a las redes de datos, inalámbrico y móvil significan dos cosas diferentes. Las redes inalámbricas pueden ser móviles o no móviles; por ejemplo, las microondas, los servicios LMDS (*Local Multipoint Distribution Services*), las comunicaciones láser de línea de vista, o los enlaces *Bluetooth* no soportan movilidad y simplemente son usados para proporcionar acceso de red fijo. Las redes móviles pueden ser establecidas tanto en infraestructuras inalámbricas así como en infraestructuras alámbricas.

El término *inalámbrico* significa exactamente algo que puede existir sin conductores. Así, por ejemplo, red inalámbrica se refiere a una red construida sobre el aire (o en el espacio en caso de comunicaciones satelitales). El término *móvil* se refiere a algo que cambia su localización con el tiempo, así terminal móvil, por ejemplo, se refiere a una terminal cuya posición dentro de la red cambia con el tiempo. La *movilidad de datos* puede ser definida como la capacidad de una terminal para cambiar su punto de conexión así como su método de comunicación hacia la red mientras mantiene ininterrumpida la conectividad. Por lo tanto los sistemas con capacidad para soportar movilidad son llamados *sistemas móviles*, y los dispositivos del usuario final que soportan movilidad son llamados *móviles, estaciones móviles, y nodos móviles*.

5.4.2 Significado de VPN en el Ambiente Inalámbrico de Paquetes de Datos

La tecnología celular de paquetes de datos está basada en el concepto de *tunneling* dinámico en el cual túneles secuenciales son creados entre las redes exteriores visitadas por la estación móvil y su red local. La complejidad de proporcionar servicio VPN en este ambiente está en cómo combinar esta técnica con la topología de *tunneling* fija o cuasi-fija requerida en la parte alámbrica para proporcionar a los usuarios móviles acceso de red seguro y privado. Esta tarea se convierte

especialmente compleja cuando es requerido el servicio de VPN obligatoria. En este caso el operador inalámbrico debe poseer el equipo capaz de soportar no solo *tunneling* dinámico sino también conmutación dinámica de túneles entre las partes dinámica y fija de su infraestructura. La figura 5.8 proporciona un ejemplo que ilustra este requerimiento.

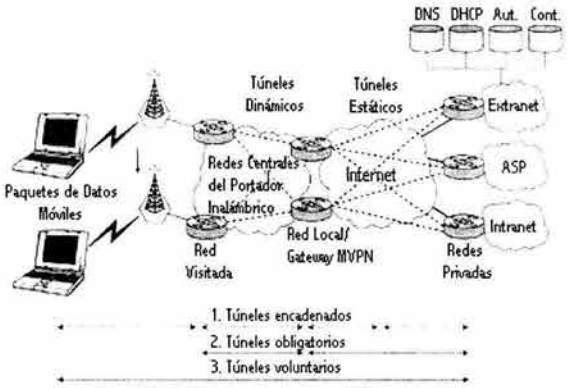


Figura 5.8 VPN en ambientes inalámbricos de paquetes de datos

En el caso de VPN voluntaria, esta tarea se simplifica, ya que el túnel de extremo-a-extremo generalmente es ajeno de las infraestructuras subyacentes mientras que las direcciones IP de los puntos extremos permanecen fijas. Este requerimiento puede ser manejado por los esquemas de movilidad de datos utilizados en GPRS o CDMA2000.

El soporte de MVPN requiere de complejos nodos de red con capacidad de conmutación de túneles y de dispositivos móviles. En los paquetes de datos inalámbricos, las estaciones móviles son habilitadas por mecanismos de la capa de red para cambiar su localización y su punto de enlace hacia la red mientras mantienen la conexión hacia su red local. A menudo la estación móvil anda en redes exteriores soportadas por otros operadores diferentes que su portador original. Mientras vaga, la estación móvil guarda su conectividad hacia su red local a través del uso de esquemas de *tunneling* que soportan movilidad como los sistemas GPRS y UMTS o el sistema IP Móvil en CDMA2000. En un ambiente semejante, es impráctico establecer algún tipo de circuito de conexión permanente del estilo dial-up entre la estación móvil y la red privada.

La mejor tecnología para el acceso de red privado en este ambiente es MVPN, ya sea obligatoria o voluntaria, basada en protocolos de *tunneling* que permitan movilidad al menos sobre algún trecho de la trayectoria de los datos.

5.4.3 MVPN Voluntaria

Una MVPN basada en *tunneling* voluntario es implementada exactamente igual que una VPN alámbrica. Es importante considerar si el proveedor de servicio usa esquemas de direccionamiento IP público o privado y qué mecanismos de traducción de dirección IP son usados (si es necesario). Otra consideración, la cual es única para el ambiente inalámbrico, es la estabilidad de la dirección IP asignada a la estación móvil. Generalmente, los protocolos de *tunneling* que soportan movilidad en los sistemas modernos de paquetes de datos ayudan a mantener constantes las direcciones IP asignadas a las estaciones móviles.

Sin embargo, en algunos sistemas inalámbricos ciertos modos de acceso proporcionan movilidad IP limitada. Por ejemplo, en CDMA2000, el modo de acceso IP Simple proporciona movilidad al usuario sólo dentro de los límites del mismo nodo PDSN/FA. Aquí los túneles de extremo-a-

extremo no pueden ser mantenidos "con vida" cuando se cambia de nodo PDSN, ya que el portador de los paquetes de datos necesita ser restablecido hacia el nuevo PDSN y la estación móvil debe adquirir una nueva dirección IP. El uso de una tecnología de VPN obligatoria con modo de acceso IP Simple no mejoraría la situación, ya que la conectividad extremo-a-extremo está perdida y un nuevo procedimiento de acceso remoto necesita ser reiniciado cada vez que es visitado un nuevo nodo PDSN. Esto puede cambiar si se utiliza un modo de acceso basado en IP Móvil. El modo de acceso IP Móvil puede ser utilizado de dos maneras diferentes. Una proporciona acceso directo a la red que el usuario final necesita acceder, mientras le proporciona movilidad. La otra forma es el acceso ininterrumpido a Internet ofrecido por el operador móvil, en el cual el usuario puede elegir voluntariamente la instalación de un túnel utilizando un cliente VPN.

5.4.4 MVPN Obligatoria

Una MVPN obligatoria está basada en los mismos principios que su contraparte alámbrica. Sin embargo, mientras la VPN obligatoria alámbrica está basada en un túnel fijo sencillo (o rara vez en una serie de túneles fijos concatenados), la MVPN implementada en un ambiente inalámbrico es diferente y está basada en una combinación de túneles dinámicos que soportan movilidad y túneles fijos en el lado alámbrico. Para llevar a cabo esta funcionalidad, referida como *conmutación dinámica de túneles*, los operadores inalámbricos deben desplegar elementos inteligentes capaces de soportar una variedad de técnicas de *tunneling*.

Los dispositivos que soportan la capacidad de conmutación de túneles deben ser habilitados para encaminar los datos del usuario por los túneles mediante la terminación de los túneles que transportan los datos de entrada y originando los túneles que encapsulan los datos de salida. Esto está basado en una serie de políticas proporcionadas en los dispositivos de red o en los dispositivos individuales por el portador inalámbrico. Alternativamente, en vez de usar túneles, puede ser desplegada una red privada de líneas físicas arrendadas o VCs ATM o Frame Relay entre el *gateway* de acceso del operador inalámbrico y la empresa. Sin embargo, la propuesta de las líneas arrendadas podría eliminar las ventajas en costos de una VPN y la facilidad de administración, lo cual es especialmente importante en el ambiente móvil.

Una MVPN obligatoria puede ser implementada de manera diferente dependiendo del patrón de movilidad permitido. Por ejemplo, es posible construir un servicio obligatorio en CDMA2000 con el modo de acceso IP Simple dado que la movilidad del usuario sería limitada. Este es a menudo el caso para los usuarios comerciales que acceden a redes corporativas desde sitios críticos como salas de aeropuertos o cuartos de hoteles. Este servicio requiere el establecimiento dinámico de un túnel L2TP entre el nodo PDSN de servicio y la red cliente. De hecho, no es posible asignar un nodo PDSN particular donde es definido un túnel obligatorio estático entre la corporación y el portador inalámbrico, ya que el suscriptor puede estar usando cualquier PDSN de la red de radio acceso donde está localizado.

El servicio obligatorio puede ser implementado en los sistemas CDMA2000 o GPRS habilitando al dispositivo que es un punto de terminación de los protocolos que soportan movilidad, como un nodo PDSN o un HA y un nodo GGSN, respectivamente, para ser el punto de origen de intercambio de tráfico con las redes cliente vía una serie de túneles fijos.

El modelo obligatorio no encaja con el modo de acceso WLAN, ya que los métodos de control del acceso requieren que el usuario adquiera primero una dirección IP y entonces autenticarse en un portal para tener acceso a la red. Esto requiere el uso de una dirección IP asignada por DHCP que pertenece no a la corporación sino a la red que el suscriptor visita. Por lo tanto, no es posible admitir al usuario en la red de la corporación. Una forma de salir de esta situación es utilizar movilidad basada en IP Móvil, ya que IP Móvil viene con su propio control del acceso y se le puede asignar a la estación móvil una dirección IP que pertenece a la red de acceso de la corporación.

CAPÍTULO 6

DIRECCIONAMIENTO, ROAMING Y SEGURIDAD EN REDES DE DATOS INALÁMBRICOS

6.1 Direccionamiento

El concepto de direccionamiento en una arquitectura de comunicaciones es complejo y cubre un número de cuestiones, que incluyen las siguientes:

- Nivel de direccionamiento
- Alcance del direccionamiento
- Identificadores de la conexión
- Modo de direccionamiento

Estos conceptos se ilustran en la figura 6.1, la cual muestra una configuración que usa la arquitectura TCP/IP. Los conceptos son esencialmente los mismos para la arquitectura OSI y cualquier otra arquitectura de comunicaciones.

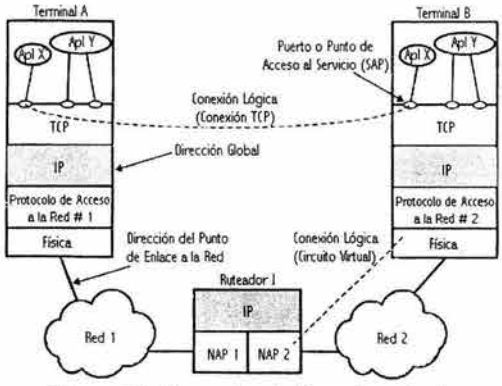


Figura 6.1 Conceptos de Direccionamiento

El **nivel de direccionamiento** se refiere al nivel en la arquitectura de comunicaciones en el cual una entidad es nombrada. Típicamente, una dirección única es asociada con cada sistema final (por ejemplo, una estación de trabajo o un servidor) y cada sistema intermedio (por ejemplo, un ruteador). Tal dirección es, en general, una dirección a nivel de red. En el caso de la arquitectura TCP/IP, ésta es referida como una dirección IP, o simplemente una dirección de internet. En el caso de la arquitectura OSI, es referida como un punto de acceso al servicio de red (NSAP). La dirección a nivel de red es usada para encaminar una Unidad de Paquetes de Datos (PDU) a través de una red o redes hacia un sistema indicado por una dirección a nivel de red dentro de la PDU.

Una vez que los datos llegan al sistema destino, deben ser encaminados hacia algún proceso o alguna aplicación en el sistema. Típicamente, un sistema soporta múltiples aplicaciones y una aplicación puede soportar múltiples usuarios. A cada aplicación y, quizá, a cada usuario de una aplicación, le es asignado un identificador único, referido como un puerto en la arquitectura TCP/IP y como un punto de acceso al servicio (SAP) en la arquitectura OSI. Por ejemplo, un sistema terminal podría soportar una aplicación de correo electrónico y una aplicación de transferencia de archivos. Como mínimo cada aplicación tendría un número de puerto o SAP que es único dentro

del sistema. Además, la aplicación de transferencia de archivos podría soportar múltiples transferencias simultáneas, en la cual cada transferencia es asignada dinámicamente a un número de puerto único o SAP.

La figura 6.1 ilustra dos niveles de direccionamiento dentro de un sistema. Este es típicamente el caso de la arquitectura TCP/IP. Sin embargo, puede existir direccionamiento en cada nivel de una arquitectura. Por ejemplo, un SAP único puede ser asignado en cada nivel de la arquitectura OSI.

Otra cuestión en relación a la dirección de un sistema final o un sistema intermedio es el **alcance del direccionamiento**. La dirección de internet o la dirección NSAP es una dirección global. Las características de una dirección global son las siguientes:

- No ambigüedad global: Una dirección global identifica a un sistema único. Un sistema puede tener más de una dirección global.
- Aplicabilidad global: Es posible con alguna dirección global identificar alguna otra dirección global, en algún sistema.

Debido a que la dirección global es única y globalmente aplicable, permite encaminar datos desde algún sistema enlazado a alguna red hacia otro sistema enlazado a otra red.

La figura 6.1 ilustra que otro nivel de direccionamiento puede ser requerido. Cada red debe mantener una dirección única para cada interfaz del dispositivo. Por ejemplo, una dirección MAC sobre una red IEEE 802 y una dirección de terminal X.25. Esta dirección permite a la red encaminar las unidades de datos (tramas MAC, paquetes X.25) a través de la red y entregarlas al sistema destino enlazado. Podemos referirnos a tal dirección como una dirección de conexión a la red.

El alcance del direccionamiento es relevante sólo para las direcciones a nivel de red. Un puerto o SAP arriba del nivel de red es único dentro de un sistema dado pero no es necesariamente globalmente único. Por ejemplo, en la figura 6.1, puede ser un puerto 1 en el sistema A y un puerto 1 en el sistema B. La designación completa de estos dos puertos podría ser expresada como A.1 y B.1, las cuales son designaciones únicas.

El concepto de **identificadores de la conexión** entra en juego cuando se habla de transferencia de datos orientados a conexión (por ejemplo, circuito virtual). Para la transferencia de datos sin conexión, un nombre global es usado con cada transmisión de datos. Para la transferencia de datos orientados a conexión, es deseable alguna veces sólo un nombre de conexión durante la fase de transferencia de los datos. El escenario es este: la entidad 1 en el sistema A requiere una conexión hacia la entidad 2 en el sistema B, quizá usando la dirección global B.2. Cuando B.2 acepta la conexión, un identificador de la conexión (usualmente un número) es proporcionado y es utilizado por ambas entidades para futuras transmisiones. El uso de un identificador de conexión tiene algunas ventajas:

- Encabezado reducido: Los identificadores de conexión son generalmente más cortos que los identificadores globales. Por ejemplo, en el protocolo X.25 usado sobre redes de conmutación de paquetes, la conexión solicita los paquetes que contienen los campos de las direcciones origen y destino.
- Ruteo: En la instalación de una conexión, puede ser definida una ruta fija. El identificador de la conexión sirve para identificar la ruta hacia sistemas intermedios, como nodos de conmutación de paquetes.
- Multiplexaje: Una entidad puede desear gozar más de una conexión simultáneamente. Entonces, las PDUs deben ser identificados por el identificador de la conexión.
- Uso de información de estado: Una vez que la conexión ha sido establecida, los sistemas finales pueden mantener información del estado en relación a la conexión. Esto permite funciones como control de flujo y control de errores.

La figura 6.1 muestra algunos ejemplos de conexiones. La conexión lógica entre el ruteador J y la terminal B es en el nivel de red. Por ejemplo, si la red 2 es una red de conmutación de paquetes que usa X.25, entonces esta conexión lógica sería un circuito virtual. En un nivel más alto, muchos protocolos del nivel de transporte, como TCP, soportan conexiones lógicas entre los usuarios del servicio de transporte. TCP puede mantener una conexión entre dos puertos en sistemas diferentes.

Otro concepto de direccionamiento es el **modo de direccionamiento**. Más comúnmente, una dirección se refiere a un sistema o a un puerto; en este caso es referida como una dirección *unicast* o individual. También es posible para una dirección referirse a más de una entidad o puerto. Tal dirección identifica a múltiples recipientes simultáneos de datos. Una dirección para múltiples recipientes puede ser *broadcast*, destinada a todas las entidades dentro de un dominio, o *multicast*, destinada a una serie específica de entidades. La tabla 6.1 ilustra las posibilidades.

Tabla 6.1: Modos de direccionamiento

Destino	Dirección de la Red	Dirección del Sistema	Dirección del Puerto/SAP
Unicast	Individual	Individual	Individual
Multicast	Individual	Individual	Grupo
	Individual	Todas	Grupo
	Todas	Todas	Grupo
Broadcast	Individual	Individual	Todas
	Individual	Todas	Todas
	Todas	Todas	Todas

6.2 Seguridad

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad. La salida de estas ondas de radio fuera del área de cobertura de la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible de la red y de la seguridad informática de la misma. La seguridad es muy importante para la adecuada operación de las VPNs. Un buen sistema de seguridad debe proporcionar servicios que ayuden a simplificar la tarea de manejar la seguridad de la información. Estos servicios incluyen *autenticación, integridad de los datos, confidencialidad, control del acceso, y no repudiación.*

6.2.1 Autenticación

La autenticación verifica que un usuario es exactamente quien afirma ser. Proporciona las bases para el control del acceso en las redes y otros sistemas computacionales. Diferentes esquemas de autenticación son usados por los usuarios en sitio y los usuarios remotos. El esquema de autenticación más común para los usuarios en sitio es la combinación de ID del usuario y contraseña. Para los usuarios de acceso remoto, los esquemas de autenticación más comunes incluyen dirección restringida, ID de la llamada entrante, volver a llamar (callback), PAP, CHAP, y Servicio Remoto de Autenticación del Usuario Dial-In (RADIUS).

6.2.1.1 Dirección Restringida

En este servicio, una lista de direcciones de redes remotas es almacenada en una base de datos localizada en la red corporativa. Cuando un usuario marca a la red, la dirección de red que origina la llamada es verificada en la lista. Si la dirección aparece en la lista, la llamada es permitida; de otra manera, es rechazada.

Este esquema previene de usuarios no autorizados que acceden a los recursos, pero este esquema tiene algunas desventajas. Valida al equipo más que al usuario, lo que significa que cualquier equipo robado puede ser usado para acceder a la red. Además, asume que las direcciones de red son asignadas estáticamente. Por lo tanto, este esquema no puede ser usado en ambientes donde las direcciones de red son asignadas dinámicamente por un servidor DHCP debido a que la dirección IP de un equipo puede cambiar cada vez que solicite una dirección IP.

6.2.1.2 ID de la Llamada Entrante

En este servicio, cada usuario que desea marcar remotamente hacia la red corporativa es requerido para que proporcione su número telefónico, el cual el administrador de la red almacena en una base de datos localizada en la red corporativa. El *switch* de la compañía debe ser capaz de presentar el ID de la línea que llama. Entonces, cuando una llamada llega al servidor de acceso remoto, el *switch* presenta el ID de la línea que llama al servidor de acceso remoto, el cual valida el número de la lista de números permitidos en la base de datos. Si el número aparece en la lista, la llamada es aceptada; de otra manera es rechazada.

Un inconveniente de este esquema es que requiere que el *switch* presente el ID de la llamada. Además, no soporta usuarios móviles. Finalmente, no hay garantía de que la persona que llama no sea un intruso. Al igual que el servicio de dirección restringida, este esquema valida al equipo más que al usuario.

6.2.1.3 Volver a Llamar (Call-back)

En este servicio, cada usuario remoto es requerido para que proporcione su número telefónico, el cual está almacenado en una base de datos localizada en la red corporativa. Cuando un usuario marca a la red, primero es autenticado con su contraseña. El servidor de acceso remoto entonces termina automáticamente la llamada y llama de regreso al usuario.

Este servicio trabaja bien para los usuarios remotos, quienes siempre acceden con el mismo teléfono. Sin embargo, no trabaja en el caso de un usuario móvil que frecuentemente cambia el número telefónico. Por otra parte, los usuarios que tienen una llamada para enviar pueden redirigir fácilmente la llamada desde una localización autorizada hasta cualquier localización deseada.

6.2.1.4 Protocolo de Autenticación de la Contraseña (PAP)

PAP es un protocolo de autenticación que está asociado con PPP. Cuando el servidor de acceso remoto recibe una llamada del usuario, el servidor alista al usuario para su ID y su contraseña secreta. Entonces el servidor de acceso remoto transmite el ID del usuario y la contraseña a un servidor central de autenticación, el cual es una base de datos de contraseñas. La llamada es aceptada (esto es, el usuario es autenticado) si la contraseña proporcionada por el usuario coincide con la contraseña almacenada en la base de datos.

La contraseña almacenada en la base de datos de autenticación está encriptada, pero el ID y la contraseña son enviados al servidor de autenticación sin ser encriptados.

6.2.1.5 CHAP (*Challenge Handshake Authentication Protocol*)

El protocolo CHAP es otro protocolo asociado con PPP. Éste utiliza un protocolo sofisticado demanda-saludo para validar periódicamente a los usuarios. La autenticación inicial de CHAP es ejecutada durante el intento de *log-in*, y el administrador de la red puede especificar la tasa de autenticaciones subsecuentes. El uso de autenticaciones repetidas está pensado para limitar el tiempo que la red está expuesta a ataques. CHAP requiere que el usuario encripte la respuesta a un mensaje de demanda.

Cuando un usuario marca a la red, un servidor CHAP envía una clave aleatoria de encriptación (demanda) al modem del usuario o al puente/ruteador para encriptar la contraseña del usuario. La contraseña encriptada es enviada al servidor CHAP, el cual la desencripta para autenticar al usuario. El servidor CHAP envía periódicamente una clave aleatoria al modem del usuario (o al puente/ruteador), el cual retorna una contraseña encriptada. De esta forma, una encriptación diferente de la contraseña es regresada para cada mensaje de demanda.

CHAP es más seguro que PAP porque las transmisiones CHAP son encriptadas. Sin embargo, la base de datos de contraseñas de CHAP está en texto plano, haciéndola vulnerable a ataques.

6.2.1.6 RADIUS

El Servicio Remoto de Autenticación del Usuario *Dial-In* (RADIUS) es un esquema distribuido de seguridad desarrollado por *Livingston Enterprises* (ahora *Lucent Technologies*). Es un protocolo cliente/servidor que almacena los perfiles de los usuarios en el servidor central RADIUS localizado en el sitio corporativo. El cliente RADIUS reside en un ruteador o servidor de acceso remoto que está localizado en la misma red del servidor RADIUS. RADIUS ejecuta tres funciones básicas: autenticación, autorización, y contabilidad. Como se definió anteriormente, la autenticación determina que el usuario sea quien dice ser. Después de que un usuario ha sido autenticado, la autorización determina qué puede hacer el usuario y qué recursos de la red le están disponibles. La contabilidad es usada para registrar la actividad del usuario en la red.

Cuando un cliente RADIUS recibe una llamada de un usuario remoto, alista al usuario para su ID y su contraseña como parte de la negociación PPP. Después de recibir está información, el cliente RADIUS intenta autenticar al usuario comparando el ID y la contraseña con las entradas en su tabla local de usuarios. Si no encuentra el nombre del usuario, el cliente RADIUS pasa el ID del usuario y su contraseña al servidor RADIUS. Si el servidor RADIUS es capaz de autenticar al usuario, regresa una respuesta de aceptación al cliente RADIUS, junto con información del perfil tal como la dirección IP, la cual permite al cliente RADIUS instalar la conexión. Con esta información, el cliente RADIUS puede completar las negociaciones PPP con el usuario. Si el servidor RADIUS no es capaz de autenticar al usuario, regresa un mensaje de rechazo con las razones de tal determinación. Con esta información, el cliente RADIUS puede terminar la conexión. La figura 6.2 ilustra como trabaja RADIUS.

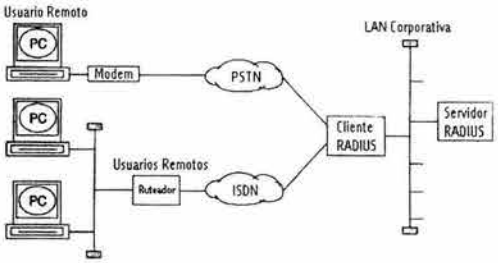


Figura 6.2 Como funciona RADIUS

El proceso de autenticación ocurre solo una vez, durante el proceso de *log-in*. Después de que la autenticación RADIUS ha sido completada, el usuario puede comunicarse con la red, que limita su acceso a los recursos que le están permitidos. Una ventaja de RADIUS es que permite la seguridad de toda la información por estar centralizada en una base de datos.

6.2.1.7 Autenticación de Dos Factores

Los servicios de autenticación presentados en los párrafos anteriores son referidos como servicios de autenticación de un solo factor. Ellos usualmente dependen de una contraseña estática o

reusable para el control del acceso. Una contraseña reusable es utilizada muchas veces para acceder a la red. Sin embargo, las contraseñas reusables son vulnerables a ataques.

Autenticación basada en contraseñas está basada en algo familiar al usuario, como una palabra, un número o un código secreto (esto es, una combinación de palabras y números).

Autenticación basada en señales está basada en algo que el usuario posee, lo cual es una señal infalsificable. Ésta puede ser una tarjeta inteligente con procesador y memoria. La autenticación basada en señales proporciona un nivel de seguridad más alto que la autenticación basada en contraseñas debido a que un *hacker* solo puede tener acceso a la red robando la señal al usuario o fabricando una señal falsa.

Autenticación Biométrica está basada en una característica personal medible del usuario (o una biométrica), tal como las huellas dactilares, la firma, la retina, o la voz. Cuando un usuario desea ser autenticado, una medición física del patrón biométrico apropiado es realizada y el resultado es comparado con el patrón del usuario, el cual está almacenado en el servidor de autenticación. Desafortunadamente, aunque la autenticación biométrica proporciona un alto nivel de seguridad, los dispositivos de autenticación biométrica son más caros que los sistemas de autenticación ya mencionados.

Un servicio de autenticación que utiliza más de un factor es llamado una *autenticación fuerte*. Un caso especial de autenticación fuerte es la autenticación de dos factores, la cual combina las características de la autenticación basada en contraseñas y la autenticación basada en señales. Así, la autenticación basada en dos factores requiere dos elementos independientes: algo que el usuario conozca (contraseña), y algo que el usuario posee (señal). Un sistema de autenticación de dos factores crea una contraseña única una vez en la forma de un número de identificación personal (PIN) para cada usuario. Además, al usuario le es entregada una tarjeta inteligente (o señal). Cuando un usuario desea ser autenticado, debe proporcionar su PIN y su señal. La autenticación de dos factores asegura la no repudiación (esto es, una acción del usuario no puede ser negada).

6.2.1.8 Autenticación Simple por Firma

En muchas redes corporativas, un usuario necesita una contraseña para ingresar a cada aplicación de la red. Por ejemplo, una contraseña para el servidor de correo, otra para el servidor *Novell*, y así sucesivamente. Sin embargo, múltiples contraseñas pueden comprometer la seguridad.

La autenticación simple por firma permite a un usuario ser autenticado una vez para todas las aplicaciones de la red (o recursos) a los que está autorizado acceder. Una vez que el usuario ha sido autenticado, puede acceder a los recursos sin ser reautenticado en cada recurso. Cuando el usuario desea acceder a un recurso que requiere autenticación, el sistema recupera la contraseña del usuario y la pasa a un nuevo sistema, el cual usa la contraseña para autenticar al usuario de una manera transparente.

La autenticación simple por firma simplifica los procedimientos de ingreso reduciendo el tiempo que toma a un usuario acceder a las aplicaciones. Además, elimina la necesidad de memorizar múltiples contraseñas y mejora la seguridad de la red haciendo transparente el ingreso. Finalmente, la autenticación simple por firma simplifica la administración de la seguridad ya que requiere mínima administración y reduce los costos de soporte a través de procesos automatizados.

6.2.2 Integridad de los Datos

Esta propiedad asegura que los datos sean transmitidos desde el origen hasta el destino sin alteración. Si los datos han sido alterados en su ruta hacia el destino, la alteración será detectada y los datos serán rechazados. La *integridad orientada a conexión* asegura que el orden de los datos

transmitidos sea preservado. Una firma digital es generalmente utilizada para asegurar la integridad de los datos.

6.2.3 Confidencialidad

Esta propiedad asegura que los datos se mantengan privados y, por lo tanto, vistos y accedidos por el recipiente destinado. Los recipientes no destinados no pueden acceder al mensaje. Así, la confidencialidad es igual a la privacidad. La encriptación es utilizada para asegurar la confidencialidad cuando los datos son transmitidos sobre la red.

6.2.4 Control del Acceso

El control del acceso establece los derechos de acceso de un usuario autenticado a los recursos y dispositivos de la red. Los derechos de acceso usualmente son definidos a través de un sistema de políticas, el cual identifica los recursos que están accesibles para cada usuario. Algunas veces el término autorización es usado para el control del acceso, particularmente en referencia a RADIUS.

6.2.5 No Repudiación

La no repudiación asegura que las partes no puedan negar sus acciones electrónicas. Permite al recipiente de un mensaje probar que éste viene de un mensajero específico. La autenticación de dos factores y la firma digital pueden ser utilizados para asegurar la no repudiación.

Con respecto a la comunicación de datos, existen tres formas diferentes de no repudiación:

- No repudiación del servicio de entrega
- No repudiación del servicio de origen
- No repudiación del servicio de sumisión

La no repudiación del servicio de entrega proporciona al mensajero la prueba de que un mensaje fue entregado al receptor deseado.

La no repudiación del servicio de origen proporciona al recipiente la prueba del origen del mensaje y su contenido.

La no repudiación del servicio de sumisión prueba que un mensajero particular envie un mensaje a través del servicio de transporte.

6.2.6 *Firewalls*

Un *firewall* es típicamente definido como un sistema o un grupo de sistemas que hace cumplir y actúa como una política de control entre dos redes. También puede ser definido como un mecanismo usado para proteger una red custodiada de una red no custodiada. Todo el tráfico desde adentro hacia fuera y viceversa debe pasar por el *firewall*. Solo al tráfico autorizado, definido por la política de seguridad local, se le permite pasar. El sistema mismo es altamente resistente a la penetración. Un *firewall* selectivamente permite o rechaza el tráfico de la red (figura 6.3).

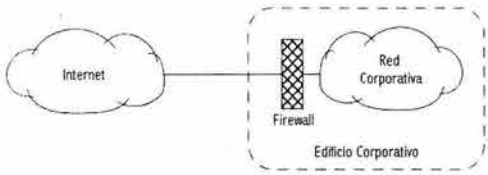


Figura 6.3 Acceso desde Internet controlado por un *firewall*

Los *firewalls* pueden ser clasificados dentro de tres categorías: *filtros de paquetes, servidores proxy (los cuales incluyen gateways de aplicación y gateways de nivel de circuito), y filtros de paquetes de estado*:

- Los ruteadores pueden ser configurados para definir qué protocolos en la capa de aplicación, en la capa de red, o en la capa de transporte pueden entrar y salir del ruteador –de manera que el ruteador está básicamente actuando como un filtro de paquetes.

- Un servicio *proxy* es una aplicación que redirecciona las peticiones del usuario hacia los servicios actuales en base a la política de seguridad de la organización. Toda la comunicación entre un usuario y el servidor actual ocurre a través del servidor *proxy*. Así, un servidor *proxy* actúa como un corredor de comunicaciones entre los clientes y los servidores de aplicación actuales. Debido a que actúa como un punto de inspección donde las peticiones son validadas contra aplicaciones específicas, un servidor *proxy* usualmente está en procesamiento intensivo y puede llegar a convertirse en un cuello de botella bajo condiciones de tráfico pesado.

  Los servidores *proxy* pueden operar en la capa de aplicación o en la capa de transporte.

  Gateways de aplicación: Un *gateway* de aplicación es un servidor *proxy* que proporciona control del acceso en la capa de aplicación. Actúa como un *gateway* entre la red protegida y la red no custodiada. Debido a que opera en la capa de aplicación, es capaz de examinar el tráfico en detalle y, por lo tanto, es considerado el tipo de *firewall* más seguro. Puede prevenir ciertas aplicaciones, como FTP, y también puede cortar todas las actividades de la red de acuerdo a las aplicaciones para propósitos de contabilidad y seguridad. Los *gateways* de aplicación pueden también ocultar información. Ya que todas las peticiones para los servicios en la red protegida pasan por el *gateway* de aplicación, éste puede proporcionar la funcionalidad de traducción de la dirección de red y ocultar las direcciones IP en la red protegida de Internet remplazando la dirección IP de cada paquete saliente (esto es, los paquetes que van de la red protegida hacia Internet) con su propia dirección IP. La traducción de dirección también permite que las direcciones IP no registradas sean utilizadas libremente en la red protegida ya que el *gateway* las mapeará hacia su propia dirección IP cuando los usuarios intenten comunicarse con el mundo exterior.

  Gateways de nivel de circuito: Un *gateway* de nivel de circuito es un servidor *proxy* que valida las sesiones TCP y UDP antes de permitir una conexión o un circuito hacia el *firewall*. Está activamente involucrado en el establecimiento de la conexión y no permite que los paquetes sean enviados hasta que las reglas de control del acceso han sido cumplidas. Un *gateway* de nivel de circuito no es tan seguro como un *gateway* de aplicación debido a que valida las sesiones TCP y UDP sin el completo conocimiento de las aplicaciones que usan estos servicios de transporte. Por otra parte, una vez que una sesión ha sido establecida, cualquier aplicación puede correr a través de esa conexión. Este funcionamiento expone a la red protegida a ataques de intrusos. A diferencia de un *gateway* de nivel de circuito, un *gateway* de aplicación puede diferenciar las aplicaciones que necesitan ser bloqueadas de aquellas que pueden ser permitidas.

- Filtros de Paquetes de Estado: Aunque el *gateway* de aplicación proporciona la mejor seguridad, su requerimiento de intenso procesamiento disminuye el funcionamiento de la red. Un *gateway* de filtro de paquetes de estado intenta proporcionar la misma seguridad sin comprometer el funcionamiento de la red. A diferencia de un *gateway* de aplicación, examina los datos que pasan en la capa de red pero no los procesa. El *firewall* mantiene la información del estado para cada sesión, donde el estado de la sesión incluye una combinación de la fase de comunicación y el estado de la aplicación del punto final. Cuando un *gateway* de filtro de paquetes de estado recibe un paquete de datos, comprueba el paquete contra el estado conocido de la sesión. Si el paquete difiere del estado de la sesión esperado, el *gateway* bloquea el resto de la sesión.

6.2.7 Encriptación

La mejor forma de proteger los datos es utilizando la encriptación –esto es, codificar los datos de tal manera de transformarlos en un documento ilegible para todos excepto para aquellos que están autorizados para tener acceso a los datos. El contenido de un documento original es referido como texto plano. Cuando la encriptación es aplicada al documento, el texto plano es invertido, a través del uso de un algoritmo y una variable o una clave. La clave es una cadena de números seleccionada aleatoriamente. Generalmente, a mayor longitud de la cadena se tiene mayor seguridad.

Existen dos categorías principales de los algoritmos de encriptación: simétricos y asimétricos (también llamados encriptación de clave pública).

6.2.7.1 Encriptación Simétrica
En la encriptación simétrica, el emisor y el receptor utilizan la misma clave. Hay dos enfoques para codificar los datos usando la encriptación simétrica: cifrado en bloques y cifrado en cadena. Con el enfoque de cifrado en bloques, el algoritmo codifica el texto en bloques de bits fijos, usando una clave cuya longitud también es fija. Con el enfoque de cifrado en cadena, el algoritmo codifica la cadena de datos secuencialmente, sin segmentarla en bloques. Ambas técnicas requieren un método seguro para intercambiar las claves entre los participantes.

Los algoritmos de encriptación simétrica incluyen a los siguientes:

- ***Data Encryption Standard* (DES):** DES fue desarrollado en los 70's y es muy popular en la industria bancaria. Es un cifrado en bloques que codifica el texto dentro de bloques de bits fijos, utilizando una clave de 56 bits. DES esta siendo remplazado por AES (*Advanced Encryption Standard*) que especifica tres longitudes para la clave –128 bits, 192 bits, y 256 bits.

- ***Triple DES* (3DES):** 3DES es una encriptación de 168 bits que usa tres claves de 56 bits. 3DES aplica el algoritmo DES al bloque de texto plano tres veces.

- ***Rivest Cipher 4* (RC4):** RC4 es una técnica de cifrado en cadena; un cifrado en cadena añade la salida de un generador de números pseudoaleatorios bit por bit a los bits secuenciales del texto plano digitalizado.

- ***Blowfish*:** *Blowfish* es una codificación en bloques de 64 bits que tiene claves de 32 a 448 bits de longitud.

- ***International Data Encryption Algorithm* (IDEA):** IDEA, desarrollado por *ETH Zurich*, es usado en PGP (*Pretty Good Privacy*) y en *Speak Freely*, un programa que permite encriptar la voz digitalizada para enviarla sobre Internet.

6.2.7.2 Encriptación Asimétrica
La encriptación de la clave requiere un método seguro para intercambiar las claves entre los participantes. La solución a la distribución de las claves llegó en 1975, con el esquema de criptogrfía de clave pública de *Diffie y Hellman*. Este permite el uso de dos claves, una de las cuales puede ser publicada abiertamente. Este esquema se conoce como *criptografía de clave pública*.

La criptografía asimétrica puede ser usada para autenticación. Después de encriptar una firma usando una clave privada, alguien con acceso a la clave pública puede verificar que la firma pertenece al dueño de la clave privada. Como se muestra en la figura 6.4, los siguientes son los pasos que tienen lugar en la encriptación de clave pública:

1. El usuario A "mezcla" el texto plano.
2. El usuario A encripta el valor de la "mezcla" con una clave privada.
3. El usuario A encripta el texto plano con la clave pública del usuario B.
4. El usuario B decodifica el texto cifrado con la clave privada.
5. El usuario B decodifica el valor de la "mezcla", usando la clave pública del usuario A, confirmando así la autenticidad del emisor.
6. El usuario B compara el valor de la "mezla" desencriptado con el valor de la "mezcla" calculado localmente sobre el texto plano encriptado, confirmando de esa manera la integridad del mensaje.

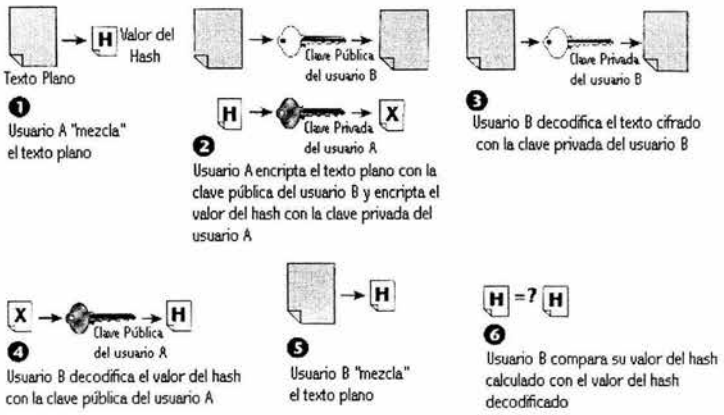


Figura 6.4 Encriptación y autenticación

La administración de la clave pública involucra el intercambio de secretos que ambos extremos usan para producir claves aleatorias de la sesión para autenticarse uno al otro. Este es un método de encriptación de datos que usa dos claves separadas. El emisor usa una clave pública que generalmente es proporcionada como parte de un certificado emitido por una Autoridad Certificadora para invertir los datos para la transmisión. El receptor entonces usa una clave privada única para desencriptar los datos en el recipiente. La Autoridad Certificadora es una entidad que emite certificados que contienen datos acerca de individuos o empresas que han sido verificados para ser auténticos. En esencia, la Autoridad Certificadora responde por la autenticidad de las partes de tal manera que sus comunicaciones sean seguras.

La autenticación del mensaje verifica la integridad de un mensaje electrónico y también verifica que un mensaje electrónico fue enviado por una entidad particular. El mensaje es encriptado antes de que salga, una función criptográfica de "mezcla" (*hash*) –la cual es una versión elaborada de una comprobación de suma (*checksum*)- es ejecutada sobre éste. La función de "mezcla" comprime los bits del mensaje de texto plano dentro de una síntesis de tamaño fijo, o valor de la "mezcla", de 128 o más bits.

Los mecanismos de autenticación del mensaje incluyen *Message Digest-5* (MD5) y *Secure Hash Algorothm-1* (SHA-1). MD5 mezcla un archivo de longitud arbitraria dentro de un valor de 128 bits. SHA-1 mezcla un archivo de longitud arbitraria dentro de un valor de 160 bits.

La administración de la clave pública proporciona un método seguro para obtener la clave pública de una persona o una organización, con la suficiente seguridad de que la clave es correcta. Existen tres algoritmos de clave pública: RSA (llamado así por sus creadores, *Rivest, Shamir, y Adelman*), *Diffie-Hellman*, y PGP.

Sin una infraestructura universal de clave pública, no podemos confiar y adquirir fácilmente los certificados que contienen las claves públicas de las personas u organizaciones con las que queremos comunicarnos. Existen estándares al respecto, entre los que se incluyen *Public Key Infrastructure* (PKI), *IETF Public Key Infrastructure X.509* (PKIK), *Simple PKI* (SPKI), y *Public-Key Cryptography Standards* (PKCS).

PKI es un sistema que proporciona protocolos y servicios para el manejo de claves públicas en una Intranet o en Internet –involucra la distribución de las claves de una forma segura. PKI asegura aplicaciones de comercio electrónico tales como correo electrónico privado, órdenes de compra, y automatización del flujo de trabajo. Utiliza certificados y firmas digitales para autenticar y encriptar los mensajes y una Autoridad Certificadora para manejar los procesos de verificación. Permite la creación de objetos de identificación legalmente verificables, y también dicta una técnica de encriptación para proteger los datos transmitidos sobre Internet. Los navegadores Web como *Internet Explorer de Microsoft y Navigator de Netscape* incluyen un soporte rudimentario para PKI proporcionando una interfaz dentro de una provisión de certificado de la computadora, y los navegadores a menudo incluyen los certificados de algunas Autoridades Certificadoras de nivel superior.

IKE es el protocolo de intercambio de claves usado por IPSec, en computadoras que necesitan negociar asociaciones de seguridad con otras computadoras. Una asociación de seguridad es una conexión entre dos sistemas, establecida para el propósito de asegurar los paquetes transmitidos a través de la conexión. Soporta claves precompartidas, lo cual es una forma simplificada de intercambiar claves. No requiere certificados digitales. Cada nodo debe estar enlazado a cualquier otro nodo por una clave única, y el número de claves necesarias puede crecer indefinidamente; por ejemplo, 2 dispositivos necesitan 1 clave, y 8 dispositivos necesitan 28 claves. Las nuevas versiones de IKE generan claves a través de una Autoridad Certificadora.

Uno de los más grandes obstáculos para las compañías de comercio electrónico es la confirmación de la identidad de las partes involucradas. Para asegurar la identidad se requiere un ID encriptado del objeto que puede ser verificado por una tercera parte y aceptado por un navegador del usuario. Los IDs personales digitales contenidos en los navegadores de los usuarios realizan esto. Históricamente, estos certificados de los clientes han sido usados para control del acceso a los recursos en una red de negocios, pero también pueden contener otra información del usuario, que incluye nivel de descuento de la identidad o el tipo de cliente. Las terceras partes (esto es, las Autoridades Certificadoras) garantizan este tipo de certificados. El navegador del usuario lee el certificado del servidor, y si lo acepta, el navegador genera una sesión de clave simétrica, usando la clave pública del servidor. El servidor entonces desencripta la clave simétrica, la cual es usada para encriptar el resto de la transacción. La transacción es entonces firmada, utilizando el ID digital del usuario, que verifica la identidad del usuario.

6.2.8 Certificados Digitales

Los certificados digitales, basados en la especificación X.509 de ANSI, se han convertido en el estándar de facto para Internet. Los certificados digitales son un método para registrar la identidad del usuario con una tercera parte, una Autoridad Certificadora (como *Entrust, UserTrust, o VeriSign*). Un certificado digital liga a un usuario a una firma electrónica que puede ser acreditada como una firma escrita e incluye información de autenticación, de los derechos de acceso, y de verificación. Las Autoridades Certificadoras preparan, emiten, y manejan los certificados digitales, y mantienen una base de datos directorio de la información de los usuarios, verificando su precisión y perfección, y emiten los certificados electrónicos en base a esa información. Una Autoridad Certificadora firma un certificado, verificando la integridad de la información que contiene.

Los certificados de los servidores aseguran a los compradores de Internet la identidad del sitio Web del vendedor. Estos certificados contienen detalles acerca del sitio Web, como el nombre del dominio del sitio y quién es el dueño. Las terceras partes, garantizan entonces esta información.

Los sitios con certificados de los servidores nombran a la Autoridad Certificadora, y los navegadores de Internet aceptan sus certificados para transacciones seguras.

6.2.9 Mecanismos de Seguridad en las Redes Inalámbricas (Wi-Fi)

Los mecanismos utilizados habitualmente son:

6.2.9.1 WEP (*Wired Equivalent Protocol*)

El protocolo WEP aparece para simular la seguridad que existe en los entornos con cable fijo, que carecen de cifrado en las dos primeras capas OSI, y no supone en ningún momento una solución de seguridad de extremo a extremo. WEP es un procedimiento de seguridad que consiste en el cifrado de los datos transferidos entre dos dispositivos inalámbricos, ya sean *laptops* o puntos de acceso propuesto por el comité 802.11 implementado en la capa MAC.

WEP es, por tanto, el encargado de autenticar las estaciones y de cifrar las comunicaciones, utilizando para ello claves de longitud real de 40 bits, transformados en 64 bits al sumar un Vector de Inicialización (IV) de 24 bits.

El algoritmo utilizado para la encriptación es RC4. Utiliza una clave de encriptación asignada por el administrador tanto a los dispositivos móviles como a los puntos de acceso. La encriptación es simétrica con la misma clave tanto para encriptación como para desencriptación.

6.2.9.2 OSA (*Open System Authentication*)

Es un mecanismo de autenticación definido por el estándar 802.11 y consiste en autenticar todas las peticiones que recibe. El principal problema de este mecanismo es que no realiza ninguna comprobación del cliente y, además, todas las tramas de gestión son enviadas sin ningún tipo de encriptación, incluso cuando se ha activado WEP.

6.2.9.3 ACL (*Access Control List*)

Si bien no forma parte del estándar, la mayor parte de los productos dan soporte al mismo. Utiliza como mecanismo de autenticación la dirección MAC de cada estación, permitiendo el acceso únicamente a aquellas estaciones cuya dirección MAC está en la lista de control de acceso.

6.2.9.4 CNAC (*Closed Network Access Control*)

Sólo se permite el acceso a la red inalámbrica a aquellas estaciones que conozcan el nombre de la red o SSID (*Service Set Identifier*). Este nombre viene a actuar como contraseña.

6.2.9.5 WPA (*Wi-Fi Protected Access*)

Este mecanismo pretende sustituir a WEP, WPA necesita una clave maestra por cada usuario. Esta clave maestra es una contraseña que WPA utiliza para generar una clave para cifrar el tráfico de la red y esta clave de cifrado es generada automáticamente usando la clave maestra cada vez que se produce una transmisión, lo que aumenta sensiblemente la seguridad. WPA ha sido diseñada como una mejora de WEP por lo que la mayoría de los dispositivos inalámbricos podrán ser actualizados a esta nueva tecnología.

6.3 *Roaming*

El *roaming* es una característica inherente a una red inalámbrica, que crea situaciones en las cuales los suscriptores pueden vagar fuera de su área local de llamadas o fuera del área de su proveedor de servicio.

Para propósitos de *roaming*, una estación base puede ser vista como un miembro de una red y una red como miembro de un sistema. Un sistema contiene una o más redes y una red una o más estaciones base. Una red es identificada por su NID (identificación de la red). De la misma forma, un sistema es identificado por su SID (identificación del sistema).

Cada abonado a la red tiene la posibilidad de poder usar su propio terminal también en el extranjero; más concretamente en el ámbito del área de cobertura del país en que se encuentra.
La estación móvil tiene una lista de pares SID-NID en la memoria de su tarjeta SIM con las que se ha establecido un acuerdo de *roaming*; la lista se actualiza automáticamente cada vez que se enciende el teléfono, para permitir así añadir los nuevos países con los que se efectúen acuerdos.
La estación móvil es considerada como una estación local, es decir, sin *roaming*, si la estación base con la cual se comunica tiene un par SID-NID que coincide con uno de los pares dentro de la lista de la estación móvil. Por lo tanto, un suscriptor puede moverse de una red a otra o un sistema a otro y aún ser considerado un suscriptor local. La estación móvil es considerada un "vagabundo NID" si la estación móvil con la cual se comunica tiene un par SID-NID del cual sólo el SID está dentro de la lista de la estación móvil. En una forma similar, es considerada un "vagabundo SID" si su estación base tiene un SID que no pertenece a alguno de los pares SID-NID de la estación base.

Las tarifas durante el *roaming* se calculan del siguiente modo:

- Las llamadas efectuadas en la red visitada están sujetas a las tarifas vigentes de la misma para los clientes *roamers*; algunos operadores pueden aplicar un recargo por gastos administrativos ligados al *roaming* de hasta un 15%.
- Cuando se recibe una llamada en el extranjero se carga a cuenta la transferencia internacional de la llamada desde la red a la que se pertenece hasta la visitada, aquella en la que se encuentra momentáneamente, según las tarifas para llamadas internacionales vigentes.

En las redes inalámbricas típicas dentro de edificios se requiere más de un punto de acceso para cubrir todos los cuartos. Dependiendo de la solidez y material de las paredes, un punto de acceso tiene un rango de transmisión de 10 a 20 metros. La movilidad entre puntos de acceso también es llamada *roaming*. Los pasos para *roaming* entre puntos de acceso son los siguientes:

- Una estación inalámbrica decide que la calidad del enlace a su punto de acceso actual es demasiado pobre. La estación entonces comienza a buscar (*scanning*) otro punto de acceso.
- La exploración involucra buscar otra BSS (*Basic Service Set*).
- Entonces la estación selecciona el mejor punto de acceso y envía una petición de asociación para seleccionar al punto de acceso.
- El nuevo punto de acceso contesta con una respuesta de asociación. Si la respuesta es exitosa, la estación se mueve al nuevo punto de acceso. De otra manera, la estación continua buscando un nuevo punto de acceso.
- El punto de acceso que acepta una petición de asociación indica la nueva estación en su BSS para el sistema de distribución. El sistema de distribución actualiza su base de datos, la cual contiene la localización actual de las estaciones inalámbricas. Esta base de datos es necesaria para el envío de tramas entre diferentes BSSs, es decir entre los diferentes puntos de acceso que controlan los subsistemas BSS.

El *roaming* transparente es el que se lleva a cabo sin que exista un *hand-off* del dispositivo móvil cuando éste se cambia del área de cobertura de un punto de acceso conectado a un segmento de red A, al área de cobertura de otro punto de acceso conectado a un segmento de red B; es decir, el dispositivo móvil se encuentra conectado en todo momento a pesar de su movimiento y el cambio de células y de red. En aplicaciones de transmisión de voz, datos y video en tiempo real, el *roaming* transparente es sumamente importante para evitar la pérdida de datos de la señal transmitida y mantener una comunicación continua con los dispositivos móviles.

CAPÍTULO 7

SOLUCIONES CON GSM/GPRS, CDMA2000 Y UMTS VPN

7.1 Soluciones Para Conmutación de Circuitos con GSM y UMTS

La conmutación de circuitos de datos (CSD) ha sido la norma en las redes celulares por muchos años. En GSM, están disponibles los servicios portadores de CSD para 9.6 y 14.4 Kbps. Sin embargo, estas tasas de transferencia no proporcionan el soporte adecuado para las aplicaciones de hoy en día que requieren de gran ancho de banda. UMTS define servicios portadores de CSD de 64 Kbps y superiores.

Actualmente los servicios de conmutación de circuitos son ampliamente utilizados para aplicaciones basadas en WAP.

7.1.1 Tecnologías Para las Soluciones CSD

Para proporcionar acceso a una red de datos, el portador CSD sobre la red de acceso inalámbrico necesita ser terminado en una función IWF, donde toma lugar el acceso directo a la red o la conversión de los protocolos de conmutación de circuitos alámbricos. Típicamente, PPP es utilizado para proporcionar servicios de la capa de enlace y servicios de configuración de la autenticación de la terminal sobre los portadores CSD. En estos ambientes existen dos proposiciones para proporcionar servicios VPN:

- La función IWF podría terminar el portador inalámbrico, convertirlo a un circuito ISDN (por ejemplo, parte de un enlace PRI hacia un *switch*), y entonces terminar las llamadas ISDN hacia algún dispositivo RAS que pueda actuar como un LAC o simplemente proporcionar servicios de acceso a la red.

- La misma función IWF podría proporcionar funcionalidad de LAC y manejar los túneles L2TP establecidos hacia los LNSs en las redes cliente o dentro de la red del operador.

7.1.2 Escenarios de Despliegue de CSD

Son posibles dos áreas para usar VPN basada en CSD: el acceso a la red corporativa y el aprovisionamiento de servicios basados en WAP. El aprovisionamiento del servicio WAP puede usar Servicios Suplementarios de Datos no Estructurados (USSD), y SMS, pero estos canales son más apropiados para aplicaciones de muy baja tasa de transferencia, aplicaciones transaccionales, o para soportar un *canal de empuje* hacia la terminal. La navegación en el Web mediante *gateways* WAP normalmente requiere servicios CSD. Sin embargo, el protocolo WAP es también utilizado en despliegues GPRS, y las aplicaciones basadas en WAP son comúnmente usadas en las actuales terminales GPRS equipadas con las interfaces de usuario básicas.

La necesidad de VPNs CSD típicamente se presenta cuando la red usada para proporcionar acceso basado en CSD es compartida por otras aplicaciones. Por ejemplo, la red entre la función IWF y el *gateway* WAP puede ser utilizada para otros propósitos más que simplemente transportar tráfico WAP, y la misma IWF podría soportar conectividad hacia múltiples *gateways*, posiblemente fuera del dominio de la red del operador. Por ejemplo, algunos bancos pueden requerir terminar el circuito –posiblemente sobre un túnel L2TP- en un *gateway* WAP o un RAS que pertenecen al mismo banco. La misma red podría también ser usada para pasar el tráfico por túneles hacia centros de datos corporativos, redes ASP de terceros, e ISPs. Es requerido normalmente un número de teléfono diferente para acceder a diferentes servicios cuando es utilizado un portador CSD. El número telefónico puede estar asociado a un NAS, un LAC, o un punto de acceso de un *gateway* WAP.

La figura 7.1 ilustra el caso donde el tráfico CSD pasa por túneles vía L2TP hacia un LNS que proporciona acceso a una red WAP y de servicios de valor agregado. La misma red puede ser accedida usando L2TP desde un nodo GGSN, esto es, vía el acceso basado en paquetes. Entonces, es posible definir una IP VPN basada en L2TP que permita el aprovisionamiento de los mismos servicios.

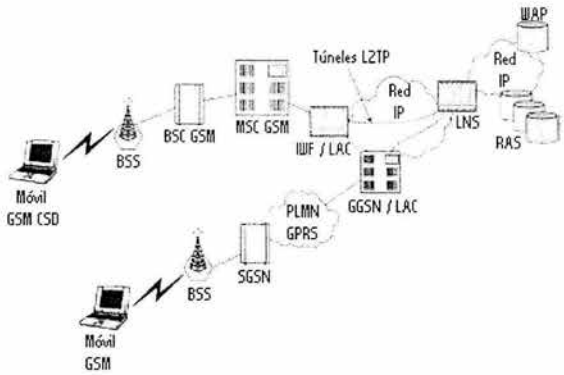


Figura 7.1 VPNs IP para el servicio CSD.

7.2 Soluciones Para Paquetes de Datos en GSM y UMTS

Los sistemas GSM y UMTS ofrecen capacidades para paquetes de datos. El sistema GSM, el cual fue diseñado y optimizado para soportar servicios de voz y de datos por circuitos, ha sido aumentado con capacidades para paquetes de datos vía la incrustación de GPRS. Por lo tanto, el sistema GPRS no siempre entrega transmisiones de datos óptimas u ofrece un alto funcionamiento. Contrariamente, UMTS ha sido diseñado para soportar servicios de paquetes de datos a través de su dominio PS, así su funcionamiento es mucho más eficiente y su tasa de transferencia de datos es mayor que la de GPRS.

Las diferencias en el servicio de VPN entre los sistemas GPRS y UMTS son en su mayoría insignificantes; salvo algunas excepciones:

- Se introdujeron nuevas características en los estándares 3GPP Release 99, como múltiples niveles de QoS por sesiones de datos sencillas.
- El soporte de DHCP Relay y de FA IP Móvil en el nodo GGSN.

7.2.1 Soluciones de la Tecnología de Paquetes de Datos

Comencemos esta sección enfocándonos en el nodo GGSN. El nodo GGSN se sitúa entre la red inalámbrica y las redes de datos alámbricas que se comunican con éste. Este elemento de red es común para los sistemas GPRS y UMTS. Este elemento también es la clave para proporcionar servicios de datos avanzados tales como MVPN.

El registro HLR, el subsistema AAA, los nodos SGSN, el perfil de usuario, y los subsistemas de administración de las relaciones de clientes también son componentes críticos en la entrega de servicios IP, pero la inteligencia de los servicios IP está concentrada en el nodo GGSN, ya que este es el punto que procesa los paquetes de usuario en la capa de red. El GGSN es un elemento de red que termina los túneles GTP establecidos desde el SGSN, donde el usuario está localizado. El GGSN proporciona puntos de acceso hacia las redes de paquetes de datos (PDNs). Cada punto de acceso es identificado mediante un nombre lógico, o *nombre del punto de acceso* (APN).

El nodo SGSN, en el tiempo de instalación de la sesión, resuelve el APN vía DNS hacia una dirección IP o una lista de direcciones IP que pertenecen a uno o más GGSNs que ofrecen el punto de acceso deseado. De hecho, para propósitos de disponibilidad del servicio o simplemente para la escalabilidad y compartir la carga, es deseable que un punto de acceso sea distribuido sobre más de un nodo GGSN. Esto resulta eventualmente en la selección de una dirección IP para ser utilizada para establecer un túnel GTP.

El proceso de establecimiento de un túnel GTP es la clave para el aprovisionamiento de servicios VPN. El primer mensaje utilizado para instalar el túnel GTP contiene la identidad del usuario proporcionada por el IMSI (*International Mobile Station Identifier*) y la MSISDN (*Mobile Station ISDN*). Además, transporta otras dos piezas de información muy importantes: el Identificador de Red y el Modo de Selección. Es posible autentificar al usuario en base al IMSI o a la MSISDN –por ejemplo, pasando el IMSI o la MSISDN y el APN hacia los servidores AAA que consideran que la información de la identidad debe ser acreditada, ya que ésta proviene de la red inalámbrica. Como parte de este proceso, el nodo GGSN puede recibir información del perfil del usuario en los mensajes recibidos del subsistema AAA. Entonces, esta información puede ser utilizada en el GGSN para recuperar los parámetros relacionados al servicio IP y las políticas desde bases de datos externas, como los directorios LDAP o COPS.

El Identificador de Red es usado en el GGSN para asociar la sesión a una red externa apropiada y determinar cuál es el método de autenticación del usuario y el protocolo (IPv4, IPv6 o PPP) que son utilizados, así como determinar si la sesión PPP necesita ser manejada en el GGSN o simplemente retransmitida hacia un LNS vía un túnel L2TP (en este último caso el GGSN actuaría como un LAC).

El elemento de información del Modo de Selección determina en qué forma entra la sesión del usuario a un punto de acceso específico –esto es, de acuerdo a qué criterio le fue permitido al usuario utilizar el APN mediante la red (SGSN). El APN puede de hecho ser especificado a la estación móvil, especificado a la red, o ser parte del perfil de suscripción y generado por la estación móvil o por la red.

En base a la recepción de la información del APN, y en la consulta de la información de manejo de sesión configurada por el APN, pueden ser ofrecidos en el GGSN diferentes servicios de acceso a la red. Estos servicios pueden clasificarse de la siguiente manera:

- Tipo IP PDP
  - IP Simple
  - IP con opciones de configuración de protocolo
  - DHCP Relay e IP Móvil
- Tipo PPP PDP
  - PPP Relay
  - PPP terminado en el nodo GGSN

En los estándares, se define que el *acceso transparente* es cuando el nodo GGSN no participa en la autenticación del usuario. El nodo GGSN no interroga a un servidor externo para la autenticación del usuario, y la autenticación del usuario para al acceso a la red simplemente depende de la autenticación de acceso en la red inalámbrica. La autenticación de acceso en la red inalámbrica es ejecutada cuando el usuario se enlaza al Administrador de Movilidad de los Paquetes (PMM, *Packet Mobility Management*) en el nodo SGSN o si el usuario cambia de SGSN conforme se mueve, en base a la acreditación de la información del SGSN antiguo o en base a la reautenticación de la estación móvil en el nuevo SGSN.

En este caso sólo es autenticada la tarjeta SIM (o USIM) en el dispositivo inalámbrico (estación móvil), más que el usuario de la tarjeta. El PIN es un secreto compartido con el proveedor inalámbrico y no es considerado como un secreto del usuario para el acceso a la red externa (esto es, la red externa no puede basar la autenticación del usuario en el PIN usado para la

autenticación de acceso inalámbrico). Así, las redes externas que ofrecen "servicio de acceso transparente" se basan en una relación de confianza con el portador inalámbrico. En los estándares, el *acceso no transparente* se refiere a todos los otros métodos de acceso donde el nodo GGSN participa en la autenticación del usuario.

7.2.2 Tipo IP PDP

El tipo IP PDP permite la provisión de servicios de acceso a la red IP para IPv4 e IPv6 ofreciendo a la estación móvil conectividad y servicios de la capa IP.

Las soluciones basadas en este tipo abarcan diferentes formas para ofrecer asignación de dirección IP, configuración de terminal, y conectividad de la capa más baja hacia la red IP. El valor del identificador de red enviado al nodo GGSN determina qué combinación de estos bloques que componen el servicio serán usados para las sesiones en base a la configuración del GGSN.

7.2.2.1 IP Simple

Un APN configurado para el modo de acceso IP Simple ofrece los siguientes tipos de servicios:

- Conectividad de capa 2 (ATM, MPLS, Frame Relay, PPP, etc.) o basada en túnel (modo túnel de IPSec, IP/IP, GRE, etc.) hacia la red externa.
- Posibilidad de comunicación con el servidor AAA para ejecutar la autenticación basada en IMSI o MSISDN o la asignación de dirección IP basada en RADIUS.
- El uso de la contabilidad RADIUS para comunicar de los eventos relacionados a la sesión a los servidores de contabilidad o servidores de aplicación.
- Asignación de dirección IP dinámica o estática.
- Activación del contexto PDP iniciado en la red.

Cuando es soportado el contexto PDP iniciado en la red, la dirección IP necesita estar estáticamente asociada al IMSI de la estación móvil. La dirección IP es asignada utilizando los *pools* locales en el GGSN, o en un cliente DHCP o RADIUS.

La gran limitación de este modo de acceso está en su modelo de confianza, el cual implica que la red externa depende completamente de la red inalámbrica para proporcionar autenticación del usuario. Por esta razón, este modo de acceso es más utilizado para proporcionar acceso a aplicaciones y servicios que no requieren autenticación del usuario. Además, si una aplicación accedida vía IP Simple requiere estricta autenticación del usuario, puede ser utilizada alguna autenticación basada en *login* y contraseña dentro de la sesión TLS.

Por el otro lado, este modo de acceso es más conveniente para servicios que requieren mínima interacción entre el usuario y la terminal para iniciar la conectividad. Este modo de acceso, si está acompañado por el uso de la autenticación o la contabilidad RADIUS, puede ser utilizado para proporcionar simple suscripción mediante la transferencia de información relacionada con la sesión a la capa de acceso a los servicios que distribuye la identidad y dirección IP del usuario para planear las aplicaciones. De hecho, la capa de acceso al servicio puede conocer el mapeo de la dirección IP para el IMSI o la MSISDN vía la asignación de la dirección IP basada en RADIUS o mediante el reporte del mapeo de la dirección IP para la identidad del usuario (IMSI o MSISDN) vía mensajes de contabilidad RADIUS. Hoy en día este mapeo dirección IP-identidad del usuario es el más utilizado en los *gateways* WAP o en servidores http para permitir características avanzadas de facturación y condicionamiento de contenido.

Con IP Simple se requiere que la estación base sea manualmente configurada por el usuario, posiblemente con la ayuda de algunas herramientas de software proporcionadas con el paquete de suscripción en un CD-ROM de instalación, con la dirección IP de los servidores NetBIOS (*Network Basic Input-Output System*) o de los servidores DNS. En resumen, este modo de acceso es

conveniente para terminales simples que requieren acceso a aplicaciones que pueden resolver la autenticación del usuario en una forma independiente de la autenticación de acceso a la red.

7.2.2.2 IP con Opciones de Configuración del Protocolo

La arquitectura del método de acceso IP con opciones de configuración del protocolo es descrita en la figura 7.2. El mensaje de solicitud de *creación del contexto PDP* puede contener el Elemento de Información con las Opciones de Configuración del Protocolo (PCO IE). Este elemento de información es un contenedor transparente de información de la configuración y autenticación de la terminal que es intercambiada entre el equipo terminal (TE) y los componentes de la terminal móvil (MT) de la estación móvil. El equipo terminal puede ser una *laptop* u otro dispositivo que se comunica con la terminal móvil a través de un enlace basado en PPP. La fase de autenticación PPP puede estar basada en PAP o en CHAP. La terminal móvil siempre autentica exitosamente al equipo terminal, junta material de autenticación de éste, y entra a la fase del protocolo de control IPCP (*Internet Protocol Control Protocol*). Este material de autenticación y la solicitud de configuración de IPCP son incluidos en el elemento PCO IE dentro de una solicitud de *activación del contexto PDP* enviada al nodo SGSN, el cual transfiere transparentemente esta información al nodo GGSN en un mensaje de solicitud de *creación del contexto PDP*. Eventualmente, el GGSN utiliza esta información para autenticar a la estación móvil. Si la estación móvil es autenticada, entonces el GGSN determina qué información de configuración de la terminal necesita ser enviada de regreso a la estación móvil (incluyendo una dirección IP para la estación móvil, las direcciones IP de los servidores DNS primario y secundario, o posiblemente las direcciones IP de los servidores NetBIOS primario y secundario) utilizando un elemento PCO IE dentro de la respuesta de *creación del contexto PDP*.

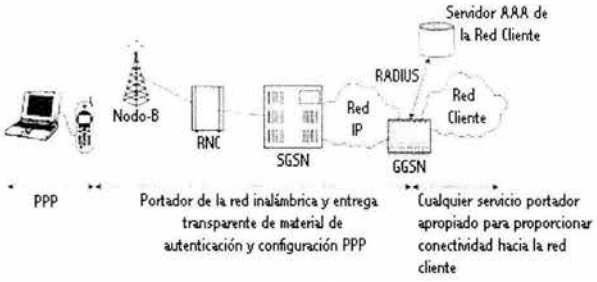


Figura 7.2 Arquitectura IP con modo de acceso basado en PCO

Este modo de acceso basado en el tipo IP PDP permite la conectividad de capa 2 o basada en túnel hacia la red asociada al APN como en el caso de IP Simple, pero éste añade la capacidad de ejecutar la autenticación del usuario para el acceso a la red en base a un secreto compartido entre la entidad administrativa de la red externa y el usuario final. La única debilidad de este modelo es la posibilidad de que un usuario malicioso obtenga el par demanda/respuesta enviado en un PCO IE y entonces lo utilice para obtener acceso a la red. De hecho, este modo de acceso no permite que el nodo GGSN (o el subsistema AAA) genere una demanda para la estación móvil, exponiendo al sistema a ataques.

Por la definición del nombre de usuario (usuario@dominio), IP con el modo de acceso PCO permite que el GGSN sea utilizado en una red visitada. Además, cambiando el componente de dominio, algunas plataformas inteligentes de servicios IP pueden ser configuradas para informar en el atributo de identificador de filtro u otros atributos RADIUS del nombre de un servicio cuya definición, en términos de políticas de acceso a la red, puede ser recuperado desde un LDAP. Las diferentes políticas de servicio pueden, por ejemplo, permitir al GGSN encaminar los paquetes de usuario hacia diferentes redes dependiendo del componente de dominio del nombre de usuario,

permitiendo al suscriptor seleccionar una red específica y el servicio que ésta ofrece en base a este valor.

7.2.2.3 DHCP Relay e IPv4 Móvil

La liberación R99 de los estándares 3GPP ha mejorado las especificaciones del sistema GPRS para permitir que el APN sea configurado para soportar el servicio DHCP Relay o la funcionalidad de agente externo (FA) de IP Móvil. La figura 7.3 describe un escenario típico del método de acceso DHCP Relay. Cuando la solicitud de creación del contexto PDP es enviada al nodo GGSN por un APN configurado para soportar DHCP o FA de IP Móvil, una respuesta de creación del contexto PDP es enviada inmediatamente al nodo SGSN. Éste define un túnel GTP y un portador hacia una estación móvil sin ninguna dirección IP asociada. Este túnel puede ser usado para intercambiar mensajes DHCP de configuración o mensajes de registro y avisos de IP Móvil. Eventualmente la estación móvil será asignada a una dirección IP usando métodos de DHCP o de IP Móvil. El acceso a la red remota será obtenido utilizando métodos de encapsulación permitidos por IP Móvil, o utilizando las tecnologías de capa 2 y de *tunneling* definidas por IP Simple cuando es configurado DHCP.

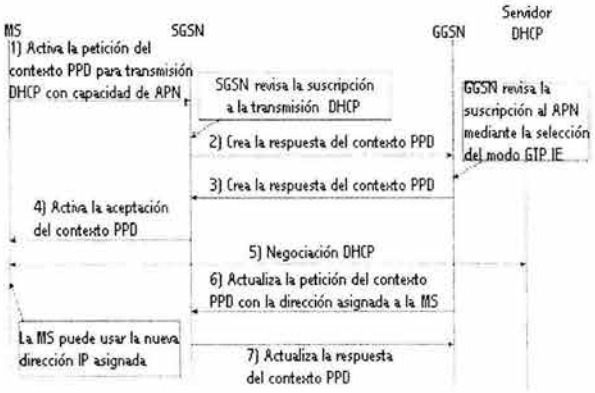


Figura 7.3 DHCPv4 en sistemas GPRS

El modo de acceso DHCP Relay es usado cuando se requieren métodos avanzados de configuración de terminales y cuando se requiere un modo de acceso "*LAN-like*". El modo de acceso *LAN-like* es particularmente conveniente para los dispositivos inalámbricos que requieren descubrir una gran cantidad de información relacionada con el servicio, tal como la dirección IP del *proxy* HTTP. Aquí la autenticación del usuario puede ser mejorada por el uso de la autenticación DHCP.

El modo de acceso IPv4 Móvil es también conveniente para el modo de acceso *LAN-like*, y soporta el *handoff* entre GPRS/UMTS y otras tecnologías de acceso como WLAN.

7.2.3 Tipo PPP PDP

El tipo PPP PDP permite el uso de encriptación y compresión PPP, así como el uso de protocolos de la capa de red. PPP define un protocolo de autenticación extensible (EAP) que permite terminar la negociación LCP sin determinar el protocolo de autenticación, el cual es transparente para el servidor de acceso a la red (NAS), y sólo es determinado en la fase de autenticación. Éste toma en cuenta la evolución de los protocolos de autenticación usados sin la necesidad de cambiar el NAS y la infraestructura AAA. Éste también permite el uso de avanzados algoritmos de autenticación,

como tarjetas inteligentes y biométrica, que no pueden ser usados por los métodos de autenticación existentes como PAP y CHAP.

PPP checa periódicamente la disponibilidad del enlace extremo-a-extremo utilizando un mensaje LCP de *eco solicitud/respuesta*. El GGSN y la terminal móvil tienen portadores GPRS/UMTS locales de disponibilidad de información. Ambas entidades pueden eliminar la retransmisión de solicitudes LCP de eco y responder ellas mismas a las solicitudes de eco. En el caso de PPP Relay, el nodo GGSN y la terminal móvil actúan como *proxies* de mensajes LCP de eco (el GGSN hacia NASs externos, la terminal móvil hacia el equipo terminal). Cuando el protocolo PPP es terminado en el GGSN, el GGSN no transmite solicitudes LCP de eco, y la terminal móvil actúa como un *proxy* LCP. Esta instalación garantiza el funcionamiento óptimo de un tipo PPP PDP basado en MVPN, y no representa alguna limitación práctica en la detección del estado del enlace.

Algunas implementaciones de clientes MVPN –como los clientes VPN basados en L2TP y los clientes VPN basados en IPSec- normalmente intercambian mensajes *"mantener-vivo"* con el *gateway* VPN. En este caso la red no tiene control sobre estos mensajes, no puede actuar como un *proxy* para evitar el uso ineficiente de los radio recursos. Además, una solución basada en un tipo PPP PDP con *proxy* LCP permitiría que el portador de extremo-a-extremo estuviera arriba mientras el portador inalámbrico esté arriba, mientras que un enlace cliente VPN-*gateway* VPN puede estar abajo aún cuando el portador inalámbrico no esté (por ejemplo, porque los mensajes *mantener-vivo* del túnel VPN se perdieron sobre la radio).

El beneficio adicional de una MVPN basada en un tipo PPP PDP es que en el caso de PPP Relay, el proveedor de servicio puede dejar al administrador de la red privada ejecutar la asignación de direcciones y funciones AAA, minimizando así el impacto y la complejidad sobre la administración de la red celular.

7.2.3.1 PPP Relay

En el tipo de acceso PPP PDP un APN puede ser configurado para transmitir tramas PPP hacia un dispositivo NAS externo predefinido. La tecnología estándar utilizada en este caso es L2TP.

L2TP puede ser transmitido sobre Frame Relay, ATM, y UDP/IP. El APN en el nodo GGSN debe estar configurado con la dirección L2 (Frame Relay o ATM) o la dirección IP del servidor LNS, así como con el nombre y la contraseña del túnel L2TP. La información asociada al APN determina qué tramas PPP de la red remota van a ser transmitidas, requiriendo entonces sólo del GGSN para instalar el túnel y las llamadas L2TP dentro de éste. Esto constituye una instalación realmente simple que puede garantizar un nivel suficiente de seguridad extremo-a-extremo cuando los túneles L2TP están asegurados vía el modo de transporte de IPSec y la encriptación PPP es negociada. La figura 7.4 describe los *stacks* de protocolos involucrados en una configuración típica de PPP Relay usando L2TP transportado sobre UDP/IP.

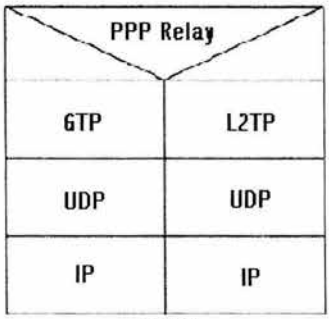


Figura 7.4 PPP transmitido usando L2TP.

Ya que el GGSN intenta transparentemente establecer las llamadas hacia el servidor LNS configurado por el APN de PPP Relay, se recomienda incluir el APN en la serie de información del contexto PDP almacenada en el HLR. De esta forma, el modo de selección entrante IE en la petición de Creación del Contexto de PDP es puesto al valor "0" y aquellos suscriptores que no están autorizados para intentar establecerse los túneles L2TP les es negado el derecho de establecer la llamada L2TP. Esta característica ayuda a proteger contra ataques de negación de servicio (DoS). También, el par atributo-valor del número L2TP debería ser fijado al MSISDN de la estación móvil, de modo que el LNS pueda ser configurado para rechazar las llamadas entrantes de números que no pertenecen a una cierta serie preconfigurada de números permitidos. El administrador del LNS puede usar esta opción para detectar el MSISDN de los usuarios que intentan tener acceso al LNS sin derechos, si es necesario, para razones de seguridad. También, el envío de este par atributo-valor es necesario para el LNS para transmitir la información MSISDN al subsistema AAA o a los *gateways* WAP vía una interfaz propietaria o basada en RADIUS (en cuyo caso el atributo RADIUS usado sería el atributo Identificador de la Estación que Llama).

7.2.3.2 PPP Terminado en el Nodo GGSN

El método de acceso PPP terminado en el nodo GGSN ofrece los beneficios de la configuración y autenticación de la terminal basadas en el protocolo PPP. Por ejemplo, cuando el usuario es autenticado, el servidor AAA puede retornar un nombre de un servicio para ser proporcionado al usuario o posiblemente la información necesaria para pasar las tramas PPP por un túnel hacia un LNS. El nodo GGSN también puede soportar compresión PPP, lo cual permite el uso más eficiente de la interfaz de radio.

En la misma plataforma GGSN usada para terminar los túneles GTP del tipo PPP PDP, es posible terminar y originar túneles L2TP, y por lo tanto la consolidación de múltiples tecnologías de acceso. La figura 7.5 ilustra los *stacks* de protocolos soportados por un nodo GGSN que termina el protocolo PPP.

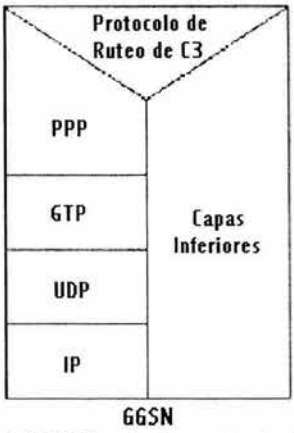


Figura 7.5 PPP terminado en el nodo GGSN.

Una comparación entre los modos de acceso PPP terminado en el nodo GGSN e IP PCO nos ayudará a comprender las debilidades y fortalezas de cada uno. El modo PPP terminado en el nodo GGSN es más amigable para la operación del protocolo GTP, ya que en este caso el túnel GTP puede ser establecido inmediatamente, sin requerir que el nodo GGSN espere los procesos de configuración y de usuario AAA para completarse.

En algunas implementaciones del nodo GGSN, es posible instalar el GGSN para inmediatamente establecer una llamada L2TP cuando un mensaje de entrada de Creación del Contexto PDP del tipo IP PDP es para un APN específico del modo de acceso "IP con opciones de configuración del protocolo". Esta instalación, sin embargo, constituye un uso no estándar de L2TP, y hace vulnerable a la sesión extremo-a-extremo de potenciales ataques que afecten el modo IP PCO. El establecimiento del túnel L2TP y el proceso de usuario AAA pueden crear problemas para el protocolo GTP en el nodo SGSN. En principio, un operador puede sintonizar los contadores GTP e intentar las retransmisiones para crear solicitudes de contexto PDP para tomar en cuenta la latencia asociada a "IP con opciones de configuración del protocolo" en la instalación de túneles, pero esta no es una medida segura y no ofrece suficientes garantías para proporcionar un servicio aceptable cuando el usuario está vagando hacia redes que no adoptan la misma sintonización de los parámetros GTP.

Finalmente, el tipo PPP PDP permite protocolos de compresión PPP, como STAC LZS y MPPC, para ser usados y negociados, lo cual es algo que no se permite en IP. En suma, IP con opciones de configuración del protocolo resulta ser dominado por el tipo PPP PDP terminado en el nodo GGSN.

7.2.4 Acuerdos del Nivel de Servicio

Usualmente, los acuerdos del nivel de servicio (SLAs) incluyen figuras de disponibilidad, pérdidas de paquetes por clase de servicio, políticas de reposición de las unidades faltantes en la red cliente si el operador también proporciona el equipo del cliente, soporte para la localización de fallas y ayuda para los administradores, capacitación técnica para los administradores, información de direccionamiento IP, y el alcance de las variables que el cliente puede administrar remotamente. Las comisiones de disponibilidad y soporte acordadas en el SLA pueden ser expresadas en términos del tiempo promedio entre fallas (MTBF), del tiempo medio para reparaciones (MTTR), y el alcance del soporte técnico o la disponibilidad de partes sobrantes para reemplazar las partes averiadas. Por ejemplo, puede haber diferentes tarifas aplicadas si está garantizado el soporte continuo o el soporte limitado.

Los niveles de QoS garantizados pueden también ser parte del SLA, junto con un acuerdo de las condiciones de tráfico según el modelo *DiffServ*, que incluyen un perfil del tráfico que el cliente debe cumplir y las políticas y reglas de mercado que el proveedor debe cumplir. El SLA también especifica cómo instalar las características de seguridad y confidencialidad de IPSec, incluyendo:

- Qué algoritmos de encriptación y autenticación del encabezado se espera sean utilizados.
- Si es utilizada la configuración manual o la infraestructura PKI para la distribución de las claves de autenticación.
- Si se utiliza el modo de transporte o el modo de túnel.
- Políticas particulares de IPSec.
- Las direcciones IP de los *gateways* de seguridad.

El criterio de administración de contraseñas para los túneles L2TP también es incluido. Dentro de esta sección del SLA relacionada a los parámetros de seguridad, debe ser descrito el manejo de los perfiles de los suscriptores. También, la existencia de la relación de confianza entre el cliente y el proveedor a menudo depende de cláusulas y garantías muy específicas.

Los métodos de instalación de las cuentas y del servicio de inscripción para los suscriptores asociados con la red cliente deben ser parte del acuerdo. El proveedor de servicio puede proporcionar un servicio de inscripción de página Web para este propósito. El tipo de información para autenticación del suscriptor que puede ser solicitada para obtener servicios de localización de fallas y soporte debe ser incluida, y el manejo de tales datos, que es materia de confidencialidad y privacidad, debe ser explicado detalladamente.

Otras especificaciones que el acuerdo debe incluir son:

- El método de acceso al servidor AAA (vía *proxy* o acceso directo), así como información de direccionamiento IP para los servidores de información de configuración de la terminal y los métodos permitidos de acceso a la red (IP con PCO, PPP Relay, PPP terminado), junto con los atributos de disponibilidad, seguridad y AAA requeridos para el servicio.

- Las condiciones de los métodos de pago y fecha de facturación, la documentación integral de los datos usados, y otros aspectos financieros y de facturación.

- Para el caso del servicio de conmutación de circuitos, los números telefónicos del servidor de acceso a la red, así como algunas condiciones asociadas con la terminación de las sesiones de usuario en los descansos.

- Las direcciones IP para el servidor LNS u otros puntos extremos de los protocolos de *tunneling*.

- Disponibilidad del servicio MVPN cuando se está en *roaming*.

Este documento, más allá de los aspectos legales y de negocios, reglamenta las expectativas del cliente y también define el servicio que éste recibirá. Es importante que el proveedor de servicio y el cliente puedan percibir el acuerdo como una herramienta útil para su interacción, definición del servicio, e implementación.

El nivel del acuerdo varía dependiendo del tamaño de la MVPN del cliente. También depende de si el proveedor desea estandarizar un servicio o si el proveedor desea utilizar la flexibilidad de su red para adaptar las diferentes necesidades de los clientes.

7.2.5 Cobro y Facturación

Los operadores pueden definir los planes de cobro en base a las tarifas, a los umbrales del volumen de tráfico, u otros parámetros, tales como la información a nivel de aplicación derivada de la inspección profunda de los paquetes. Todos los planes de cobro están basados en la apropiada colección de datos de cargo.

EL cobro en GPRS está basado en los Registros de Datos de Cargo (CDR colectados para la contabilidad del uso del acceso inalámbrico). Sin embargo, la contabilidad RADIUS es también utilizada para contar la duración de la sesión y posiblemente para comunicarse con una infraestructura de contabilidad operada por una red socio. Por ejemplo, RADIUS es utilizada cuando la red cliente requiere reunir los datos de contabilidad para analizarlos y retratar el perfil usado, y posiblemente de cobro para el acceso a la red misma en una manera independiente de la facturación ejecutada por el proveedor de servicio inalámbrico. Los estándares también definen el soporte de servicios de prepago en GPRS. El estándar es CAMEL Fase 3 (ver figura 7.6), el cual define la interacción del nodo SGSN con la función de control de servicio GSM (GSM SCF) para la provisión de servicios de prepago. El protocolo usado para tal interacción es llamado *CAMEL Aplication Part*, o CAP.

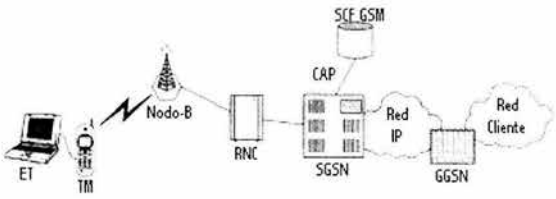


Figure 7.6 Arquitectura de los sistemas de prepago CAMEL Fase 3

7.2.6 *Roaming*

Una de las fortalezas de los sistemas GSM/GPRS y UMTS es su capacidad de *roaming* a través de países y redes que pertenecen a diferentes operadores. Esta capacidad también puede ser utilizada para soportar servicio MVPN.

El soporte de *roaming* en GSM ha sido una de las razones principales por las que fue establecida la Asociación GSM. Muchos operadores acordaron proporcionar servicio de *roaming* a los suscriptores dentro de sus propias redes desde otras Redes Locales Móviles Públicas (HPMNs) de acuerdo a una serie de reglas definidas en el Memorando de Entendimiento de GSM (MoU).

Uno de los principios del MoU de GSM es que la Red Pública Móvil Visitada (VPMN) no puede proporcionar más servicios de los que el usuario recibe en la red HPMN. Las redes que entran dentro de un acuerdo de *roaming* necesitan especificar qué servicios van a recibir los usuarios en el modo de visitante, y también tienen que acordar las reglas que gobiernen las formas en que tales servicios puedan ser negados. El operador local siempre puede definir clases de usuarios a los que se les puede ofrecer servicios de *roaming* por VPMNs definiendo la exclusión de información sobre todos o un subconjunto de servicios disponibles en una red VPMN. Esta información es almacenada en la base de datos HLR y descargada en el nodo de servicio en la red visitada en el momento de conexión del usuario, o esta información es transferida hacia un nodo de servicio cuando un usuario ejecuta un procedimiento de actualización de localización (*handoff*). Cuando la estación móvil intenta enlazarse a una red y el usuario no tiene derecho para obtener servicio de *roaming*, la red debe señalar esto, y la estación móvil no intentará de nuevo enlazarse a la red.

Para el caso de servicios de conmutación de circuitos de datos (CSD), el soporte de *roaming* es equivalente al soporte de *roaming* para servicios de voz. El *roaming* de datos en los sistemas GPRS/UMTS está gobernado por los estándares y los documentos de los consorcios industriales. Los estándares GPRS permiten a un usuario vagar en una red visitada y usar un nodo GGSN en la red local, o usar un nodo GGSN en la red visitada. La interfaz entre el GGSN en la red local y el SGSN en la red visitad es llamada interfaz Gp. El túnel GTP, cuando es utilizado un nodo GGSN en la red local, atraviesa una red que es proporcionada por el proveedor de servicio de red de tránsito. Esta red, ilustrada en la figura 7.7, es llamada GRX (*GPRS Roaming Exchange*), y está basada en un esquema de direccionamiento público.

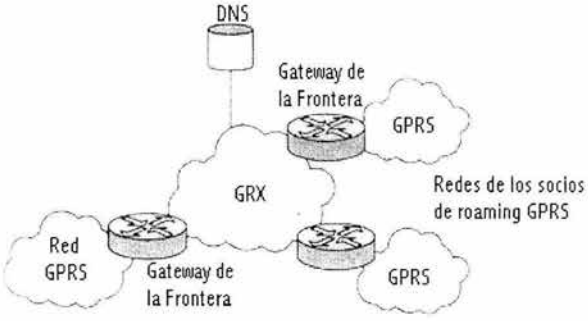


Figura 7.7 Redes GPRS para el servicio de *roaming*.

El acceso a la red GRX puede ocurrir en los puntos centrales de intercambio, los cuales son equivalentes a los puntos IXC (*Internet Exchange Points*), donde muchos operadores pueden intercambiar tráfico de *roaming* e instalar BGP4, sobre una infraestructura L2 proporcionada por el proveedor de la red GRX. Las rutas BGP anunciadas sobre la GRX no son distribuidas fuera de la GRX, y tampoco ninguna de las rutas de Internet son distribuidas sobre la GRX. Por lo tanto, no existe una capa de red mutua entre Internet y la red GRX: la GRX es una red privada basada en un esquema de direccionamiento público.

El servicio de MVPN basado en GPRS es normalmente ofrecido en base a un nodo GGSN en la red local. Esto se lleva acabo dedicando un APN para la red cliente, y este APN resolverá una dirección IP o una lista de direcciones IP que pertenecen a un nodo GGSN en la red local. Esta proposición requiere que los túneles GTP entre los nodos SGSN y los nodos GGSN locales estén protegidos mediante el modo de transporte de IPSec, de tal manera que no se requiere que la relación de confianza entre el operador de la red visitada y el operador de la red local sea extendida sobre todos los proveedores de red atravesados por el túnel GTP.

Sin embargo, también es posible usar un nodo GGSN en la red visitada, definiendo un APN que pueda ser traducido por el nodo SGSN de la red visitada dentro de un APN que resuelva una o más direcciones IP pertenecientes al nodo GGSN en la red visitada. Esto requiere un APN de tipo PPP PDP, o un APN que soporte el tipo IP PDP con modo de acceso PCO, y la capacidad del GGSN para asignar dinámicamente la solicitud de entrada del usuario a una VPN apropiada y para establecer conectividad, si no está instalada estáticamente. La asignación al usuario de una VPN está usualmente basada en la información del perfil de usuario obtenida del subsistema AAA (por ejemplo, vía el identificador de filtro de RADIUS o información del túnel L2TP de RADIUS). Otras soluciones pueden requerir más personalización del nodo GGSN (por ejemplo, búsqueda de tablas).

Cuando un usuario que está vagando utiliza un nodo GGSN local, la información de contabilidad en el GGSN es crítica para registrar los datos usados en la red local independientemente de la red

visitada. También, el GGSN local puede usar la contabilidad de RADIUS para adaptar las necesidades de la red cliente. La autenticación del usuario en un nodo GGSN local es ejecutada de la misma forma que en un escenario sin *roaming*. Para los casos en los que depende estrictamente de los datos de suscripción de la base de datos HLR para la autenticación del usuario, se requiere la protección de la integridad de la señalización GTP desde el nodo SGSN visitado hasta el nodo GGSN local, de tal manera que el elemento de información de Modo de Selección no puede ser alterado y por lo tanto se espera sea válido, ya que es generado por una red visitada que tiene una relación de confianza con la red local. Como parte del acuerdo de *roaming*, la forma en que la integridad de la señalización GTP es garantizada debe estar sujeta a la negociación y a la definición. De la misma forma deben ser definidas las políticas de IPSec para VPNs.

La autenticación del usuario en un nodo GGSN de la red visitada está gobernada por un acuerdo de *roaming* AAA, donde el GGSN visitado puede estar actuando como un cliente AAA para una infraestructura AAA basada en un *proxy* RADIUS y que posiblemente incluya un corredor RADIUS (ver figura 7.8).

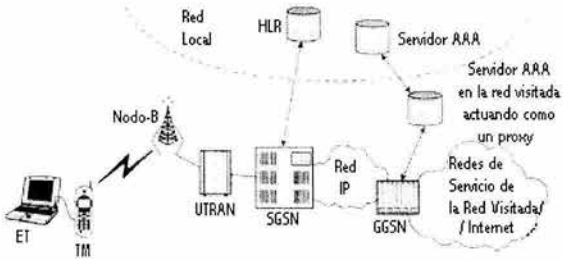


Figura 7.8 *Roaming* en GPRS con GGSN en una red visitada.

7.3 Soluciones VPN de CDMA2000

7.3.1 Visión del Acceso a una Red Privada en CDMA2000

El sistema de datos de la red central de CDMA2000 está basado en los servicios de la capa de enlace proporcionados por el protocolo PPP combinado con un elaborado esquema de movilidad. Por lo tanto, el servicio de VPN obligatoria ofrecido dentro de este sistema puede estar basado en la encapsulación PPP que utiliza mecanismos tal como L2TP, que permite a una corporación ejecutar la autenticación del usuario y la configuración de la terminal mediante la terminación de las sesiones PPP en un servidor LNS propio. Alternativamente, puede ser utilizado el protocolo IP Móvil y la capa de enlace PPP es terminada en la red portadora; en esta configuración son utilizadas las características avanzadas de IP Móvil para autenticación y *roaming* del usuario y configuración dinámica de la dirección IP. La funcionalidad soportada por el nodo PDSN en la infraestructura de CDMA2000 es especialmente importante para el soporte de MVPNs. Este nodo maneja las sesiones PPP originadas por la estación móvil y encapsula el tráfico de usuario para el viaje adicional a través de la red central del portador o a través de redes públicas como Internet. Inversamente, el nodo PDSN termina los túneles originados en las redes privadas y envía los paquetes IP hacia los dispositivos móviles del usuario u otros puntos finales de destino. Cuando la decisión de utilizar túneles obligatorios está hecha, para asegurar el nivel deseado de seguridad extremo-a-extremo, los operadores de la red privada deben averiguar acerca de la protección de la seguridad disponible para el segmento de la trayectoria de los datos no protegido por el túnel obligatorio, como la interfaz de radio y los enlaces internos hacia la red del operador. Así con cualquier otro tipo de túnel obligatorio, la red privada con sus datos debe acreditar a un proveedor de acceso inalámbrico, en cuya red son originados y terminados los túneles VPN. Normalmente, los operadores inalámbricos proporcionan a sus clientes un alto grado de confianza en el nivel de

seguridad dentro de su red, como una precondición para establecer la relación de confianza necesaria para correr un servicio de VPN obligatoria (también conocida como basada en red).

Las VPNs basadas en IP Simple e IP Móvil en CDMA2000 no son la excepción de la necesidad de una relación de confianza en el servicio de VPN obligatoria. Aún cuando el esfuerzo fue hecho en los estándares para excluir al portador inalámbrico de la asociación de seguridad entre la estación móvil y la red privada, los datos que pasan a través de la red de acceso inalámbrico son susceptibles del acceso no autorizado en el nodo PDSN. Ya que el PDSN en la red del operador inalámbrico es el punto de terminación del protocolo PPP y opcionalmente el punto de origen de IP Móvil o de L2TP, los paquetes IP del usuario están expuestos a inspecciones indeseables dentro de este dispositivo por personas o procesos no autorizados por la red privada. Por esta razón, el nodo PDSN puede ser considerado un ejemplo de un enlace débil en la cadena de dispositivos involucrados en el transporte del tráfico del usuario cuando son usados en los modos de VPN obligatoria.

7.4 IP Simple: ¿Una verdadera MVPN?

En IP Simple, las sesiones PPP originadas por las estaciones móviles son terminadas en el nodo PDSN de manera similar que en IP Móvil. Sin embargo, si la estación móvil de IP Simple debe cambiar el actual nodo PDSN de servicio, la sesión PPP es terminada y la estación móvil debe obtener una nueva dirección IP cuando se enlace a un nuevo nodo PDSN.

Los vendedores de infraestructura de CDMA2000 han hecho grandes esfuerzos para manejar este problema sobre las capas física y de enlace. Una solución popular es enredar completamente la red de Funciones de Control de Paquetes (PCFs) y los PDSNs. Esta solución asegura que la estación móvil permanezca anclada en el mismo PDSN aunque la función PCF de servicio cambie. Esto es posible debido a que la conexión PPP es establecida entre la estación móvil y el nodo PDSN, y si la red fundamental puede mantener "viva" la conexión, la sesión PPP será preservada. De esta forma, la dirección IP de la estación móvil permanece constante y puede sobrevivir aún cuando cruce los límites del controlador de la estación móvil. Sin embargo, esta duración solo trabaja por la duración de la sesión. En otras palabras, nuevas direcciones IP dinámicas deben ser adquiridas si la sesión se cae y entonces reinstalada por el móvil. Como resultado, IP Simple no es el principal método de acceso que se ofrece a los clientes de VPN de CDMA2000 cuando requieren soportar patrones de alta movilidad. Debido a estas limitaciones, los suscriptores corporativos que utilizan móviles que operan en el modo IP Simple a menudo no pueden obtener un servicio de MVPN. En muchas ocasiones, las estaciones móviles conectadas a redes CDMA2000 en el modo IP Simple no pueden mantener sus conexiones de VPN obligatoria o voluntaria si se cambia el nodo PDSN de servicio.

7.4.1 Arquitectura de IP Simple Para VPN

El modelo de la arquitectura de IP Simple, es descrita en la figura 7.9. Como en las redes de acceso remoto alámbricas, la sesión PPP iniciada por la estación móvil es terminada por un servidor de acceso a la red (NAS), cuya funcionalidad en este caso es soportada por el nodo PDSN y entonces transmitida sobre un túnel hacia un punto remoto de terminación del túnel mantenido detrás de un *firewall* en la red privada. El protocolo de *tunneling* recomendado para este caso es L2TP. La funcionalidad del Concentrador de Acceso L2TP (LAC) soportada por el nodo PDSN, encapsula la sesión PPP de la estación móvil y la transporta sobre una red IP arbitraria hacia un servidor L2TP (LNS) remoto, el cual termina el enlace PPP en la red privada.

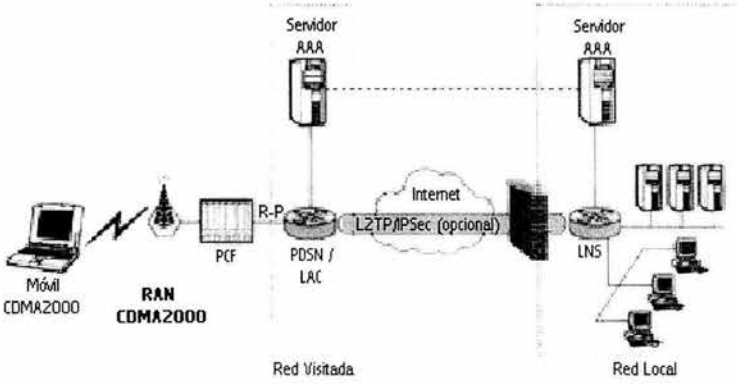


Figura 7.9 Modelo de la arquitectura VPN en IP Simple.

Una VPN inalámbrica basada en IP Simple con L2TP originado en el nodo PDSN puede ser clasificada como un caso típico de *tunneling* obligatorio. El enlace PPP del usuario móvil es efectivamente transmitido a través del nodo PDSN sobre un túnel L2TP hacia un servidor LNS remoto, que terminal el enlace PPP y, en combinación con el servidor AAA local proporciona funciones primarias de autenticación y asignación de dirección, que permite a los dueños de la red privada retener una cantidad significante de control sobre la autenticación y asignación de dirección de la estación móvil. El nodo PDSN y el servidor AAA visitado asociado completan las negociaciones CHAP necesarias para descubrir la dirección del servidor LNS privado. Al contrario de IP Móvil, el método de acceso de IP Simple no requiere un Agente Local pero depende de la infraestructura AAA distribuida para acceder a los servidores AAA remotos asociados con el servidor LNS en las redes privadas. Si el servicio de VPN no es solicitado durante la etapa de negociación de IP Simple, el nodo PDSN se convierte en un elemento responsable de la asignación de la dirección IP y de la autenticación del usuario.

En la figura 7.10 se muestra un modelo de referencia del protocolo IP Simple para VPN. En esta figura, L2TP es aumentado con protección IPSec.

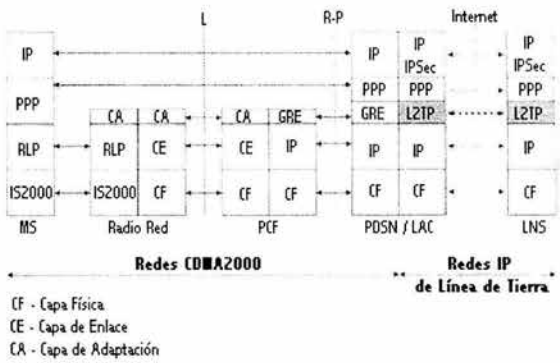


Figura 7.10 Modelo de referencia del protocolo IP Simple para VPN.

Una VPN basada en IP Simple también puede ser utilizada por el portador inalámbrico para seleccionar a los usuarios, como el personal de mantenimiento, para acceder a su propia Intranet privada. Esta Intranet privada incluye un servidor LNS dedicado, al cual puede acceder el personal

de mantenimiento mediante el ingreso, por ejemplo, de su combinación nombre de usuario/NAI para pasar por un túnel hacia su LNS y entonces ser proporcionado el acceso al centro de servicio de la red o cualquier otra red apropiada.

7.4.2 Escenario de la Llamada de VPN en IP Simple

Consideremos la secuencia de establecimiento de la conexión VPN de IP Simple descrita en la figura 7.11. Este escenario asume que una estación móvil está enlazada a su red local –esto es, la red donde le fue asignada su dirección IP original.

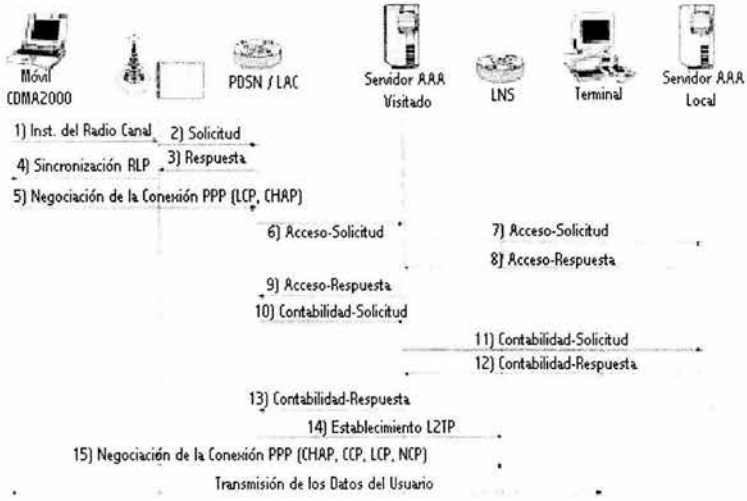


Figura 7.11 Establecimiento de la conexión VPN en IP Simple

Hay dos fases de establecimiento de la VPN: el establecimiento de la conexión entre la estación móvil y el nodo PDSN de servicio y el establecimiento de la sesión L2TP que encapsula el tráfico PPP entre el nodo PDSN que soporta la funcionalidad de LAC y un LNS en la red privada.

En el inicio de la primera fase, es instalado el radio enlace entre la estación móvil y el subsistema de la estación base (BSS), y subsecuentemente es establecida la conexión de la capa de enlace entre la estación móvil y la función de control de paquetes (PCF). Para autenticar al usuario, el PDSN envía una petición de autenticación al servidor AAA local, éste envía de regreso una respuesta de autenticación que indica si la petición es aceptada o rechazada. El mensaje del servidor AAA también contiene el tipo de túnel (L2TP en nuestro caso) y la dirección IP destino del servidor LNS dentro de la red privada. Si el usuario es autenticado positivamente, el acceso a la red privada es concedido y es establecido el enlace PPP.

Durante la siguiente fase, el PDSN/LAC crea un túnel L2TP hacia el servidor LNS en la red privada. El LNS posiblemente después una negociación LCP y autenticación del usuario adicionales asigna la dirección IP a la estación móvil del *pool* de direcciones IP de la red privada utilizando RADIUS, DHCP, u otro mecanismo dinámico de asignación de dirección en la fase de establecimiento del protocolo NCP (*Network Control Protocol*). Enseguida, el LNS se despoja de los encabezados de encapsulación y encamina el paquete IP hacia la terminal destino dentro de su red privada. En la otra dirección, los paquetes IP desde una terminal que trata de enviar paquetes a una estación móvil, llegan al servidor LNS, el cual los encapsula en tramas PPP y los envía al PDSN/LAC donde la estación móvil está anclada a través del túnel L2TP. El PDSN/LAC se despoja

del encabezado L2TP y envía las tramas PPP a la estación móvil. Si la estación móvil cambia su localización y se enlaza a otro PDSN, este procedimiento debe repetirse y deben ser asignadas nuevas direcciones IP.

7.5 VPN Basada en IP Móvil

El servicio de VPN por IP Móvil de CDMA2000 maneja muchos de los problemas de una solución basada en IP Simple mediante la preservación de las direcciones IP de la estación móvil mientras emigra a través del área cubierta por más de un nodo PDSN. Una VPN de IP Móvil puede ser implementada en dos formas básicas en los sistemas basados en CDMA2000, como se muestra en la figura 7.12. La primera, a la cual nos referiremos como *VPN de HA remoto público*, asume que el Agente Local reside en una red privada y estará conectado con un nodo PDSN, el cual reside en el dominio del portador inalámbrico vía un túnel IP Móvil. La otra, a la cual nos referimos como *VPN de HA local privado*, asume que el Agente Local residirá en la misma Intranet como un nodo PDSN y será poseído y mantenido por un portador inalámbrico. Los servicios de VPN en este caso serán soportados por una combinación de túneles IP Móvil y opciones de transporte arbitrarias, como encadenamiento con otros túneles, líneas arrendadas, o PVCs de ATM.

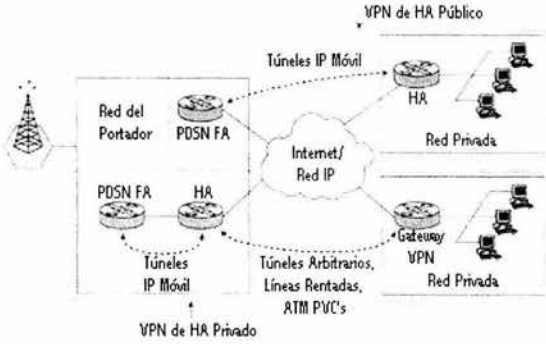


Figura 7.12 Opciones VPN de IP Móvil.

7.5.1 Opción VPN de HA Público

Se espera que esta opción VPN de IP Móvil sea el escenario principal soportado por la mayoría de los operadores inalámbricos de CDMA2000 que ofrecen servicios de MVPN. En esta proposición, descrita en la figura 7.13, todo el tráfico descendente (hacia la estación móvil) que es originado en una red privada pasa por un túnel desde el HA que reside ahí hacia el nodo PDSN que reside en la red del portador. El tráfico ascendente (originado por la estación móvil) pasa por un túnel desde el nodo PDSN en la red de acceso inalámbrico hacia el HA en la red cliente. Para este propósito, el PDSN puede establecer un túnel opcional de regreso. Ambos túneles IP Móvil (hacia delante y de regreso) están basados en los protocolos IPIP o GRE y pueden estar combinados con seguridad IPSec.

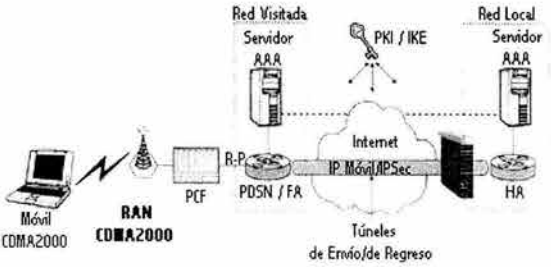


Figura 7.13 Arquitectura de HA VPN Público.

La dirección IP de la estación móvil es asignada del espacio de direcciones de la red cliente, el cual puede depender de esquemas de direccionamiento IP públicos o privados, relevando al proveedor de acceso inalámbrico de la obligación de administrar las direcciones IP. La dirección del HA en la red privada es descubierta utilizando el NAI en la petición de registro de IP Móvil cuando el HA es asignado estáticamente. En este escenario la estación móvil debe registrarse con los servidores AAA local y visitado y experimentar un procedimiento AAA que involucre a los clientes AAA en el PDSN y en el HA.

7.5.1.1 Seguridad en la VPN de HA Público

Los túneles IP Móvil hacia y desde redes privadas establecidos a través de redes IP públicas como el Internet generalmente son inseguros y requieren protección de la seguridad, de forma similar a la situación con túneles L2TP en el caso de IP Simple. Tal protección puede ser proporcionada por el protocolo IPSec combinado con un mecanismo de distribución de claves, como IKE (*Internet Key Exchange*). La figura 7.14, describe un modelo de referencia del protocolo para esta opción de VPN. Es importante para el HA verificar la identidad del nodo PDSN del portador inalámbrico que tendrá acceso a los datos de usuario sin protección por la duración de la sesión. Es también importante para el PDSN verificar la identidad del HA de modo que el tráfico de usuario no sea dirigido hacia una localización desconocida. En el escenario de una VPN de HA público, el HA es operado por la red privada hacia la cual el usuario tiene acceso y administrará la seguridad y movilidad del usuario formando asociaciones dinámicas de seguridad con los PDSNs.

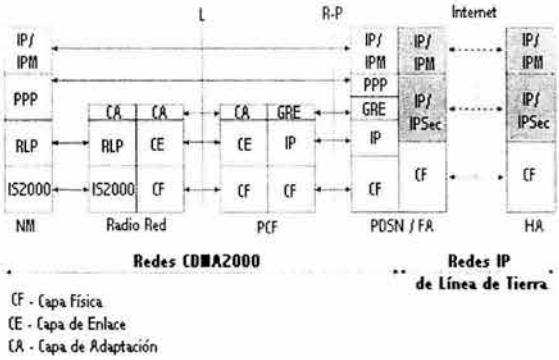


Figura 7.14 *Stack* de protocolos para HA VPN Público

Normalmente, los portadores inalámbricos despliegan seguridad IP para la comunicación inter-dominio y para protección de la señalización de IP Móvil. Para minimizar las probabilidades de una violación de seguridad, el tráfico hacia y desde el HA puede ser encriptado. El nodo PDSN puede

decidir qué política aplicar en base al atributo de *Nivel de Seguridad* de RADIUS. Durante la instalación de un túnel entre el PDSN y el HA, es utilizado el mecanismo IKE para verificar la identidad del PDSN y del HA. La asociación de la clave de seguridad puede ser:

- Un secreto configurado estáticamente por la extensión de autenticación HA-FA de IP Móvil
- Un secreto pre-compartido IKE configurado estáticamente
- Un secreto pre-compartido IKE dinámico distribuido por la infraestructura AAA local
- PKI con certificados

La extensión estática de autenticación HA-FA de IP Móvil reemplaza al secreto pre-compartido IKE estático, que reemplaza al secreto IKE dinámicamente distribuido, que reemplaza al certificado de PKI en el orden de precedencia. El pre-aprovisionamiento de la clave pre-compartida MN-HA-AH se requiere en la versión actual de [IS835], el estándar que gobierna la mayor parte de los requisitos de la infraestructura central de CDMA2000. El material de las claves que es distribuido durante el proceso de registro AAA debería ser protegido contra escuchadores escondidos. Si un atacante pudiera aprender estas claves, podría llevar a la negación del servicio o de la sesión contra los nodos móviles. Esta protección puede ser proporcionada en una base de salto-por-salto —por ejemplo utilizando IPSec entre servidores AAA visitados en el resto de la infraestructura AAA. Cuando es usada una asociación de clave secreta estática pre-compartida, la primera fase de intercambio es autenticada con códigos de autenticación de mensaje. El uso de secretos pre-compartidos puede simplificar la operación porque evita la necesidad de procesos y certificados de validación. Sin embargo, estas asociaciones pueden introducir una carga adicional debido a la necesidad de establecerlas en pares PDSN-HA. Por esta razón, el estándar [IS835] proporciona un mecanismo para la distribución de claves pre-compartidas dinámicas vía la infraestructura AAA durante el registro del nodo móvil. Mientras la infraestructura AAA local procesa y valida la demanda-respuesta de la estación móvil, puede generar un secreto pre-compartido y distribuirlo con la respuesta AAA hacia el PDSN. El PDSN puede entonces usar el secreto, junto con una identidad construida de la respuesta, para llevar a cabo la negociación IKE con el HA. Esto permite el establecimiento seguro de la seguridad IP entre el PDSN y el HA sin la necesidad de la configuración manual de las claves entre todos los pares posibles.

Si el túnel de regreso es soportado por el HA según lo indicado por el servidor AAA local en el atributo RADIUS de *Especificación del Túnel de Regreso* de [IS835], la seguridad de IPSec es autorizada para pasar los datos por el túnel, y el móvil solicita la construcción del túnel de regreso, entonces el PDSN proporcionará la seguridad sobre el túnel de regreso. Los túneles de regreso son instalados como resultado del nodo móvil que fija el bit "T" en su petición de registro. Esto causa que todos los paquetes del nodo móvil sean encapsulados y entregados al HA por el nodo PDSN. Tales túneles permiten el uso de direcciones privadas no únicas, por los nodo móviles, y los túneles de regreso (así como los túneles hacia adelante) pueden ser opcionalmente protegidos con IPSec.

7.5.2 VPN de HA Privado

La trayectoria de los datos del suscriptor de CDMA2000 siempre incluirá el nodo PDSN y el HA, al menos en una dirección. El tráfico de datos descendente debe pasar a través del HA en la red local de la estación móvil y del PDSN de servicio. El tráfico ascendente (desde la estación móvil) debe pasar a través del nodo PDSN sólo si la estación móvil solicita acceso a Internet, y a través del par PDSN/HA unidos por el túnel IP Móvil de regreso si la estación móvil solicita acceso a la red privada. Para satisfacer estos requerimientos, los portadores inalámbricos deben desplegar bastante capacidad del HA para soportar a las estaciones móviles de IP Móvil si requieren acceso a la red privada o sólo requieren acceso a Internet.

Teniendo una enorme infraestructura HA ya disponible, los portadores inalámbricos que desean ejercer tanto control como sea posible del aprovisionamiento al suscriptor podrían entonces rechazar completamente el acceso a los HAs en las redes privadas, forzando todo el tráfico hacia y desde las redes privadas a través de sus propios HAs y entonces enviándolo entre las redes

privadas mediante el uso de otra tecnología, como se muestra en la figura 7.15. En este escenario, las redes privadas no necesitan mantener el HA y terminar los túneles IP Móvil. En lugar de eso, el portador inalámbrico y la red privada deben depender de un serie de túneles concatenados en el HA perteneciente al portador combinados con acuerdos privados y SLAs específicos para ser capaces de proporcionar ofertas seguras de VPN.

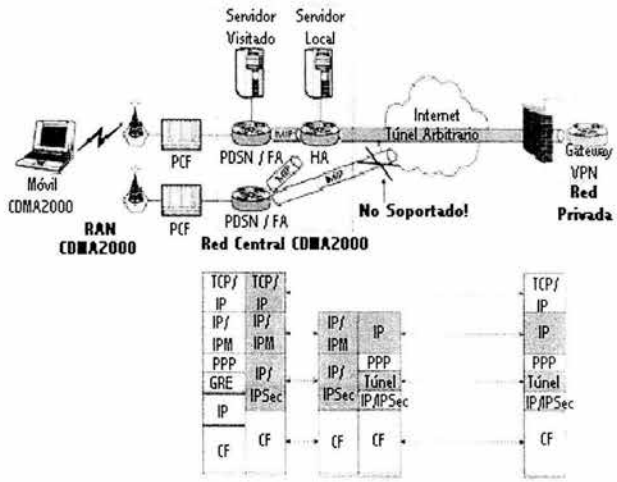


Figura 7.15 Arquitectura del HA VPN privado y el stack de protocolos

Las reglas de despliegue para una VPN de HA privado son muy diferentes de aquellas para una VPN de HA público y traen algunas consecuencias significantes para los operadores. Posiblemente, la VPN de HA privado simplifica la asignación de la dirección IP para los usuarios móviles permitiendo a una entidad, un portador inalámbrico, controlar el procedimiento. Opcionalmente los portadores pueden ser capaces de consolidar –al menos en teoría- el proceso de asignación de dirección IP dentro de una localización, un terreno hipotético de HA combinado con un depósito de direcciones IP y servidores DHCP y AAA de gran tamaño. Por otra parte, los portadores inalámbricos pueden retener el control sobre el aprovisionamiento de los usuarios y la seguridad de la carga útil y del tráfico de señalización. Los operadores que están a favor de la VPN de HA privado tendrán que recoger la carga del aprovisionamiento del usuario, extensamente empleado en los negocios estilo ISP, ser responsables de suministrar millones de direcciones IP a sus usuarios móviles, y estar preparados para limitar sus ofertas a las corporaciones y renunciar a otras ventajas y la simplicidad del estándar basado en una VPN de HA público.

La responsabilidad de asignar direcciones IP posee un dilema para el operador de CDMA2000. Los operadores deben decidir si proporcionar a sus suscriptores una dirección IP pública o privada o una mezcla de ambas.

Otro desafío asociado con una VPN de HA privado es la necesidad de crear una infraestructura de conmutación de túneles alrededor del HA. La creación de este marco será un ejercicio que involucre nuevos tipos de definiciones de SLAs, nuevas disposiciones para facturación, y nuevos requerimientos para las plataformas HA –las cuales necesitarán soportar tecnologías WAN y de conmutación de túneles sobre una escala portador-clase, además de otras nuevas tareas.

La arquitectura mostrada en la figura 7.15 puede estar basada en una de las tecnologías de *tunneling* definidas por el IETF, como IPSec desplegada en el modo de túnel o combinada con

MPLS. En tal escenario los túneles IP Móvil hacia y desde PDSNs geográficamente distribuidos estarían terminados en el HA privado en la red del portador y luego concatenados con los túneles IPSec correspondientes creados por empresas individuales, que asumen la existencia de relaciones predefinidas con el portador inalámbrico. Este escenario asume que la asignación de la dirección IP y la autenticación de las estaciones móviles será completada en la red del portador.

7.6 Asignación del HA en la Red

En esta sección se presentan las opciones de despliegue para el HA en la red central de CDMA2000 así como su impacto en la arquitectura de MVPN.

7.6.1 Asignación del HA Privado en Relación al PDSN

Recordando del capítulo 4 que por definición un PDSN debe cubrir una cierta región geográfica, mientras que un HA, que representa a la red local de la estación móvil, sirve como un punto de anclaje para la sesión de datos. Los PDSNs atienden a los usuarios locales y a los usuario que andan vagando, quienes se encuentran en una región o red particular, mientras que el HA siempre atiende a la misma serie de usuarios estipulados no importando si se encuentran enlazados a su red local o si están vagando fuera de ella. A este respecto, hay dos escenarios principales de asignación de HA a ser considerados: HA colocado y HA localizado en el centro.

7.6.1.1 PDSN/HA Colocado

En el escenario de asignación de HA colocado, existe más de una localización del HA en la red. Ya que todo el tráfico IP Móvil de usuario (al menos en el enlace ascendente) debe pasar a través de pares PDSN/HA.

La principal ventaja de este enfoque está en la capacidad de reaprovisionar grupos locales de PDSN/HA si la combinación del cliente cambia– esto es, el *roaming* contra la proporción en la que el cliente se encuentra en su red local- cambia. Por ejemplo, durante una muestra de negocios o cualquier otro evento profesional que acumula grandes grupos de usuarios con móviles asignados a HAs que sirven a otras localizaciones geográficas, más usuarios móviles de lo normal tendrán que ser atendidos por los PDSNs locales, los cuales tendrían que transportar el tráfico por túneles hacia HAs alrededor del mundo. Para manejar esta situación, los portadores que despliegan HAs colocados serán capaces de reaprovisionar fácilmente grupos locales de PDSN/HA para mayor capacidad del PDSN. Cuando el evento termina, el grupo puede ser cambiado a sus proporciones usuales.

Otra ventaja de este enfoque es para los portadores que esperan servir a grandes números de usuarios estacionarios en diferentes localidades de un país, como los portadores inalámbricos que compiten con las compañías telefónicas locales por los mercados de telefonía alámbrica local y de larga distancia. Ya que en tales redes no hay mucha movilidad, los usuarios usualmente permanecen dentro de las regiones cubiertas por HAs locales permitiendo a los operadores minimizar el uso de su red.

Finalmente, cuando son utilizados HAs colocados, cada grupo PDSN/HA puede utilizar más eficientemente sus capacidades de administración de direcciones siendo capaz de asignar direcciones IP a las estaciones móviles de los *pools* de direcciones IP proporcionadas localmente.

7.6.1.2 HA Localizado en el Centro

En el escenario del HA localizado en el centro, los HAs que atienden a todos los usuarios de IP Móvil en la red están localizados en una sola central de datos. Esta solución tiene algunas ventajas, especialmente para los operadores que atienden a los usuarios, una mayoría de los cuales son altamente móviles y a menudo cambian sus PDSNs, y por lo tanto deben ser terminados en su HA original. Las centrales de datos proporcionan mayor facilidad de

administración para los operadores, incluyendo aprovisionamiento, mantenimiento, y actualización. Además, ya que los recursos y las reservas disponibles son mejor compartidos en una localización centralizada que en sitios distribuidos. Otra ventaja es una mayor posibilidad de proporcionar balanceo de carga del HA que incluye todas las capacidades del HA, al contrario del balanceo de carga de pequeña escala dentro del grupo local del HA en el modelo del HA colocado.

7.6.1.3 Confiabilidad del HA

La confiabilidad del HA se vuelve especialmente importante en el modelo del HA localizado en el centro. Una estación móvil puede ser atendida por cualquier PDSN local disponible. En caso de que el PDSN falle, la estación móvil funciona similarmente al evento de re-localización del PDSN enviando mensajes que solicitan avisos hasta que un PDSN en estado de espera entra en servicio.

Los efectos de las fallas del HA sobre una estación móvil –en los escenarios de VPN de HA público y privado- son más profundos y puede tener consecuencias devastadoras para la conectividad de los datos de la estación móvil. En CDMA2000, cada estación móvil de IP Móvil está programada para acceder sólo a un HA específico. Esto significa que si el HA proporcionado con la direcciones IP de un cierto grupo de estaciones móviles falla, todas las estaciones móviles asociadas con éste no serán capaces de recibir el servicio de paquetes de datos. Para remediar la situación, la plataforma del HA debe incluir opciones extensivas contra fallas internas e inter-chasis, las cuales, por ejemplo, asociarían automáticamente las direcciones IP proporcionadas en el HA que falla a otro elemento de hardware dentro del grupo local del HA.

7.6.2 Asignación del HA Dinámico

En la actual arquitectura la estación móvil está codificada con la dirección de un HA particular, que es incluida en su petición de registro durante el procedimiento de inscripción del PDSN. Un HA estático es más simple de soportar, debido a que la dirección IP del HA es configurada dentro del nodo móvil y un secreto compartido estático puede ser utilizado por la extensión de autenticación MN-HA. Sin embargo un HA asignado dinámicamente, colocado o localizado cerca de un PDSN, puede proporcionar significante optimización de operación debido a la mayor disponibilidad del servicio y a rutas más óptimas en el caso cuando una estación móvil está vagando bastante lejos de su red local para hacer gastos sustanciales (por ejemplo, los datos desde un PDSN en Alaska no tendrían que ser enviados hacia y desde un HA en Texas cada vez que el usuario desee leer sus correos electrónicos desde un servidor de correo localizado en Seattle, si el HA posiblemente fue asignado dinámicamente a un agente local cercano).

La figura 7.16 detalla los pasos necesarios para asignar dinámicamente un HA.

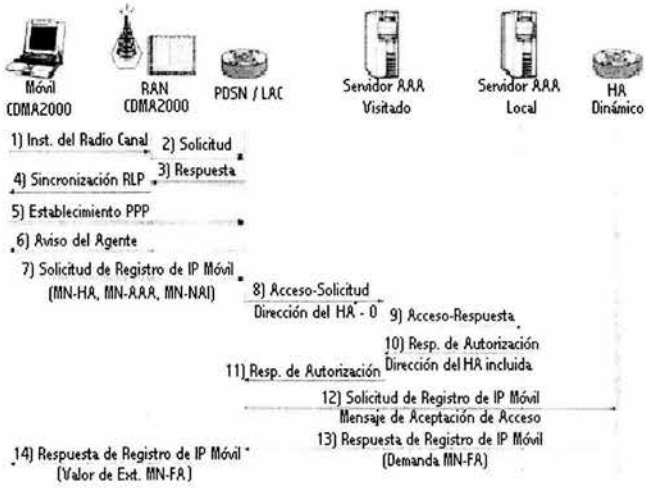


Figura 7.16 Establecimiento de la asignación de un HA dinámico

El establecimiento del HA dinámico requiere el desarrollo de un secreto compartido entre la estación móvil y el HA de modo que subsecuentemente los registros de movilidad puedan ser autenticados conforme la estación móvil cambia de PDSNs. En el caso de la asignación del HA dinámico, la dirección del HA está determinada por un servidor AAA y no por el mensaje de petición de registro de IP Móvil, como es el caso con la asignación estática del HA. Un servidor AAA local asigna dinámicamente un HA en una red privada del proveedor de servicio o en una red privada remota e informa su dirección a un servidor AAA visitado y un nodo PDSN, con secretos compartidos MN-HA dinámicamente distribuidos a la estación móvil y al HA para posterior autenticación. Estos secretos son protegidos criptográficamente por la red AAA en tránsito. El PDSN entonces devuelve estos valores a la estación móvil, la cual comienza a usar su nueva dirección local.

Para soportar la asignación dinámica de una dirección local, la estación móvil debe suministrar un NAI en su petición de registro IP Móvil. Este es un nombre único de la forma usuario@dominio que identifica al usuario que está solicitando servicio de la red. El nombre actúa como un identificador y no está asociado con la dirección IP del dispositivo. El NAI le permite a la red de servicio encontrar la red local (posiblemente localizada en una red privada) mediante una infraestructura AAA. Utilizando las extensiones solicitud/respuesta de IP Móvil, las credenciales de los usuarios pueden ser autenticadas por el dominio local. Una vez que el usuario es autenticado y es autorizado para recibir servicio en la red visitada, la estación móvil puede registrarse con el HA. Debido a que en una petición de registro aparece un NAI y no una dirección IP, el agente local puede entonces asignar una dirección local para el nodo móvil e informarle en la respuesta de registro.

7.7 Administración de la Dirección IP en CDMA2000

En esta sección se proporciona una visión de la administración de la dirección IP desde la perspectiva de un portador inalámbrico y desde la perspectiva de una red privada. Cuando una estación móvil se conecta a una red privada en el modo de IP Simple o en el modo de IP Móvil, ésta puede ser asignada a una dirección IP privada fuera del espacio de direcciones de la red privada. Debido a que una autoridad no global asigna tales direcciones, éstas pueden no ser globalmente encaminables o únicas. Esto es importante, sin embargo, para la arquitectura del PDSN de modo que pueda manejar convenientemente tal situación, esto es, el PDSN deber ser capaz de encaminar apropiadamente los paquetes hacia y desde los HAs aún cuando tengan

traslape de las direcciones privadas. Para realizar esto, el PDSN debe hacer uso de la dirección del HA en el encabezado IP exterior de los paquetes que pasan por el túnel y de la información de identificación de la capa de enlace en el lado de la red de acceso (esto es en la interfaz R-P) del PDSN para resolver potenciales colisiones en las direcciones IP asignadas a diferentes estaciones móviles.

7.7.1 Asignación de Dirección VPN en IP Simple

En CDMA2000, la asignación de la dirección en IP Simple es manejada por el nodo PDSN a no ser que sea requerido el servicio de VPN. Al contrario de IP móvil, el método de acceso IP Simple no permite que direcciones estáticas sean proporcionadas en la estación móvil. En vez de eso, la dirección IP debe ser asignada dinámicamente a la estación móvil, durante el inicio de PPP cuando la estación móvil se registra primero con el PDSN y envía una dirección IP 0.0.0.0 durante la fase IPCP para solicitar una dirección IP dinámica. La dirección asignada a la estación móvil puede ser una dirección privada o una dirección pública.

La siguiente lista bosqueja las opciones disponibles para la asignación de la dirección IP en IP Simple:

- Asignación desde un *pool* de direcciones configurado en el nodo PDSN o en un grupo del PDSN. El *pool* puede estar asociado estáticamente al usuario mediante una tabla de mapeo proporcionada en cada nodo PDSN, o el nombre del *pool* de direcciones puede ser devuelto al PDSN en el mensaje de aceptación de acceso de RADIUS por el servidor AAA.

- Asignación mediante el uso de un servidor AAA como RADIUS o DIAMETER cuando se ejecuta la autenticación de la estación móvil. La dirección es comunicada al cliente durante la negociación PPP.

- Asignación vía DHCP, lo cual requiere que el PDSN soporte un cliente DHCP.

Cuando es solicitado el servicio de VPN obligatoria en el modo IP Simple, la responsabilidad de asignar la dirección IP al móvil es transferida a la red privada. En este caso el enlace PPP es terminado y encapsulado dentro de un túnel L2TP y enviado al servidor LNS en la red privada.

7.7.2 Asignación de Dirección VPN en IP Móvil

AL igual que en el servicio de IP Simple, el proceso de asignación de dirección para el servicio de IP Móvil puede ser proporcionado mediante una variedad de opciones. Sin embargo, al contrario de IP Simple, las estaciones móviles que solicitan servicio de IP Móvil se les pueden proporcionar direcciones IP estáticas pre-configuradas. Cuando una dirección IP es asignada estáticamente a una estación móvil, ésta será propuesta al PDSN vía IPCP durante la negociación PPP. La asignación de la dirección para el servicio de IP Móvil en CDMA2000, y para IP Móvil en general, siempre es manejada por el agente local (HA).

Después de que la estación móvil es autenticada con el PDSN, puede solicitar direcciones IP públicas o privadas desde su HA. El HA responde, dentro del mensaje de Respuesta de Registro de IP Móvil, con la dirección IP que va a utilizar el móvil, la cual es enviada hacia la estación móvil por el PDSN.

Múltiples direcciones privadas que se traslapan son soportadas por el nodo PDSN por el estándar [IS835] de la TIA, mientras que las direcciones de cada HA son únicas y no se traslapan. Otra opción que distingue a IP Móvil de IP Simple es la capacidad para soportar múltiples direcciones IP en la estación móvil para soportar múltiples sesiones de comunicaciones entre el móvil y su red privada (algo similar al concepto de múltiples contextos PDP en las redes GPRS y UMTS).

Si la estación móvil requiere acceso a una dirección local privada, entonces tiene que negociar un túnel de regreso. Como resultado, el PDSN forma una asociación lógica que contiene el identificador de sesión R-P, la dirección local de la estación móvil, y la dirección del HA. Cuando el PDSN recibe un paquete de una estación móvil registrada desde el HA, el PDSN mapea la dirección del HA y la dirección local de la estación móvil para una asociación, y transmite el paquete sobre la conexión R-P indicada por el identificador de la sesión R-P.

7.8 Autenticación, Autorización, y Contabilidad Para el Servicio de MVPN

7.8.1 Arquitectura AAA de CDMA2000

En el capítulo 4 se describieron los conceptos básicos de AAA en el ambiente de CDMA2000, los cuales están basados en el uso de RADIUS y otros protocolos como CHAP y PAP. En esta sección se analiza con más detalle la arquitectura AAA de CDMA2000 y su impacto en los servicios de MVPN. Para satisfacer mejor los requerimientos para diferentes métodos de acceso a la red privada sin la necesidad de preestablecer acuerdos, ésta evolucionó hacia la forma de arquitectura AAA *visitada-corredor-local*, mostrada en la figura 7.17. Esta arquitectura fue desarrollada con un objetivo similar a GRX en la red GPRS, para facilitar una arquitectura de red que pueda ser compartida por muchas entidades privadas, que incluyen ISPs, ASPs, redes corporativas, y portadores inalámbricos.

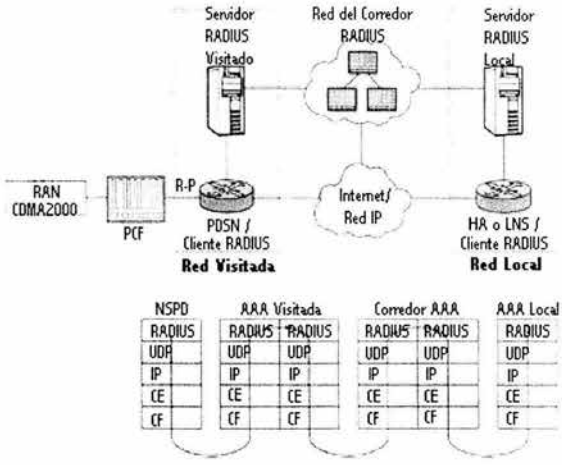


Figura 7.17 Arquitectura AAA basada en RADIUS de CDMA2000 y modelo de referencia del protocolo

La estación móvil que accede a una red privada a través de una red de acceso proporcionada por una entidad de terceros debe ser autenticada por ambas redes. Como resultado, la estación móvil es identificada en la red de acceso por su identificador (ID), tal como un Identificador Internacional de la Estación Móvil (IMSI), y es identificada en la red privada mediante un NAI. Como se muestra en la figura 7.17, tal autenticación requiere funcionalidad AAA en las redes visitada y local. En CDMA2000, esta funcionalidad es lograda a través de un cliente (usualmente recibido por el nodo PDSN) y un servidor AAA de RADIUS en la red visitada, y de un cliente (usualmente recibido por un HA para IP Móvil y un LNS para VPN por IP Simple) y un servidor AAA de RADIUS en la red local.

Además para autenticar y autorizar a la estación móvil en comunicaciones genéricas de CDMA2000, cuando es solicitado el acceso a la red privada, las peticiones de autenticación son

enviadas desde un servidor AAA *visitado* asociado con el PDSN hacia un servidor AAA *local* asociado con el HA, y las respuestas de autorización son enviadas en la otra dirección. La información de contabilidad debe ser almacenada por el servidor AAA visitado y opcionalmente puede ser enviada al servidor AAA local y entonces se manda al sistema de facturación. Para el servicio de VPN, la información de contabilidad puede incluir parámetros como el NAI, QoS, el identificador de la sesión para el servicio de IP Simple, y la dirección destino.

Este modelo es fundamentalmente similar para VPN por IP Simple y para VPN por IP Móvil. La comunicación entre los clientes y los servidores RADIUS puede ser asegurada con IPSec para proporcionar una asociación de seguridad entre la estación móvil, el PDSN, y el HA (o LNS en el caso de IP Simple) y soportar la distribución dinámica de claves que usa IKE.

7.8.2 Comisión AAA en CDMA2000

La infraestructura AAA local/visitada fue diseñada para atender a las redes local y visitada con las relaciones preestablecidas mediante una serie de acuerdos SLAs. En los casos donde tales relaciones no han sido establecidas pero la estación móvil visitante solicita servicio de datos, debe ser utilizado la comisión AAA. Los servidores AAA local y visitado pueden tener una relación bilateral directa. La arquitectura celular, sin embargo, implicará miles de dominios con muchas redes privadas poseídas por empresas que buscan el servicio inalámbrico de datos para su fuerza de trabajo móvil. Si el número de dominios fuera pequeño, las redes local y de servicio podrían tener relaciones preexistentes. Sin embargo, esta no sería una solución escalable; esto requeriría que demasiadas relaciones fuesen preestablecidas.

Los corredores AAA tienen directorios que les permiten que las peticiones AAA sean enviadas en base al NAI a las redes locales o a otros corredores que conocen en qué parte se encuentra la red local. Los corredores pueden también adquirir un papel financiero en el establecimiento de cuentas entre los dominios y pueden procesar los registros de contabilidad para las peticiones del acceso de red que autorizan. Debido a que la red visitada no proporcionará servicio a menos que pueda obtener la autorización de la red local del usuario móvil, o de un corredor que acepte la responsabilidad financiera, la infraestructura AAA debe ser confiable. Esto implica que los servidores deben retransmitir las peticiones y conmutarlas a otros servidores de reserva cuando se detecta una falla de la unidad primaria.

Las redes AAA deben soportar tres modos de operación del corredor:

- Modo no transparente, donde los corredores esencialmente terminan las peticiones hacia y desde los servidores AAA visitado y local e inician nuevas peticiones. En este modo se le permite al corredor cambiar el contenido y los atributos de los mensajes.

- Modo transparente, donde el corredor no está autorizado para realizar algún cambio a los mensajes AAA y sólo se le permite redireccionarlos hacia los puntos destino apropiados.

- Modo de redirección, donde el servidor AAA del corredor refiere al proveedor de servicio hacia otro servidor AAA.

Otra importante tarea de un corredor AAA es facilitar los servicios de *roaming*. Los servicios de *roaming* permiten a los usuarios móviles salir del área de cobertura de su portador para usar las redes de otros portadores para acceder a Internet o a otras redes privadas.

7.8.3 Perspectiva de VPN en IP Móvil

En el caso de VPN por IP Móvil, cuando una estación móvil accede a un HA en la red privada, el proveedor de acceso inalámbrico (el dueño del nodo PDSN) no debe estar involucrado en la asociación de seguridad entre la estación móvil y su red local. Con el atributo de Nivel de Seguridad TIA en los mensajes de Aceptación de Acceso, el servidor AAA local es capaz de

autorizar al PDSN sobre una base por-usuario para utilizar opcionalmente IPSec en los mensajes de registro y en los datos que pasan por el túnel.

Si el servidor AAA local ha indicado que una asociación de seguridad IP debe ser usada entre el PDSN y el HA, el PDSN proporcionará servicios de IPSec. Si la asociación de seguridad no toma lugar, el PDSN intenta establecerla usando el certificado HA X.509. Si el certificado HA X.509 no existe, pero si existe el certificado raíz, el PDSN intenta establecer la asociación de seguridad que utiliza los certificados X.509 que recibió en la Fase 1 de IKE. Si los certificados no existen, el PDSN intenta usar el secreto compartido distribuido dinámicamente por IKE que recibió en el mensaje de Aceptación de Acceso. Si no fue enviado el secreto, el PDSN intenta usar el secreto pre-compartido IKE configurado estáticamente. Si el PDSN no recibe el atributo de nivel de seguridad del servidor RADIUS local, y existe una asociación de seguridad IPSec hacia el HA, el PDSN continua usando la misma asociación de seguridad. Si no existe la asociación de seguridad, entonces el PDSN sigue la política de seguridad configurada localmente.

7.8.4 Perspectiva de VPN en IP Simple

Para el modo de acceso VPN por IP Simple, la arquitectura AAA no incluye el HA. Esta funcionalidad es soportada por el servidor LNS. El servidor AAA debe localizar al servidor LNS que proporciona acceso a la red local del usuario. Después de que el LNS es localizado, es establecido un túnel L2TP entre el LNS y el PDSN desde el cual la estación móvil solicita los servicios. La dirección IP del móvil es asignado por el LNS después del establecimiento del túnel. Ya que la estación móvil no participa en las decisiones de ruteo entre los puntos finales del túnel, pueden ser asignadas al nodo móvil las direcciones IP registrada y no registrada. Si está involucrado el servicio de *roaming*, el servidor AAA visitado graba el registro de contabilidad y envía el mensaje de Solicitud de Contabilidad al servidor AAA local.

Cuando una estación móvil de IP Simple inicia la conexión al PDSN, el PDSN forma un mensaje de Solicitud de Acceso y lo envía hacia el servidor AAA local para la autenticación. La solicitud es autenticada positivamente y un mensaje de Aceptación de Acceso que contiene el tipo de túnel L2TP es enviado de regreso a la AAA visitada. El nodo PDSN inicia el túnel L2TP si éste no ha sido establecido, y envía un mensaje de Solicitud de Contabilidad para propósitos de facturación para registrar el tiempo de inicio del servicio. Cuando el servicio no es requerido más, la sesión del usuario y el túnel L2TP son terminados. Finalmente, el PDSN envía otro mensaje de Solicitud de Contabilidad para registrar el tiempo en el que el servicio es detenido.

CAPÍTULO 8

ESTADO ACTUAL Y TENDENCIAS EN LOS ESTÁNDARES DE DATOS INALÁMBRICOS

No hay duda que la interoperabilidad y las soluciones basadas en múltiples vendedores son una de las exigencias claves del mercado en la industria de las telecomunicaciones hoy. En particular, la conformidad con los estándares siempre ha sido uno de los requisitos principales para las soluciones de MVPN, ya que potencialmente se extienden sobre múltiples redes (acceso, tránsito ISP, cliente) y están intrínsecamente ligadas a la interoperabilidad entre los dispositivos de acceso inalámbrico y la infraestructura de la red de acceso para permitir roaming global.

La necesidad de producir estándares para el advenimiento de la siguiente generación de sistemas inalámbricos apuntaló la fundación de varias Organizaciones de Definición de Estándares (SDOs, *Standard Definition Organizations*) durante los años pasados. Los requerimientos de los sistemas inalámbricos de la tercera generación fueron originalmente definidos por la ITU (*International Telecommunications Union*) dentro del marco de IMT-2000 (*International Mobile Telecommunications*). Aparte de definir algunos requerimientos tecnológicos y del espectro para las tecnologías de radio transmisión que serían consideradas candidatas para los servicios 3G, el marco de IMT-2000 definió requerimientos de servicio tales como el soporte de roaming global.

Esto forzó a todas las partes (fabricantes y operadores) implicados a establecer estándares para desarrollar los cuerpos de estandarización en un nivel global. El resultado fue la creación de la organización 3GPP (*Third-Generation Partnership Project*) y más tarde la fundación de una organización espejo llamada 3GPP2.

8.1 Organizaciones Regionales de Estandarización

Aparte de las organizaciones internacionales como la ITU, que no tenía casi ninguna influencia sobre la definición de los sistemas celulares inalámbricos, cada región en el mundo tenía sus propios cuerpos de estandarización dedicados a estas tecnologías.

El sistema GSM en el espectro de 900 y 1800 MHz fue definido por el ETSI (*European Telecommunications Standards Institute*) y más tarde fue también adoptado por el comité T1-P1 de la TIA (*Telecommunications Industry Association*) en Norteamérica para el espectro de 1900 MHz (dedicado a PCS, *Personal Communications Services*). La TIA ha definido también un sinnúmero de otros sistemas celulares en la región de Norte América, tanto analógicos como digitales. Japón, en contraste con el resto del mundo, definió su propio sistema digital celular llamado Comunicaciones Personales Digitales (PDC, *Personal Digital Communications*). Los cuerpos japoneses de estandarización son la Asociación de Industrias de Radio y Negocios (ARIB, *Association of Radio Industries and Businesses*) y el Comité de Tecnología de Telecomunicaciones (TTC, *Telecommunication Technology Committe*). Estos cuerpos de estandarización también influyen en la toma de decisiones en el resto del Borde del Pacífico -con excepción de Corea y China, que tienen sus propias organizaciones (la Asociación de Tecnología de Telecomunicaciones Coreana y el Grupo de Estándares de Telecomunicaciones Inalámbricas de China, respectivamente).

Cada una de estas organizaciones definía estándares regionales incompatibles con los estándares definidos por otras organizaciones, a excepción del sistema GSM de 1900 MHz, que permitiría a los clientes de GSM 900 y 1800 vagar a Norte América usando un teléfono para las tres bandas. Estaba claro que este modelo no podía trabajar más, y se despertó la necesidad de estandartizar los sistemas 3G garantizando roaming global. En un mundo ideal, una nueva organización que definiera un solo sistema para el mundo entero habría sido una solución lógica. Desde luego, no vivimos en un mundo perfecto. En cambio, la asignación del espectro para los servicios 3G en

Europa y Japón fue en la región de 1900 a 2100 MHz, que fue ya parcialmente usada por los servicios PCS en la región de Norte América. Esta situación, junto con caminos de migración diferentes hacia 3G y las diferentes tecnologías de redes principales usadas en los sistemas GSM europeo y CDMA norteamericano existentes, condujo a incompatibilidades mutuas aún más profundas, y no completamente por casualidad, directamente se dio el nacimiento de dos Organizaciones de Definición de Estándares distintas para los sistemas de la tercera generación: 3GPP y 3GPP2.

8.1.1 3GPP

3GPP es un acuerdo entre cuerpos regionales de estándares de telecomunicaciones conocidos como Socios Organizacionales (*Organizational Partners*). Actualmente, los socios de 3GPP son la ARIB, el Grupo de Estándares de Telecomunicaciones Inalámbricas de China (CWTS), el ETSI, el T1, la Asociación de Tecnología de Telecomunicaciones (TTA), y el Comité de Tecnología de Telecomunicaciones (TTC). 3GPP fue creado en Diciembre de 1998 cuando los socios firmaron el Acuerdo del Proyecto de Asociación de la Tercera Generación. Cualquier compañía puede ser un miembro de 3GPP disponiendo que conoce las reglas definidas para la asociación 3GPP.

Una segunda categoría de la asociación se creó dentro del proyecto: *socios de representación del mercado*. Estos son organizaciones y grupos de la industria conducidos por objetivos basados en necesidades a largo plazo de sus compañías miembro. En una cierta etapa, estos socios deciden que es importante tener un 3GPP que escuche su opinión como un grupo, antes que difundir esta opinión vía las compañías miembro individuales. Uno de estos grupos, el grupo foco de la industria 3G.IP, ha sido especialmente influyente en manejar la estandardización de la evolución de las especificaciones del sistema 3GPP hacia un sistema multimedia basado en IP.

El objetivo intencionado de 3GPP fue definir especificaciones técnicas y reportes técnicos para un Sistema Móvil 3G basado en una evolución de la red central de GSM. Este incluyó las tecnologías de acceso de radio que fueron seleccionadas para servicios 3G basados en la red central de GSM: Acceso de Radio Terrestre Universal (UTRA, *Universal Terrestrial Radio Access*) basado en W-CDMA en sus modos Doble División de Frecuencia (FDD) y Doble División de Tiempo (TDD). Más tarde se hizo evidente que tendría sentido ampliar el alcance de 3GPP para incluir las especificaciones técnicas y reportes técnicos de mantenimiento y evolución de GSM, y las tecnologías de acceso de radio y servicios relacionados, GPRS (*General Packet Radio Service*) y EDGE (*Enhanced Data rates for GSM Evolution*). Ahora 3GPP ha asumido los papeles de los cuales el ETSI había sido responsable.

El trabajo de 3GPP está organizado en Grupos Técnicos de Estandarización (TSGs, *Technical Standardization Groups*), que por su parte están organizados en Grupos de Trabajo (WGs, *Working Groups*). Las reglas de operación de un TSG son especificadas en el reporte técnico 3G TS 21.900 "Métodos de Trabajo del Grupo Técnico de Especificación".

La siguiente es la lista de TSGs actuales que comprenden 3GPP:

TSG-SA (Sistema y Arquitectura) define los aspectos de los sistemas y coordina el trabajo técnico de todos los demás grupos desde una perspectiva de sistemas. Este incluye cinco Grupos de Trabajo:

- SA1 maneja los requerimientos.
- SA2 Systems maneja la arquitectura de los sistemas.
- SA3 maneja la seguridad.
- SA4 Voice maneja la codificación multimedia.
- SA5 maneja la carga.

TSG-CN (Red Central) especifica la evolución de la red central.
Hay cinco Grupos de Trabajo dentro del TSG CN:

- CN1 maneja los protocolos entre el equipo de usuario (UE, también conocido como terminal, teléfono móvil, o estación móvil) y la red central [específicamente el nodo en la red central que dialoga con las terminales para manejar la movilidad de la terminal y permite a la estación móvil (MS) hacer y recibir llamadas].
- CN2 especifica la interacción de la red móvil con la funcionalidad y servicios de la red inteligente.
- CN3 define el interfuncionamiento de la red móvil con redes externas, como la red PSTN, o redes de paquetes de datos, como Internet.
- CN4 especifica los protocolos de la red central.
- CN5 especifica la aplicación de programación de interfaces y los protocolos usados para tener acceso a los servicios de red de proveedores de aplicación de terceros.

TSG-RAN (Radio Acceso de Red) define la Red de Acceso de Radio Terrestre UMTS (UTRAN). Está formado de cuatro Grupos de Trabajo:

- RAN-1 está dedicado a la especificación del protocolo de la capa física de radio.
- RAN-2 maneja la especificación de la capa de radio enlace.
- RAN-3 define la interfaz Iu (es decir, la interfaz entre la red de radio acceso y la red central).
- RAN-4 maneja los aspectos de radio.

TSG-GERAN (Evolución de la Red de Radio Acceso de GSM) define las especificaciones para la evolución de la red de radio acceso de GSM (GSM RAN). Está compuesto de cinco Grupos de Trabajo:

- GERAN1 está dedicado a los aspectos de radio.
- GERAN2 maneja los aspectos de los protocolos.
- GERAN3 está dedicado al subsistema de la estación base de GSM.
- GERAN4 especifica los aspectos de radio de las terminales.
- GERAN5 dirige los aspectos de los protocolos en las terminales.

TSG-T (Terminales) especifica los aspectos de las terminales. Éste incluye tres Grupos de Trabajo:

- T1 maneja las especificaciones para la interoperabilidad.
- T2 especifica las capacidades de las terminales.
- T3 especifica el módulo de identidad del suscriptor (SIM, *Subscriber Identity Module*) de UMTS, que es una tarjeta con chip que permite la autenticación de la identidad del suscriptor, la portabilidad de la terminal, y la ejecución de aplicaciones simples.

Un Grupo de Coordinación del Proyecto (PCG, *Project Coordination Group*) tiene el papel de determinar las reglas de operación y definir los procedimientos trabajo.

Las especificaciones de 3GPP son pronunciadas en *liberaciones*. Inicialmente, el ETSI liberaba especificaciones cada año y les asignaba nombres. La primera liberación de las especificaciones de UMTS fue nombrada Liberación 99 (R99). Más tarde, tan pronto como el plan de desarrollo de la liberación 2000 siguiente tuvo que ser articulado, se tomó la decisión para levantar la sujeción que ataba los lanzamientos de las especificaciones 3GPP a un año, y en cambio usar las liberaciones basadas en funcionalidad. Ahora las liberaciones 3GPP son nombradas con un número de liberación diferente del año en que la liberación fue publicada, comenzando a partir del año 2000. La primera liberación bajo este nuevo nombramiento por convención fue nombrada Liberación 4 (R4), la segunda Liberación 5 (R5), etc. La cuenta comenzó desde 4 porque la especificación del número de versión fue 3.x.y (donde x e y son figuras genéricas) para la Liberación 99, y la decisión fue hecha para incrementar el primer número en el número de versión de una especificación en cada liberación.

La Liberación 99 define las características básicas de UMTS asociadas con los servicios de conmutación de circuitos y conmutación de paquetes que UMTS proporciona. La Liberación 4 mejora la parte de servicios de circuitos del sistema para usar los últimos desarrollos en las tecnologías de *gateways* y controladores de *gateways*, y la Liberación 5 introduce el soporte de servicios multimedia sobre la parte de conmutación de paquetes.

La Liberación 6 (R6) introducirá, además de otras características, capacidades de *multicast* y *broadcast* para lograr que la entrega de contenidos de *multicast* sea viable económicamente.

8.1.1.1 Documentos y Proceso de Estandarización de 3GPP

3GPP produce especificaciones que resultan en dos series dentro de documentos permanentes: reportes técnicos (TRs) y especificaciones técnicas (TSs). Un reporte técnico es un documento permanente que registra la actividad de un Grupo de Trabajo, así como la investigación sobre la posibilidad de introducir algunas características en las especificaciones. Una especificación técnica es el documento actual que especifica el funcionamiento de los nodos de la red y la definición de los protocolos empleados en sistemas 3GPP. Los tres tipos de especificaciones técnicas son los siguientes:

- Escenario 1 especificaciones del esquema de servicios y de los requerimientos funcionales y están basadas en el consumo de los operadores. SA1 es el Grupo de Trabajo dentro de TSG-SA que normalmente genera todos los documentos del escenario 1 para 3GPP.

- Escenario 2 especificaciones de los requerimientos a nivel de sistema y a nivel de arquitectura que los protocolos especificados por 3GPP deben satisfacer. Estos son los documentos donde todas las estrategias de dirección y las políticas de decisiones son formalizadas. Normalmente, SA2 dentro de TSG toma el papel de generar los documentos de más alto nivel del escenario 2, mientras que cuando más competencia específica es requerida sobre el nivel de protocolos, otros Grupos de Trabajo definen los documentos del escenario 2.

- Escenario 3 documentos donde están las actuales especificaciones de los protocolos 3GPP.

La generación de una especificación técnica es un proceso formal. En la primer fase, las compañías interesadas, guiadas por un documento de conformidad o grupo de conformidades, contribuyen enormemente para generar un primer expediente del documento. El documento es generado por un Grupo de Trabajo mediante consensos. Después de la aprobación, el documento es promovido hacia un nivel más alto de estabilidad. El Grupo de Trabajo somete de nuevo el documento al pleno del TSG, sugiriendo que es lo suficientemente estable para entrar al cambio de fase. En esta etapa del tiempo de vida de un documento, las compañías pueden cambiar el documento sólo sometiéndolo a una solicitud formal de cambio (CR). Una especificación pertenece en cualquier tiempo dado a una liberación. Cuando una liberación es congelada, los cambios a un documento solo pueden ser aprobados por consenso general o porque habría problemas serios en la operación del sistema si el documento no se cambia. Un documento puede desarrollarse sobre un número de liberaciones, hasta que el 3GPP decida retirar una especificación que comienza desde una liberación 3GPP.

Los documentos (mejor conocidos como documentos temporales) sometidos por las compañías interesadas son discutidos en las juntas de los Grupos de Trabajo. Una serie de documentos son el resultado de consensos de las juntas de los Grupos de Trabajo. Esta serie de documentos es enviada al pleno del TSG, donde normalmente son aprobados. Cuando los documentos son aprobados por el pleno del TSG, el contenido es normalmente transferido a un documento permanente. Entonces, después cada número de versión de los documentos bajo el control de un TSG cambia.

8.1.2 3GPP2

3GPP2 es un acuerdo de colaboración entre las organizaciones de definición de estándares interesadas en desarrollar especificaciones para los sistemas 3G que evolucionan de la red central basada en ANSI-41, instalado en Febrero de 1999 por la misma razón que guió a la creación de 3GPP para la definición de especificaciones para sistemas 3G que evolucionan de la red central basada en GSM. Los socios que actualmente son miembros de 3GPP2 son ARIB, CWTS, TIA, TTA, TTC, y los Socios de Representación de Mercado (MRP, *Market Representation Partners*).

Al igual que 3GPP, 3GPP2 sintió la necesidad de permitir al mercado la entrada a sus actividades de estandarización. Los MRP de 3GPP2 son organizaciones que pueden ofrecer dictámenes del mercado y traer hacia 3GPP2 una visión consensada de los requerimientos del mercado (por ejemplo, servicios, características, funcionalidad) que caen dentro del alcance de 3GPP2.

La siguiente es una lista de los actuales MRPs:

- El Grupo de Desarrollo de CDMA (CDG).
- El Foro de Internet Inalámbrico Móvil (MWIF).
- El Foro de IPv6.

En particular, el MWIF ha estado proponiendo fuertemente la evolución de las especificaciones de los sistemas 3GPP2 hacia un sistema multimedia basado en IP (al igual que 3G.IP en 3GPP). La operación de 3GPP2 está guiada por el Comité de Iniciativas (*Steering Committee*). El trabajo actual en 3GPP2 es desempeñado por los TSGs. Los TSGs responsables de la generación de documentos de especificaciones técnicas de 3GPP2 son los siguientes:

- TSG-A (Interfaz de la Red de Acceso) es responsable de las especificaciones de las interfaces entre la red de radio acceso y la red central, así como también dentro de la red de acceso para las capacidades como *handoff*.

- TSG-G (CDMA 2000) es responsable de la parte de acceso de radio, incluyendo la estructura interna de los sistemas basados en especificaciones 3GPP2. Específicamente, es responsable de los requerimientos, funciones e interfaces para la infraestructura CDMA 2000 y el equipo terminal del usuario. Éste incluye las especificaciones de la capa de radio, las especificaciones de desempeño de las estaciones base y móviles y las especificaciones de prueba, soporte para mejorar la privacidad, la autenticación y la encriptación, y codificadores digitales de voz y video. También dirige las interfaces estación móvil- adaptador y otras interfaces auxiliares.

- TSG-N (ANSI-41, Red Inalámbrica Inteligente) es responsable de las especificaciones de la red central de los sistemas basados en especificaciones 3GPP2. Éstas incluyen las interfaces internas de la red central para la señalización de llamadas asociadas y llamadas no asociadas, y la evolución de la red central para la operación inter-sistemas dentro de la familia ANSI-41, procedimientos VHE (*Virtual Home Enviroment*), soporte del módulo de identificación del usuario (UIM), y soporte para mejorar la privacidad, la autenticación, la encriptación, y otros aspectos de seguridad.

- TSG-P (Redes inalámbricas de Paquetes de Datos) es responsable de las especificaciones para redes inalámbricas de paquetes de datos para sistemas 3GPP2. Éstas incluyen servicios IP inalámbricos (incluyendo gestión de la movilidad IP), diseño de la arquitectura de las redes IP inalámbricas, voz sobre IP, Internet público y acceso privado seguro a la red, contabilidad de paquetes de datos, multimedia, y métodos de calidad de servicio (QoS). Este grupo está fuertemente influenciado por los MRPs de igual manera que por el MWIF. Un TSG *All IP* ha sido creado para satisfacer los requerimientos del MWIF para un sistema basado en *All IP*.

- TSG-R (Interfaz de la tecnología de acceso de radio de 3GPP para la red central 3G evolucionando de ANSI-41) es responsable de la especificación de la Función de Interfuncionamiento (IWF) para la interfaz de acceso de radio de 3GPP2 (es decir, UTRAN). Además maneja el *handoff* entre las tecnologías de radio cdmaOne y UTRAN y el *roaming* entre las redes centrales de ANSI-41 y de GSM.

- TSG-S (Aspectos de sistemas y servicios) es responsable del desarrollo de los requerimientos de la capacidad de servicio para los sistemas basados en especificaciones 3GPP2. También es responsable de cuestiones de la arquitectura, así como también es requerido para coordinar el desarrollo de servicios a través de varios TSGs.

8.1.2.1 Documentos y Proceso de Estandarización de 3GPP2

3GPP2 produce especificaciones y reportes técnicos similarmente a 3GPP. El TSG-S define las características y requerimientos del sistema. Éstos, de igual manera que en 3GPP, son referidos como requerimientos del Escenario 1. Los reportes técnicos y las especificaciones técnicas son desarrollados dentro de los TSGs. Las especificaciones son desarrolladas en dos escenarios:

- Escenario 2 es una descripción de alto nivel de la implementación de una característica o servicio en la arquitectura 3GPP2, incluyendo mensajes de diagramas de flujo.

- Escenario 3 es el texto y la información asociada para la especificación técnica final.

Una vez que una especificación o reporte está técnicamente estable y completo, el TSG aprueba el documento como *texto de línea de base*. El documento pasa por un proceso de verificación y validación (*V&V*). Una vez que ha pasado este proceso *V&V*, el documento puede ser aprobado para su publicación por el TSG.

Después de que un TSG aprueba un documento, éste manda el documento a la Secretaría de 3GPP2. La Secretaría de 3GPP2 abre un periodo de 15 días para recibir comentarios. Si no se recibe ningún comentario, el documento es publicado como una publicación oficial de 3GPP2. Los Socios Organizacionales (TIA, TTC) subsecuentemente pueden manejar el documento de acuerdo con procesos de aprobación de estándares regionales. Una vez que esta revisión está completa, algunos cometarios son enviados al TSG 3GPP2 original. El documento pasa entonces por un proceso de actualización. El documento actualizado es entonces alineado, sujeto al proceso *V&V* y aprobado por el TSG como es necesario. Y el proceso anteriormente descrito se repite.

8.2 Cuerpo de Tarea de Ingeniería de Internet (IETF, *Internet Engineering Task Force*)

Ya que la mayoría de las aplicaciones de datos en redes inalámbricas están basadas en IP, no es ninguna sorpresa que el IETF y los protocolos que éste especifica se vuelvan cada vez más relevantes para la industria inalámbrica de datos. El IETF está organizado en áreas que organizan técnicamente todo lo relacionado a los Grupos de Trabajo. Las áreas actuales del IETF son las siguientes:

- *Área de Aplicaciones* trata con aplicaciones y protocolos de aplicación semejantes a la presencia y mensajería instantánea, el protocolo de tiempo de red, calendarización y planeación.
- *Área General* maneja tópicos relacionados con la operación general del IETF, tales como reglas de instalación.
- *Área de Ruteo* especifica los protocolos de ruteo y su aplicabilidad.
- *Área de Internet* define los problemas relacionadas con el protocolo IP, tales como la definición de su evolución, el soporte de servicios de red como PPP, y configuración IP de terminales. Recientemente, ésta tomó el papel de especificar el protocolo de IP móvil.

- *Área de Operaciones y Administración* define los aspectos relacionados a la gestión de la red y los protocolos, tales como el protocolo SNMP (*Simple Network Management Protocol*) y su evolución.
- *Área de Seguridad* maneja aspectos de seguridad en Internet.
- *Área Sub-IP* está dedicada a la definición de tecnologías y protocolos que normalmente están localizados en una capa abajo de la de IP en el *stack* de protocolos y están enfocados a la provisión de servicios como VPNs, ingeniería de tráfico, y transporte o hasta emulación de circuitos.
- *Área de Transporte* es responsable de la definición de los problemas relacionadas con el transporte, como QoS, protocolos a nivel de transporte, y control de la congestión.

Cada una de estas áreas es dirigida por uno o dos directores de área. Los directores de área y el jefe del IETF son miembros del IESG (*Internet Engineering Steering Group*), los cuales tienen el papel de evaluar la calidad de los estándares y pueden influir fuertemente en la transición de un expediente de Internet al estado de los estándares RFC propuestos, devolviéndolo al Grupo de Trabajo hasta que alcance un nivel adecuado de calidad para ser publicado.

8.2.1 Documentos y Proceso de Estandarización del IETF

El proceso de estandarización del IETF es muy diferente al de 3GPP. Primero, ninguna compañía puede oficialmente ser miembro del IETF. La membresía al IETF solo es permitida a ingenieros, científicos o estudiantes interesados en la evolución del Internet. Estos individuos, sin embargo, son a menudo patrocinados por compañías y organizaciones, cuyos intereses son por lo tanto indirectamente representados. Segundo, no hay un proceso formal de evaluación del documento. Cuando un individuo juzga que algo es necesario para añadir funcionalidad a Internet, debe presentar un expediente de Internet al Grupo de Trabajo del IETF relevante. Si no existe el Grupo de Trabajo apropiado, los individuos interesados pueden instalar uno con la aprobación del IESG, pasando primero alrededor de una discusión para medir por consenso la necesidad del Grupo de Trabajo y su alcance. Normalmente esto toma lugar en una reunión del IETF. Debe notarse que una vez que un Grupo de Trabajo es establecido, los individuos pueden someter los expedientes de Internet y discutirlos sobre una lista de direcciones del Grupo de Trabajo. Todas las decisiones son tomadas sobre la lista de direcciones, basadas en las evidencias de consensos y algunas pruebas que testifiquen que el protocolo que está siendo desarrollado realmente trabaja.

Una vez que el Grupo de Trabajo está suficientemente feliz con un expediente de Internet desarrollado por enmiendas de la lista de direcciones, el Grupo de Trabajo somete el expediente al IESG para su revisión. Cuando el IESG no tiene ningún comentario, el documento es publicado como un documento de Solicitud de Comentarios (RFC). Un documento RFC puede ser un documento informacional, el cual documenta algo sobre lo que los grupos de individuos hacen o un protocolo que emplean, o un documento de algún estándar.

Además, hay diferentes niveles de documentos del *track* de estándares. Inicialmente, un *track* de estándares RFC es un estándar propuesto. Entonces, después de algunos años de experiencia operacional y con la evidencia de al menos dos implementaciones independientes interoperables, un RFC puede llegar a ser un expediente estándar. Un expediente RFC estándar normalmente es un documento muy estable. Después de muchos años de operación, el IETF puede decidir promover un expediente RFC estándar al estado de estándar de Internet. Otras veces, cuando el protocolo se convierte obsoleto y no es muy ampliamente usado, el RFC puede convertirse en "histórico". Algunas veces, si un Grupo de Trabajo o el IESG necesita publicar algunas reglas o prácticas usadas en Internet o en el IETF, ellos publican un RFC BCP (*Best Current Practice*).

8.3 El Comité de Estándares LAN/MAN IEEE 802

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) define estándares para las redes de área local en el comité de estándares IEEE P802 LAN/MAN, que forma parte de la Asociación de Estándares del IEEE (IEEE-SA). En años recientes, el Grupo de Trabajo IEEE 802.11 definió un

estándar para las redes LAN inalámbricas (WLANs), conocido como el estándar 802.11. Esta es una muy prometedora serie de estándares, y es un serio competidor para las tecnologías 3G sirviendo al acceso de red en áreas de situación crítica (*hot-spot*) como aeropuertos, hoteles y centrales camioneras. El Grupo de Trabajo IEEE 802.11 está organizado en Grupos de Tareas (TGs). Cada Grupo de Tareas se encarga de la estandarización de un aspecto particular de la tecnología WLAN.

La siguiente es una lista de los Grupos de Tareas 802.11:

Grupo de Tareas MAC. El objetivo del proyecto es desarrollar una capa MAC común para aplicaciones WLAN, trabaja en conjunción con el Grupo de Tareas PHY. Su trabajo ha sido completado en la versión ISO/IEC del estándar original, publicado como 8802-11: 1999 (ISO/IEC) (*IEEE Std. 802.11, 1999 Edition*).

Grupo de Tareas PHY. El objetivo del proyecto es desarrollar tres capas físicas para aplicaciones WLAN, que usan Infrarrojo (IR), espectro expandido por salto de frecuencia (FHSS) en 2.4 GHz, y espectro expandido por secuencia directa (DSSS) en 2.4 GHz, en conjunción con el trabajo del Grupo de Tareas MAC. Su trabajo ha sido completado en la versión ISO/IEC del estándar original, y publicado como 8802-11: 1999 (ISO/IEC) (*IEEE Std. 802.11, 1999 Edition*).

Grupo de Tareas a. El objetivo del proyecto es desarrollar una capa física para operar en la nuevamente asignada banda UNII. Su trabajo ha sido completado en la versión ISO/IEC del estándar original como una reforma, y publicado como 8802-11:1999 (E)/Amd 1: 2000 (ISO/IEC) (*IEEE Std. 802.11a-1999 Edition*).

Grupo de Tareas b. El objetivo del proyecto es desarrollar un estándar para una capa física de tasa más alta en la banda de 2.4 GHz. Su trabajo ha sido completado y ahora forma parte del estándar como una reforma, y se publicó como *IEEE Std. 802.11b-1999*.

Grupo de Tareas b-cor1. El objetivo de este proyecto es corregir las deficiencias en la definición MIB (*Management Information Base*) del 802.11b.

Grupo de Tareas c. Este proyecto dirige una subcláusula bajo *2.5 Support of the Internal Sub-Layer Service* por procedimientos MAC específicos para cubrir la operación de puente con las MACs de IEEE 802.11. Este suplemento para ISO/IEC 10038 (IEEE 802.1D) fue desarrollado por el Grupo de Trabajo 802.11 en cooperación con el Grupo de Trabajo IEEE 802.1. El trabajo ha sido completado y es ahora párte del estándar ISO/IEC 10038 (IEEE 802.1).

Grupo de Tareas d. Este suplemento definirá los requerimientos de la capa física (canalización, patrones de salto, nuevos valores para los atributos actuales de MIB, y otros requerimientos) para extender la operación de 802.11 WLANs hacia nuevos dominios.

Grupo de Tareas e. Este grupo espera mejorar el Control de Acceso al Medio (MAC) 802.11 y la gestión de la calidad de servicio (QoS), proporciona clases de servicio, y mejora los mecanismos de seguridad y autenticación. Considera la eficiencia de mejoramientos en las áreas de Función de Coordinación Distribuida (DCF) y Función de Coordinación de Punto (PCF). Estos mejoramientos, en combinación con los recientes perfeccionamientos en las capacidades de PHY de 802.11a y 802.11b, incrementarán en gran medida la ejecución del sistema, y expande el espacio de aplicaciones para 802.11. Ejemplos de aplicaciones incluyen transporte de voz, audio y video sobre redes inalámbricas 802.11, videoconferencias, distribución de medios, mejoramiento de las aplicaciones de seguridad, y aplicaciones de acceso móvil y de acceso "nómada".

Grupo de Tareas f. Este grupo desarrolla prácticas para un protocolo de puntos de interacceso (IAPP, *Inter-Access Point Protocol*), el cual proporciona las capacidades necesarias para conseguir interoperabilidad de los puntos de acceso de múltiples vendedores a través de un Sistema de Distribución soportando enlaces IEEE P802.11 WLAN.

Grupo de Tareas g. El objetivo de este proyecto es desarrollar una extensión PHY de velocidades más altas para el estándar 802.11b. El nuevo estándar deberá ser compatible con el IEEE 802.11 MAC. La máxima tasa de datos de la capa física para este proyecto deberá ser de al menos 20 Mbps. La nueva extensión deberá implementar todas las porciones obligatorias del estándar IEEE 802.11b PHY. El actual estándar 802.11b define las tasas básicas de 1, 2, 5.5 y 11 Mbps. El proyecto propuesto apunta hacia el desarrollo de las provisiones para mejorar la capacidad de velocidad de transferencia de datos de las redes 802.11b.

Grupo de Tareas h. El objetivo de este proyecto es mejorar el estándar 802.11 MAC y la capa física de alta velocidad 802.11a en la banda de 5 GHz, para agregar la selección de canal interior y al aire libre para la licencia de 5 GHz excepto las bandas en Europa; y para mejorar la medición de energía del canal y reportar mecanismos para mejorar el espectro y la administración de la potencia de transmisión.

Grupo de Tareas i. El objetivo de este proyecto es mejorar los mecanismos de seguridad y autenticación 802.11 MAC.

Ahora es posible comprar una tarjeta WLAN PCMCIA o un punto de acceso basado en uno o más de los documentos autorizados por los grupos de tareas. WECA (*Wireless Ethernet Compatibility Alliance*) es un foro de la industria con la misión de certificar la interoperabilidad de los productos IEEE 802.11. El WECA determina los criterios para el cumplimiento, basados en las referencias de los documentos generados por los grupos de tareas 802.11.

8.3.1 Documentos y Proceso de Estandarización del IEEE

La creación de un nuevo estándar IEEE sucede mediante un Proyecto de Estándares. Éste debe ser patrocinado por un miembro del cuerpo de estandarización IEEE SA. Un Proyecto de Estándares IEEE puede ser:

Nuevo: Un documento que no sustituya o modifique substancialmente otro estándar.
Revisión: Un documento que actualiza o remplaza un estándar existente.
Reforma: Una enmienda o un cambio sustancial a un estándar existente.
Corrigenda: Un documento que contiene solo correcciones sustanciosas de un estándar existente.

Cada proyecto deber ser autorizado por el cuerpo después de una Petición de Autorización del Proyecto (PAR), la cual define el objetivo del proyecto. Una vez que el proyecto es aprobado, éste tiene que generar un expediente, antes de ser aprobado como un estándar IEEE por un comité de revisión. El comité de revisión hace recomendaciones al cuerpo de estandarización IEEE-SA sobre la aprobación o desaprobación de los documentos.

Los estándares IEEE pueden ser clasificados de cuatro formas:

Estándares. Estos documentos especifican los requerimientos obligatorios.
Prácticas recomendadas. Estos documentos clarifican procedimientos y posiciones preferidas por el IEEE.
Guías. Estas definen una serie de alternativas, pero no se hacen recomendaciones estrictas.
Documentos de prueba de uso. Válidos por 2 años, estos documentos pueden pertenecer a cualquiera de las categorías anteriores.

Cada 5 años un estándar IEEE pasa por un proceso de reafirmación para confirmar que es válido. El proceso del IEEE es mostrado en la figura 8.1.

Figura 8.1 Proceso de los estándares IEEE

CAPÍTULO 9

EQUIPOS PARA MVPN

En este capítulo nos concentramos en los bloques físicos que construyen una MVPN. Se consideran las dos categorías más importantes de productos MVPN requeridos para implementar un sistema, los clientes MVPN y los *gateways* MVPN, los cuales pueden ser soportados por plataformas de datos inalámbricas y otros dispositivos.

9.1 Clientes MVPN

Los clientes VPN están diseñados para satisfacer los requerimientos de red de una terminal sencilla. Los clientes VPN pueden por lo tanto ser implementados en cualquier tipo de dispositivo informático, desde teléfonos móviles hasta *laptops* para equipo especializado como lectores de códigos de barras o tarjetas de crédito y aplicaciones inteligentes. Los clientes VPN diseñados para un ambiente móvil deben satisfacer requerimientos específicos para dispositivos móviles, como la utilización optimizada de los recursos computacionales y del consumo de potencia y la interfaz de usuario adaptable para pantallas de tamaño pequeño. Estos requerimientos son especialmente importantes cuando los clientes VPN son instalados o incorporados dentro PDAs, teléfonos inteligentes, y otros dispositivos compactos.

9.1.1 Implementación del Cliente MVPN

Los clientes MVPN permiten a los dispositivos móviles establecer y soportar canales de comunicaciones VPN. Tienen múltiples funcionalidades, incluyendo *tunneling*, autenticación y autorización, y opciones de seguridad. Los clientes MVPN pueden ser implementados en software, los cuales deben trabajar en conjunción con el sistema operativo del dispositivo móvil, y en hardware, los cuales deben ser conectados físicamente al dispositivo móvil a través de una interfaz externa o interna (como una PCMCIA) o pueden estar dentro del dispositivo.

9.1.1.1 Funciones del Cliente MVPN

Las conexiones MVPN voluntaria son más a menudo iniciadas por el usuario, lo cual requiere unas cuantas opciones de control del acceso, autenticación y *tunneling*. Por esta razón, las funcionalidades de un cliente VPN –especialmente en ambientes móviles- constituyen una subserie de funcionalidades del *gateway* VPN. Los clientes MVPN soportan solo uno o dos tipos de tecnologías de *tunneling*, como IPSec o PPTP y clientes L2TP.

El soporte de autenticación en el cliente está usualmente dictada por el *gateway* VPN y el resto de la infraestructura implementada en la red privada. Los ambientes de red corporativos, por ejemplo, tienden a depender de la autenticación RADIUS combinada con tarjetas de muestra seguras. Un cliente VPN usado en ambientes móviles puede ser de movilidad agnóstica donde la red móvil fundamental maneja la movilidad transparentemente, o enterado de la movilidad, como es el caso de los clientes basados en IP Móvil.

9.1.1.2 Clientes Basados en Software

Este tipo de implementación del cliente VPN es por mucho la más empleada tanto para VPNs inalámbricas como alámbricas. Generalmente, los clientes basados en software son más baratos de implementar, más fáciles de distribuir y soportar, y pueden ser removidos o actualizados como sea necesario. Los clientes basados en software son usualmente menos eficientes y entonces necesitan más poder de procesamiento, lo cual lleva a que la batería se baje más rápido. Los clientes basados en software usualmente son diseñados para sistemas operativos específicos. Pueden estar integrados dentro del sistema operativo o implementados como una "cuña" entre la

capa de enlace y la capa de red del *stack* de protocolos del sistema operativo (ver figura 9.1). Algunos sistemas operativos comerciales como *Windows XP y Pocket PC 2002*, tienen clientes VPN integrados.

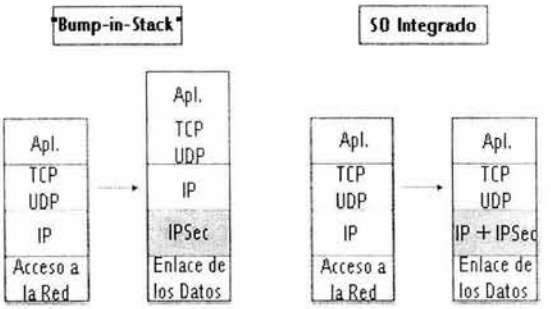


Figura 9.1 Clientes VPN de "*Bump-in-stack*" vs clientes VPN de SO Integrado

Los clientes VPN basados en software pueden ser implementados en la capa de enlace y en la capa de red del modelo OSI. Un ejemplo ampliamente utilizado de un cliente VPN de la capa de enlace es un cliente PPTP/L2TP suministrado con el sistema operativo *Windows 2000*. Sin embargo, los clientes VPN más extendidos son los clientes IPSec.

Los clientes VPN implementados como parte del sistema operativo están limitados a las características proporcionadas por el vendedor y pueden carecer de las capacidades requeridas por diferentes departamentos IT.

9.1.1.3 Clientes Basados en Hardware

Los clientes basados en hardware puede ser implementados como dispositivos añadibles, como las tarjetas PCMCIA, las tarjetas inteligentes, o hardware propietario conectado al dispositivo móvil a través de una interfaz estándar. También pueden venir como un chip o una serie de chips y pueden ser desarrollados dentro del dispositivo móvil durante su fabricación.

Las soluciones MVPN basadas en hardware deben ser dispositivos firmes y actualizables para que se mantengan a ritmo con el cambio de estándares y la evolución de la tecnología. Un cliente basado en hardware solo implementa una sub-serie de las funcionalidades del cliente VPN y deja a la aplicación de software el control de la interfaz de usuario.

9.1.2 Problemas en el Diseño de un Cliente MVPN

Existen algunos problemas de diseño para los clientes MVPN que deben ser considerados. La mayoría tiene que ver con los requerimientos específicos de los dispositivos móviles compactos y la naturaleza de las comunicaciones inalámbricas.

9.1.2.1 Recursos Limitados de la Plataforma

El diseño de los clientes MVPN para varios dispositivos móviles, como PDAs y teléfonos inteligentes, no puede darse el lujo de disponer de una potencia AC ilimitada y microprocesadores poderosos como las aplicaciones cliente VPN que residen en las computadoras personales estacionarias o en las estaciones de trabajo UNIX. Una de las formas de manejar estas restricciones es limitando las opciones y funcionalidades soportadas por un cliente móvil. Por ejemplo, el soporte de *tunneling* puede ser limitado al modo de túnel ESP de IPSec, y las opciones

de encriptación pueden ser limitadas a 3DES y RC5. También los clientes pueden ser optimizados para el uso de un sistema operativo particular, como *Pocket PC o Palm.*

9.1.2.2 Ambiente Físico Poco Confiable

Los clientes MVPN deben ser capaces de enfrentarse a una capa física o ambiente inalámbrico poco confiable. Cuando la conexión inalámbrica es poco confiable, los túneles establecidos entre el cliente y la red privada pueden romperse y es necesario reinstalarlos. Para manejar este problema, el cliente VPN debe soportar opciones o procedimientos para el restablecimiento rápido de la conexión, tales como *login* automático.

9.1.2.3 Soporte y Distribución

Los proveedores de servicio, las empresas, las instituciones, y otras entidades que implementen soluciones MVPN deben ser cuidadosos de las potenciales dificultades asociadas con la distribución de clientes MVPN, el aprovisionamiento remoto, y el soporte. Los usuarios móviles tienden a viajar con sus dispositivos en diferentes áreas y quizá sean limitadas las formas en que se comunican con los grupos de soporte de la red centralizada. Y también, no es factible mandar técnicos cuando constantemente cambia la posición del usuario remoto para repararlos en caso de que falle el soporte remoto.

La distribución e instalación del software del cliente MVPN representa desafíos similares para los departamentos IT no solo por la constante movilidad de los usuarios sino también por la inmadurez general de los dispositivos móviles. Un remedio para estos problemas debe incluir una serie de medidas tales como un mantenimiento preventivo del dispositivo móvil, externalización del soporte del usuario móvil a un tercero, y participación más amplia de los fabricantes de equipo en actividades cotidianas de soporte.

9.1.2.4 Requerimientos de Seguridad

Los requerimientos de seguridad y autenticación para los clientes MVPN son más estrictos que aquellos para los clientes VPN fijos. Los clientes VPN estacionarios están alojados en computadoras que se encuentran en cuartos cerrados como una casa u oficina remota y están usualmente bien protegidas de perpetradores. Por el otro lado, los clientes MVPN, son usualmente soportados en dispositivos móviles, los cuales tienden a ser portados por las personas. Estos dispositivos a menudo son robados, perdidos, y dejados sin atención por largos periodos de tiempo. Esto los hace presa fácil no solo del robo de propiedades sino también de que alguien desee acceder a los recursos en cierta red privada accesible para el dispositivo. Tales problemas de seguridad adicional pueden ser manejados mediante una serie de medidas que involucran reuniones periódicas del usuario, reglas estrictas de administración de la cuenta y el uso obligatorio de tarjetas *SecureID*, y otros métodos de autenticación.

9.2 *Gateways* MVPN

Los *gateways* MVPN son las piedras angulares de las MVPNs. Al contrario de los clientes MVPN, cuya función es satisfacer las necesidades de conectividad VPN de una terminal móvil, los *gateways* MVPN son los dispositivos sobre los cuales se construye la infraestructura MVPN. Los *gateways* VPN, junto con otros elementos de red como los *firewalls*, están localizados en la frontera entre una red pública (esto es, la red del proveedor de servicio de MVPN, o una red ISP que soporta conectividad hacia la red del proveedor de servicio de MVPN) y las redes del cliente de MVPN. El *gateway* MVPN también debe soportar algún esquema de movilidad cuando está colocado con una plataforma inalámbrica de datos.

9.2.1 Implementación de un *gateway* MVPN

La principal tarea de un *gateway* MVPN es garantizar la trasmisión segura de los datos del usuario entre los clientes MVPN móviles y los destinos dentro de redes privadas estacionarias (virtuales). Esto usualmente se realiza seleccionando una plataforma hardware robusta e implementando *tunneling*, control del acceso, autenticación, seguridad, y otras funciones como ruteo y varias políticas de decisión. El *gateway* MVPN debe estar diseñado para la versatilidad y así soportar una variedad de tecnologías de red y posiblemente diferentes tipos de clientes VPN (figura 9.2).

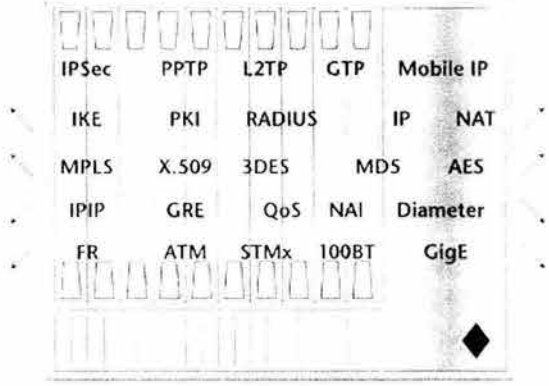


Figura 9.2 Funciones de un *gateway* para MVPN

Los *gateways* MVPN deben ser capaces de autenticar a los usuarios móviles vía múltiples mecanismos de autenticación y comunicarse con servidores AAA vía protocolos AAA cliente como un cliente RADIUS, terminar túneles originados por los clientes MVPN (en el caso de VPN voluntaria), o por los nodos de la infraestructura inalámbrica (como el nodo PDSN con capacidad IP Móvil) y establecer canales de comunicación seguros proporcionando integridad constante de los datos del usuario y protección de la confidencialidad. Los *gateways* MVPN también deben soportar una variedad de técnicas de asignación de direcciones IP estáticas y dinámicas, actualmente asumen el papel de servidores de la red de acceso, y presentan funciones adicionales asociadas con la terminación y el origen de túneles.

Al igual que los clientes MVPN, los *gateways* MVPN pueden ser implementados en software y hardware sobre una plataforma dedicada, o pueden estar combinados con otros dispositivos que realizan otras tareas dentro de una red, como servidores, ruteadores, plataformas inalámbricas de datos, o combinaciones de estos. Como resultado, las tareas no triviales asignadas a un *gateway* MVPN típico deben ser acompañadas por la capacidad para manejar ruteo y envío, administración del *buffer*, soporte de proyección de paquetes, marcado y medición de paquetes, contabilidad y monitoreo, intercepción legítima, varios esquemas de movilidad de los datos, y otras funcionalidades típicas de las redes inalámbricas de datos.

La implementación dedicada o colocada de un *gateway* MVPN puede ser *nativa*, donde la funcionalidad de un *gateway* VPN está integrada con la plataforma del sistema operativo y el hardware, o *bump-in-wire*, análoga a la implementación *bump-in-stack* de los clientes MVPN, donde un *gateway* VPN implementado sobre una plataforma dedicada está colocado con un ruteador y enlazado con éste vía una interfaz física.

9.2.2 *Gateways* MVPN y Plataformas Inalámbricas de Datos

Las plataformas inalámbricas de datos pueden ser implementadas en una variedad de formas. Las implementaciones de una plataforma inalámbrica de datos pueden ser clasificadas en dos tipos:

- Ruteador o *switch IP*
- Servidor o computadora de propósito general

Cada una tiene diferentes propiedades así como ventajas y desventajas únicas. Los servidores son computadoras de propósito general optimizadas para atender las necesidades de una red o de un grupo de usuarios más que de un usuario único. Los ruteadores son computadoras de propósito general optimizadas para enviar paquetes de datos de una interfaz física a otra.

Tradicionalmente, los ruteadores y los *switches IP* fueron implementados basados en el diseño de sistemas operativos de tiempo real (RTOSs, *Real Time Operative Systems*), como *VxWorks* producido por sistemas *Wind River*, mientras que los servidores dependieron de sistemas operativos de propósito general, como *UNIX, Linux, Windows NT, y Solaris OS*.

Las plataformas inalámbricas de datos pueden ser definidas y segmentadas en dos clases:

- Plataformas inalámbricas de datos basadas en servidor, están basadas en hardware y sistemas operativos genéricos originalmente diseñados para soportar una variedad de tareas de computación y aplicaciones generales, el mejoramiento del software para soportar tareas de red como envío o encaminamiento de paquetes, *tunneling*, y funciones AAA.

- Plataformas inalámbricas de datos basadas en ruteador/switch IP, están basadas en hardware y software dedicados a ejecutar una variedad de funciones de red (residentes en las cuatro capas más bajas del modelo OSI). La arquitectura de tales plataformas está usualmente optimizada para manejar paquetes de datos, y el envío o la conmutación y el *tunneling*.

9.2.2.1 Plataformas de Propósito General

Los sistemas diseñados para ejecutar una variedad de tareas rara vez realizan una tarea particular. Por ejemplo, las plataformas optimizadas para funcionar con sistemas operativos como UNIX y Linux han sido diseñadas para el procesamiento de datos y tareas computacionales generales, con la asignación de recursos no optimizada para tareas como ruteo, terminación PPP, y especialmente encriptación, compresión, fragmentación y reensamble de paquetes, *tunneling* y conmutación de túneles. La jerarquía de la memoria de una computadora típica diseñada para correr el sistema operativo UNIX o sus hermanos, como *SUN SPARCstations*, depende fuertemente de la memoria virtual que reside en la memoria no volátil, como discos duros u otros tipos de dispositivos mecánicos de acceso relativamente lento. A menudo, esta vía no es la más confiable, ya que los dispositivos mecánicos están más propensos a fallar, y no son óptimos para aplicaciones críticas como el ruteo que requiere frecuentes páginas rápidas de memoria local.

9.2.2.2 Ruteadores y *switches* IP

La primer clase de computadoras optimizadas para el envío de paquetes, llamadas ruteadores, fue introducida por *Cisco Systems* a finales de los 70's. El ruteador fue concebido para manejar los problemas asociados con las computadoras genéricas creando hardware especializado a menudo combinado con sistemas operativos de tiempo real optimizados para el envío de paquetes de datos y otras funciones de red. Hoy los ruteadores vienen en muchas formas y tamaños, con diferentes especializaciones y bajo diferentes nombres, como "*switch IP*" o un "dispositivo de red".

Originalmente, los ruteadores fueron diseñados para comunicarse dinámicamente con grandes números de redes vía un limitado número de enlaces. Como la tecnología de las redes de datos progresó para soportar nuevas funciones como la terminación del enlace de acceso del suscriptor, la consulta profunda de paquetes, y más tarde funciones de VPN y servicios inalámbricos de datos, fue necesario realizar modificaciones al concepto original de ruteador. Por ejemplo, los servidores de acceso remoto (RASs) fueron introducidos para manejar la terminación del suscriptor, y los *switches IP* fueron introducidos para manejar VPNs y otros servicios de datos avanzados como etiquetado, NAT, *firewalling*, IPSec y conmutación de túneles. Las últimas plataformas inalámbricas de datos tienden a estar basadas en ruteadores tradicionales, dispositivos RAS, y *switches IP*.

Para habilitar el soporte de los servicios inalámbricos de paquetes de datos en general, además de su capacidad para enviar eficientemente los paquetes, una plataforma de ruteo debe satisfacer ciertos requerimientos:

- Capacidad para terminar el tráfico del suscriptor
- Capacidad para encapsular el tráfico del suscriptor con un retardo mínimo
- Soportar significante memoria local volátil, como los recursos de la memoria dinámica de acceso aleatorio (DRAM) y *paging* rápido de la memoria
- Soportar señalización e interfaces lógicas
- Soportar tecnologías QoS tales como *DiffServ*
- Soportar esquemas de movilidad de paquetes de datos tales como GPRS e IP móvil

Además de estos requerimientos, una plataforma de datos inalámbrica que aspira a ser un *gateway* MVPN debe satisfacer lo siguiente:

- Conmutación dinámica de túneles
- Múltiples protocolos de *tunneling*
- Políticas dinámicas de aprovisionamiento (COPS, LDAP)
- Encriptación, compresión, y cliente AAA

En el lado del portador, la plataforma inalámbrica debe soportar lo siguiente:

- Una variedad de módulos de entrada/salida para interconectar el dispositivo hacia la red móvil y hacia las redes cliente.
- Capacidad para comunicarse con un gran número de redes que soportan el traslape del espacio de direcciones IP privadas, así como múltiples tablas de ruteo virtuales.

9.2.2.2.1 Ruteadores Tradicionales

Sin duda, los ruteadores tradicionales son más apropiados que los sistemas computacionales genéricos, ya que el ruteo eficiente es, sin duda, su punto fuerte. Las características de la clase del portador pueden ser fácilmente manejadas diseñando un chasis robusto con varios mecanismos de redundancia. Las capacidades de *tunneling* y etiquetado pueden ser realizadas en hardware (por ejemplo, diseñando nuevas tarjetas "aceleradoras de la encriptación") y software (optimizando los *stacks* de protocolos). Sin embargo, la conmutación de túneles y la terminación escalable del suscriptor crean ciertos problemas que obligan a cambios significantes en la arquitectura, lo cual causa que el ruteador evolucione hacia un servidor RAS o un *switch IP*. Principalmente por estas razones, los ruteadores clásicos, cuando se usan como plataformas inalámbricas de datos y *gateways* MVPN, sufren de baja escalabilidad y de una deficiencia de características esenciales.

9.2.2.2.2 Servidores de Acceso Remoto

Los servidores de acceso remoto fueron originalmente introducidos por compañías como *Livingston, Ascend Communications* (ambas adquiridas por *Lucent*), y *3Com*, para manejar la necesidad de terminar grandes cantidades de suscripciones *dial-up* utilizando protocolos de la

capa de enlace como PPP y SLIP (*Serial Line Internet Protocol*). Un servidor RAS es una combinación de un dispositivo de ruteo y bancos de módems, software optimizado para la terminación de la suscripción y además memoria adicional para almacenar información del estado de PPP. Un RAS es usado para terminar a los suscriptores que acceden a una red privada o a Internet y agrega grandes números de sesiones de comunicaciones *dial-up* de baja velocidad o llamadas ISDN establecidas sobre una red PSTN dentro de ranuras de tiempo en un número pequeño de interfaces de alta velocidad como T1s o T3s. Mientras un RAS resulta muy apropiado para los sistemas inalámbricos de circuitos de datos basados en conexiones *dial-up*, quizá sea menos conveniente para los sistemas de paquetes de datos y para MVPN debido a su número limitado de sesiones de suscriptores y a su ancho de banda.

9.2.2.2.3 *Switches* IP

Los *switches IP* están basados en un dispositivo de ruteo o un arreglo de dispositivos de ruteo, y están diseñados específicamente para la terminación escalable de los paquetes del suscriptor, vía DSL o cable módem, y la encapsulación, así como otras tareas que rebasan las capacidades de los ruteadores tradicionales o de los RAS. Ejemplos de *switches IP* incluyen *Shasta 5000* de *Nortel Networks y Springtide 7000 inalámbrico de Lucent Technologies*. Las interfaces físicas de los *switches IP* pueden ser compartidas por un gran número de sesiones de suscriptor, las cuales pueden ser balanceadas hacia arriba y hacia abajo con el ancho de banda de la interfaz hasta la cantidad de memoria y poder de procesamiento deseados por los dispositivos de ruteo y los procesadores de red. Las capacidades de *tunneling* y de conmutación de paquetes son usualmente soportadas en hardware para mayor eficiencia. La combinación de estas características, originalmente desarrolladas para manejar los requerimientos de soporte de VPN, aplicadas para soportar las funciones de paquetes de datos inalámbricos y las funciones de MVPN, hacen a los *switches IP* los mejores candidatos para la plataforma MVPN.

CAPÍTULO 10

INFRAESTRUCTURA EN MÉXICO PARA SISTEMAS INALÁMBRICOS DE DATOS

10.1 Tecnología Inalámbrica: Retos y Oportunidades

La tecnología inalámbrica ocupa cada día más un papel preponderante en nuestra vida cotidiana. De acuerdo a datos estadísticos los empleados con acceso a redes inalámbricas son más productivos, pues tienen una mayor conectividad de hasta un 22%, es decir, un promedio de $7,000 dólares por empleado, lo cual se traduce en más de 6 millones de dólares anuales en promedio en el caso de las grandes compañías. Asimismo, se espera que en el 2008 un tercio de la población mundial contará con un dispositivo inalámbrico, además de que una de las tendencias más importantes será la implantación de redes WLAN en lugares públicos como aeropuertos y universidades.

Es por ello que los proveedores de servicios inalámbricos han invertido cantidades millonarias en construir sus redes GSM/CDMA (2G), GPRS (2.5G) y UMTS/WCDMA (3G). El éxito de los proveedores de servicios de telefonía móvil ha dado como resultado la proliferación de servicios inalámbricos que ahora son considerados como básicos.

Para mantener la rentabilidad e incrementar el ingreso promedio por usuario, los proveedores están siendo retados a ampliar su portafolio de servicios, así como a mejorar la eficiencia en la entrega de servicios nuevos, desde la provisión y activación hasta la facturación y garantía del servicio.

El uso de servicios de redes inalámbricas en México puede convertirse en una herramienta de competitividad pero se requiere de una legislación que vea a estos servicios como un valor agregado para el consumidor.

A semejanza de varias ciudades del mundo, México dispone de infinidad de sitios, restaurantes, bibliotecas, parques, hoteles, entre otros, donde es posible utilizar servicios inalámbricos de red, basados en la tecnología inalámbrica Wi-Fi, sin necesidad de realizar pago alguno por ello o la exigencia de contar con un proveedor específico del servicio.

Más por uso que por promoción comercial, los servicios de redes inalámbricas crecen en popularidad, y la postura de fabricantes como Intel, uno de los principales impulsores de esta tecnología a través de su plataforma Centrino, es cabildear con las autoridades del país para que, alrededor de esta tecnología, se evite crear una regulación que frene su desarrollo y el potencial que tiene para ofrecer servicios de comunicaciones de banda ancha en zonas de difícil acceso a bajos costos, lo mismo que para apoyar labores de educación a distancia y programas de competitividad como e-México.

La experiencia internacional muestra que mientras menos restrictiva es la regulación alrededor de la tecnología inalámbrica de comunicación, mayores son los beneficios que empresas, gobierno y usuario final obtienen de su uso. Si la autoridad comienza a regular sobre precios o tarifas de acceso a los servicios y redes inalámbricas, se distorsiona el florecimiento de una tecnología que nació y ha proliferado casi de forma espontánea y que muestra sus bondades en diferentes partes del mundo donde, más que como servicio, se observa como valor agregado para el usuario.

En México, empresas como *Telmex, Tech Tec, Hot Spot International* ofrecen servicios de acceso inalámbrico a Internet en redes de área local que utilizan la frecuencia de 2.4 Giga Hertz, mejor conocida como Wi-Fi. A diferencia de otros países donde esta frecuencia se cataloga como de uso

libre, en México la Secretaría de Comunicaciones y Transportes la clasifica como de uso específico, por lo que, para ser utilizada con fines comerciales, primero requiere ser licitada.

La adopción de tecnología móvil ha superado las expectativas. En México el mercado de computadoras portátiles crece de forma acelerada, a la fecha representa más de 15 por ciento del mercado total de computadoras en el país, también se observa un incremento en la compra de equipos de cómputo de mano y bolsillo, sabemos que para poder maximizar el uso de los servicios de redes inalámbricas en el gobierno, las empresas, el hogar y las universidades, el usuario debe observar el valor que le brinda tener acceso a sus datos a través de puntos de acceso públicos, en los que no se le cobre por hacerlo.

10.1.1 Internet Inalámbrico con *Prodigy Móvil*

Prodigy Móvil de Telmex es un servicio que proporciona acceso inalámbrico de alta velocidad (Wi-Fi) a Internet en sitios públicos como aeropuertos, restaurantes, universidades, hoteles, centros comerciales, centros de convenciones, hospitales, entre otros. Los sitios están diseñados para navegar a alta velocidad. Se puede utilizar una computadora portátil (*laptop*) o un PDA, que tenga integrado o soporte la instalación de una tarjeta de acceso inalámbrico 802.11 b (Wi- Fi).

Los sitios públicos con cobertura de *Prodigy Móvil* están equipados con accesos de banda ancha (*Prodigy Infinitum*) para satisfacer las necesidades del usuario.

Los puntos de acceso instalados en el sitio público transmiten señales de radio frecuencia a los dispositivos móviles compatibles que se encuentran en la zona de cobertura.

Prodigy Móvil eligió a *Cisco Systems* como proveedor de equipos de tecnología de redes inalámbricas de área local (WLAN), así como de switcheo e infraestructura de red de servicios IP (UNINET). *Prodigy Móvil* cubrirá así el territorio mexicano con soluciones inalámbricas que se encuentran disponibles en más de 100 *hot-spots*, actualmente ubicados en restaurantes, hospitales, hoteles, centros de convenciones y aeropuertos en diferentes entidades de la República Mexicana.

Cabe señalar que diariamente se suman nuevos puntos de enlace con la intención de terminar el año con más de 300 *hot-spots*.

Adicionalmente, el servicio de *Prodigy Móvil* permite la generación de Redes Privadas Virtuales (VPN) con lo que los usuarios corporativos no tendrán ningún problema para acceder de manera segura a sus redes empresariales y a aplicaciones como Intranet, correo electrónico corporativo, etc., logrando así una mayor eficiencia en el aprovechamiento de su tiempo.

10.1.2 Internet Móvil Desarrollado por *Wireless Net Online*

Internet Móvil es una solución desarrollada por *Wireless Net Online S.A de C.V* para proporcionar un servicio de internet inalámbrico de alta calidad basado en la infraestructura de las compañías celulares, actualmente trabajan con la red GSM de Telcel. *Online* agrega optimización, contenido, correo electrónico, variedad de equipo y soporte técnico al sistema nativo, proporcionando a sus clientes una mejor experiencia al navegar por la red.

El servicio de Internet Móvil está basado en la infraestructura de las compañías celulares de voz, sin embargo, en su manera nativa el servicio móvil es lento y frecuentemente presenta problemas de conexión.

La tecnología GPRS permite en su forma original una conexión a internet desde su *laptop* a velocidades de entre 30 y 40 Kbps. Mediante el Internet Móvil GPRS de *Online* se puede llegar hasta 160 Kbps lo que permite correr la mayoría de las aplicaciones multimedia. El aumento de velocidad mediante la optimización de *Online* es de 2 a 5 veces en la mayoría de las aplicaciones.

10.1.3 Telcel

Aunque hasta el momento sólo Telcel ha anunciado formalmente sus planes de implementar una red 3G, en México la migración va por buen camino. Si se toma en cuenta que tres de los cuatro operadores móviles que existen en México (Iusacell, Unefon y Telefónica Móviles, con la integración de Pegaso) trabajan con CDMA y uno en TDMA (Telcel), la migración hacia CDMA2000 será sencilla, pues sólo se necesitarán cambios de tarjeta en las radiobases, actualizar el software y colocar un nodo de internet o un nodo de servicio de datos en paquete (PDSN).

Durante el período de 1988 a 1990, Telcel amplió su red celular en el espectro radioeléctrico de 800 MHz (Banda B) para cubrir las ciudades de Tijuana, Cuernavaca, Toluca, Guadalajara, Monterrey y la zona metropolitana de la Ciudad de México, y en 1990 comenzó a ofrecer servicios celulares en las nueve regiones en que se divide el territorio nacional. En 1998 Telcel obtuvo una concesión para ofrecer servicios PCS en el espectro radioeléctrico de 1900 MHz (Banda D) en las nueve regiones del país. Telcel introdujo sus servicios PCS en la Ciudad de México en 1999, y actualmente ofrece dichos servicios en las nueve regiones del país. En octubre de 2002 Telcel introdujo su red GSM, y al 31 de diciembre de 2002 dicha red abarcaba 70 ciudades.

Telcel es el proveedor líder de servicios de comunicaciones inalámbricas en México. Al 31 de diciembre de 2002, la red celular de Telcel cubría el 34% del territorio nacional, incluyendo las principales ciudades, y llegaba al 90% de la población del país.

Telcel cuenta con concesiones para operar redes celulares en los espectros radioeléctricos de 800 MHz (Banda B) y 1900 MHz (Banda D) en las nueve regiones en que se divide el territorio nacional. Al 31 de diciembre de 2002, Telcel tenía 20.1 millones de suscriptores, y de acuerdo con la COFETEL tenía una participación de aproximadamente el 77.4% en el mercado nacional de los servicios inalámbricos. Aproximadamente el 21% de los suscriptores de Telcel están ubicados en la zona metropolitana de la Ciudad de México.

10.1.3.1 Servicios de Datos

Servicios de mensajes: En abril de 1998, Telcel comenzó a ofrecer servicios de transmisión de mensajes cortos de una vía ("1W-SMS") a los suscriptores de sus planes de postpago. Los servicios 1W-SMS permiten enviar mensajes electrónicos personalizados de una vía e incluyen diversos servicios de información preseleccionados por los suscriptores, tales como reportes meteorológicos, cotizaciones financieras y noticias sobre espectáculos. En 2002 Telcel comenzó a ofrecer servicios de mensajes electrónicos personalizados de dos vías ("SMS"), que permiten a los suscriptores de los planes de prepago y postpago enviar y recibir mensajes cortos utilizando las tecnologías TDMA y GSM.

Internet: El protocolo para aplicaciones inalámbricas ("WAP") es un estándar de aplicación mundial que está diseñado para permitir que los usuarios de teléfonos celulares puedan obtener acceso a Internet. Actualmente, los servicios disponibles a través del protocolo WAP incluyen los de correo electrónico, transmisión de datos e información, y transacciones comerciales electrónicas. Este estándar permite que los micronavegadores o "*browsers*" instalados en los teléfonos celulares se enlacen a un servicio de acceso en la red de Telcel, permitiendo así que los usuarios puedan consultar diversas páginas de Internet.

En septiembre de 2002, Telcel introdujo su servicio de acceso al protocolo WAP en las principales ciudades de cada una de las nueve regiones en que se divide el territorio nacional, permitiendo que los suscriptores de sus planes de prepago y postpago en dichas regiones puedan tener acceso a los servicios de correo electrónico, banca, reservaciones y otras transacciones de comercio electrónico. Telcel introdujo el portal de *Internet Datum*, que proporciona a sus suscriptores acceso a diversos servicios tales como los de buzón electrónico y noticias financieras a través de un asistente personal digital ("PDA") conectado a un módem inalámbrico.

10.1.3.2 Transmisión de Datos

En septiembre del 2000, Telcel desplegó una red de servicios de transmisión de datos en paquete a través de redes digitales ("CDPD"), para los suscriptores de sus planes de postpago en las principales ciudades de cada una de las nueve regiones celulares en que se divide el territorio nacional. Estos servicios comenzaron a ofrecerse a los suscriptores de sus planes de prepago a partir de noviembre de 2001. La red CDPD es una red conmutada de paquetes que aprovecha el hecho de que en muchas aplicaciones de datos la información se envía por medio de descargas con períodos de silencio intermitentes. Para la mayoría de las aplicaciones la plataforma CDPD representa un medio para la transmisión de datos a un costo más eficiente que los servicios de transmisión de datos por redes analógicas o digitales de circuitos conmutados, ya que permite que el canal de la red sea compartido por un gran número de usuarios. En lugar de marcar a una línea telefónica, los suscriptores del sistema CDPD están conectados de manera permanente a un servicio de red que les proporciona acceso a las redes de datos en paquete.

Los servicios CDPD de Telcel tienen capacidad para soportar aplicaciones diseñadas específicamente para ciertas industrias, tales como las siguientes:

- Telemetría: Las redes inalámbricas permiten a las empresas tales como las de suministro de gas y electricidad, monitorear los niveles de consumo de sus clientes a través de una conexión inalámbrica entre los medidores y su centro de control. La Telemetría también se puede aplicar en el campo de la medicina para monitorear a los pacientes independientemente de que éstos se encuentren o no hospitalizados.

- Validación inalámbrica de tarjetas de crédito: Los equipos terminales permiten a los establecimientos mercantiles validar los pagos efectuados con tarjetas de crédito o débito. A través de la plataforma CDPD, las terminales pueden mantenerse en línea de manera inalámbrica, reduciendo significativamente el tiempo necesario para procesar una validación y eliminando la necesidad de contar con una línea telefónica a un lado de la terminal. Esto puede dar lugar al surgimiento de una gran variedad de nuevas aplicaciones en las industrias de servicios remotos tales como las de comida rápida o mensajería.

- Aplicaciones para funciones de envío: Las empresas de servicios de mensajería, las empresas repartidoras y las empresas con instalaciones o departamentos de reparaciones de gran tamaño, utilizan la plataforma CDPD para apoyar a sus empleados. Los trabajadores pueden ser despachados con órdenes de trabajo detalladas, pueden accesar las bases de datos de clientes desde cualquier punto donde se encuentren trabajando, y pueden cerrar órdenes de trabajo en línea.

- Aplicaciones para seguridad pública: Los estados y municipios pueden utilizar la plataforma CDPD como medio principal de comunicación de datos a los vehículos oficiales de seguridad pública.

- Localización automatizada de vehículos: A través de un pequeño dispositivo que contiene un módem CDPD y un sistema de posicionamiento global ("GPS"), los usuarios pueden rastrear sus flotillas de vehículos en Internet, pudiendo de esta manera acceder más rápidamente y a costos más eficientes toda la información necesaria para el diseño de rutas y el despacho de vehículos y paquetes.

A través de su nueva red GSM, Telcel ha comenzado a ofrecer servicios de transmisión de datos mediante circuitos de voz para sistema celular ("CSD") a todos sus suscriptores, y servicios de radio en paquete general ("GPRS") a sus suscriptores de postpago. En octubre de 2002, Telcel comenzó a ofrecer servicios GPRS a sus suscriptores de prepago.

Las redes inalámbricas de Telcel utilizan principalmente tecnologías digitales. Al mes de diciembre de 2002, el tráfico de señales digitales en dichas redes representaba el 68.6% del tráfico total de

Telcel. En los últimos siete años Telcel ha convertido su red analógica a una red digital, y la mayoría de sus suscriptores han cambiado su servicio al servicio digital.

Telcel utiliza la tecnología digital de acceso múltiple con división de tiempo ("TDMA") en los espectros radioeléctricos de 800 MHz (Banda B) y 1900 MHz (Banda D). La tecnología digital TDMA es una tecnología que divide el espectro radioeléctrico en espacios de tiempo asignados para la transmisión de señales.

En octubre de 2002 Telcel lanzó una nueva red celular utilizando la tecnología digital de sistema global para comunicaciones móviles ("GSM") en el espectro radioeléctrico de 1900 MHz (Banda B). La tecnología GSM es un estándar digital utilizado en Europa, Norteamérica y otros países. En virtud de que el uso de dicha tecnología se encuentra ampliamente difundido, la misma proporciona un acceso más rápido a nuevos productos y servicios y cuenta con una gama más amplia de proveedores que la tecnología TDMA. Además, la tecnología GSM proporciona acceso a una trayectoria más desarrollada hacia la tercera generación de tecnologías inalámbricas.

También existe la tecnología CDMA, una tecnología digital alternativa que divide los espectros radioeléctricos utilizando códigos en vez de segmentos de tiempo. En comparación con las tecnologías TDMA y GSM, la tecnología CDMA permite el uso de un mismo espectro radioeléctrico por un mayor número de suscriptores, pero dicha tecnología está menos desarrollada y recibe menos apoyo de parte de los proveedores.

Debido a las ventajas de la tecnología GSM sobre las tecnologías TDMA y CDMA, Telcel considera que el desarrollo de una red GSM es el paso lógico para mantener su posición de liderazgo en el mercado de los servicios inalámbricos.

10.1.3.3 Red TDMA

Telcel cuenta con una red de cobertura nacional que utiliza la tecnología digital TDMA. La tecnología TDMA hace posible el uso de avanzados teléfonos celulares bimodales de doble banda que permiten hacer *roaming* entre sistemas analógicos y digitales y entre los espectros radioeléctricos de 800 MHz y 1900 MHz. La tecnología digital TDMA también permite ofrecer mejores servicios y características, tales como los servicios de mensajes alfanuméricos, baterías de larga duración, mayor seguridad durante las llamadas y una mejor calidad de voz. Los equipos TDMA son ofrecidos por varios distribuidores líderes en la industria de las telecomunicaciones, incluyendo *Lucent, Ericsson y Nortel.*

10.1.3.4 Red GSM

Telcel ha construido e instalado una red GSM para el espectro radioeléctrico de 1900 MHz en las nueve regiones celulares del país, misma que entró en operación en octubre de 2002. La nueva red GSM permite a Telcel aumentar su capacidad digital y avanzar en su evolución hacia la tercera generación de tecnología inalámbrica. La tecnología GSM soporta una gran variedad de servicios de voz y datos, incluyendo CSD, CSD de alta velocidad y GPRS, y actualmente es el sistema inalámbrico más utilizado y probado en el mundo.

En su primera etapa, la red GSM de Telcel ofrece servicio en las nueve regiones celulares del país, pero no proporciona cobertura en todas las ciudades ubicadas en dichas regiones. Al 31 de diciembre de 2002, Telcel cubría 70 ciudades a través de su red GSM, y contaba con aproximadamente 500,000 suscriptores. A medida que Telcel avance en el despliegue de su red GSM, tiene planeado ampliar su cobertura en las nueve regiones celulares del país. Telcel espera que muchos de sus clientes elegirán equipos GSM al momento de reemplazar sus equipos TDMA actuales.

10.1.3.5 Tecnología CDPD

La plataforma de servicios de transmisión de datos en paquete a través de redes digitales ("CDPD") es un estándar de la industria que permite que la mayoría de las aplicaciones creadas para Internet y una gran cantidad de aplicaciones corporativas, operen eficientemente en la red sin necesidad de hacer modificaciones. Al utilizar la tecnología CDPD, los archivos y transmisiones de datos se dividen en pequeños paquetes y se envían a través de un canal inalámbrico dedicado. En muchas aplicaciones de datos, la información se envía por medio de descargas con períodos de silencio intermitentes. Las tecnologías de transmisión de paquetes aprovechan esta circunstancia y permiten que los datos del usuario se transporten de manera eficiente en un mismo canal de la red.

Como resultado de lo anterior, para la mayoría de las aplicaciones el servicio de paquetes conmutados CDPD representa un medio para la transmisión de datos a un costo más eficiente que los servicios de transmisión de datos por redes inalámbricas de circuitos conmutados analógicas o digitales, ya que permite que el canal de la red sea compartido por un gran número de usuarios. El uso de las funciones de conmutación de paquetes en las redes digitales existentes a través de la plataforma CDPD, está considerado como el primer nivel de transición entre las tecnologías de segunda y tercera generación en la industria inalámbrica, mismo que se conoce como 2.5G.

Telcel desplegó su servicio CDPD a través de su red TDMA en las nueve regiones celulares del país en septiembre del 2000.

10.1.3.6 Tecnología CSD y HSCSD

La tecnología de transmisión de datos mediante circuitos de voz para sistema celular ("CSD") es un sistema alternativo basado en plataformas de circuitos conmutados que proporciona servicios de datos al integrar la infraestructura de voz existente. Al igual que la tecnología CDPD, la tecnología CSD está considerada como el primer nivel de la tecnología 2.5G.

La plataforma CSD de alta velocidad (HSCSD) ofrece el mismo servicio que la plataforma CSD, utilizando canales de voz para las transmisiones de datos, pero al unir varios segmentos de información ofrece una mayor capacidad y velocidad por lo cual resulta más adecuada para satisfacer las necesidades de aquellos usuarios que transmiten grandes cantidades de información.

Telcel tiene planeado ofrecer tanto servicios CSD como servicios HSCSD a través de su red GSM en las nueve regiones celulares del país.

10.1.3.7 Tecnología GPRS

Los servicios de radio en paquete general (GPRS) constituyen un sistema de transmisión de datos en paquetes utilizando la plataforma GSM. Este sistema permite transmitir información a altas velocidades y puede ser utilizado en varios tipos de teléfonos celulares, ofreciendo algunos servicios de tercera generación pero utilizando bandas, equipos y programas distintos. La tecnología GPRS permite a los operadores de sistemas GSM ofrecer nuevos servicios del protocolo de Internet y proporciona aplicaciones inalámbricas de Internet más atractivas a un amplio grupo de usuarios.

Ofrece a los suscriptores un eficiente acceso a Internet, permitiendo que varios usuarios compartan los mismos recursos de la interfaz de aire. Los operadores que utilizan el sistema GPRS pueden cobrar a sus clientes por la cantidad de datos transmitidos en lugar de por el tiempo aire, en virtud de lo cual este sistema representa una opción más atractiva para las transmisiones de datos breves. La tecnología GPRS es similar a la tecnología CDPD que se ofrece a través de la red TDMA de Telcel, pero proporciona una mayor capacidad que la tecnología CDPD.

Los servicios GPRS, en conjunto con los servicios CSD y HSCSD, permiten a los suscriptores de los servicios GSM de Telcel seleccionar servicios de datos adecuados para satisfacer sus necesidades específicas.

Telcel está evaluando la conveniencia de seleccionar la tecnología de datos mejorados para evolución global ("EDGE"), como la arquitectura inalámbrica intergeneracional que le permitirá desplegar eventualmente la tecnología de tercera generación. Uno de los beneficios de la tecnología EDGE consiste en que la misma puede desplegarse en el espectro radioeléctrico existente.

Telcel espera que en la medida en que sus suscriptores cambien sus aparatos a la tecnología EDGE, todas las aplicaciones actualmente desarrolladas y utilizadas podrán operar a mayores velocidades y en mayor número de lugares. La tecnología EDGE está siendo desarrollada actualmente por *Ericsson, Nokia, Nortel, Lucent y Motorola.*

Se espera que la evolución de la tecnología 2.5G a la tecnología 3G dará como resultado que las redes inalámbricas sean capaces de transmitir voz, datos y video a través de una misma red. La industria inalámbrica convino recientemente en encaminarse a la adopción de un estándar común CDMA de banda ancha ("W-CDMA") para el desarrollo de la tecnología de tercera generación. La tecnología W-CDMA cuenta con configuraciones que permiten el procesamiento multifacético y hacen posible la transmisión de grandes volúmenes de datos, tales como los datos de video, a altas velocidades.

Como parte de la evaluación estratégica del lanzamiento de la tecnología EDGE, Telcel está sosteniendo discusiones con sus proveedores y tiene planeado poner a prueba dicha tecnología entre sus usuarios corporativos o de uso intensivo. Telcel espera introducir el sistema EDGE con las tecnologías celulares o PCS existentes, y adoptar la tecnología de tercera generación W-CDMA una vez que la COFETEL licite una nueva serie de frecuencias de banda ancha.

10.1.4 Competencia

Los principales competidores de Telcel incluyen a Grupo Iusacell, S.A. de C.V. (que está controlado por *Verizon Wireless y Vodafone*), Movistar (una marca utilizada por un grupo de empresas controladas por Telefónica Móviles, S.A. de C.V., una filial del grupo español Telefónica) y Operadora Unefon, S.A. de C.V. De acuerdo con la COFETEL, al 31 de diciembre de 2002, Telcel tenía una participación de aproximadamente el 77.4% en el mercado celular de México.

Desde su entrada en el mercado mexicano, Telefónica Móviles ha tenido como objetivo ser un operador global con presencia en todo el mercado de México. Tras el cierre de la adquisición del 65.23% del capital de Grupo Pegaso Telecomunicaciones a mediados de septiembre 2002 y la integración de esta compañía con las operaciones de Telefónica Móviles en el norte del país, Telefónica Móviles México se ha convertido en el segundo operador de telefonía móvil del mercado mexicano, con licencia para operar en todo el país. En este sentido, a finales de diciembre 2002, Telefónica Móviles México contaba con más de 2.4 millones de clientes.

Telefónica Móviles México, S.A. de C.V., está conformada por Telefónica Móviles, S.A. (92%) y Grupo Pegaso (8%). Telefónica Móviles México ya opera bajo la marca Telefónica MoviStar en los nueve Estados del norte de la República Mexicana: Baja California, Baja California Sur, Sonora, Sinaloa, Chihuahua, Durango, Coahuila, Tamaulipas y Nuevo León. Pegaso PCS cuenta con concesión para operar en todo el territorio nacional.

La tecnología que soporta los servicios de Telefónica Móviles México es una tecnología madura y probada. En México, Telefónica Móviles está invirtiendo en desarrollar la mejor tecnología y la mayor cobertura nacional.

Durante el 2003 se llevó a cabo un importante despliegue de red por las principales ciudades, que llevó la tecnología GSM e innovadores productos y servicios a 40 localidades de toda la República. Telefónica Móviles cuenta con una gran experiencia en GSM desde la creación del estándar tecnológico, en la que participó con otros operadores y fabricantes. La compañía es miembro fundador de la *GSM Association.*

Grupo Iusacell, S.A. de C.V. (Iusacell, NYSE: CEL; BMV: CEL) es la proveedora de servicios celulares inalámbricos en siete de las nueve regiones de México incluyendo el Distrito Federal, Guadalajara, Monterrey, Tijuana, Acapulco, Puebla, León y Mérida. Las regiones de servicio de la Compañía cubren un total de aproximadamente 92 millones de habitantes (POPs), lo que representa aproximadamente el 90% de la población total del país.

Mientras Telcel fue el primero en anunciar la puesta en marcha de su red GSM, Iusacell presentó la Red Express 3G, que le permitirá ofrecer servicios avanzados de transmisión de datos desde dispositivos de comunicación móvil, como teléfonos celulares 3G o PDA con tarjeta módem inalámbrica incorporada.

Con ello, ambos operadores compiten nuevamente en la entrega de servicios de telecomunicaciones, que son una muestra clara de lo que será la Tercera Generación (3G). En este sentido, a través de la Red Express 3G de Iusacell, los usuarios podrán conectarse a internet y redes corporativas, enviar y recibir correo electrónico, así como transferir archivos de texto e imágenes a una velocidad de 144 kbps en cualquier momento.

Dadas sus características, el servicio estará disponible en las zonas de cobertura donde impere el ambiente empresarial, de negocios y comercial, mientras que en el resto del territorio nacional continuará vigente el servicio de acceso de datos a 14.4 kbps.

De entre las más de 400 aplicaciones 3G que existen para el mundo, destacan por su éxito las siguientes: descarga de internet de distintos tonos de timbrado para los teléfonos móviles; envío de mensajes cortos acompañados de multimedia (imágenes, fotos o videoclips); descarga de videoclips, juegos, aplicaciones de información y navegación relacionadas con mapas y localización de lugares (establecimientos comerciales, direcciones específicas o más convenientes rutas de circulación).

CAPÍTULO 11

SERVICIOS MÓVILES PARA EL FUTURO

11.1 Industria Actual de los Sistemas Inalámbricos y Evolución de los Sistemas 3G

Históricamente, muchas regiones del mundo han estado dominadas por el proteccionismo –el deseo de imponer barreras al libre movimiento de la gente, la información, los bienes, y los capitales a través de límites regionales, para el propósito de protección y sostenimiento de las economías locales y preservación de la riqueza de los países. Además de otras consecuencias negativas esto ha resultado en la creación de sistemas inalámbricos y estrategias de asignación del espectro incompatibles en diferentes regiones del planeta. Sin embargo, recientemente dos factores están cambiando este modelo tradicional: el desarrollo y el comercio de productos están sucediendo cada vez más en una escala global y un Internet global hace el intercambio de la información simple y a menudo libre.

Como está incrementando el número de personas que gozan la capacidad de cruzar libremente las fronteras para negocios o entretenimiento mientras requieren servicios básicos como correo electrónico, comercio y depósitos financieros, noticias, y mensajería virtual, se necesita encontrar una manera de integrar o al menos armonizar los sistemas inalámbricos. En respuesta a esta situación, en Abril del 2002, los socios de 3GPP y 3GPP2 se reunieron en Canadá y alcanzaron un acuerdo para seguir un camino común en el desarrollo de la evolución de los sistemas 3G basados en IP. El último objetivo fue permitir *roaming* global a través de las tecnologías. La capacidad para soportar acceso a los servicios de múltiples tecnologías ha sido reconocida como un importante requerimiento para los sistemas 3G. La convergencia del transporte es una de las principales razones detrás del éxito de IP en las redes alámbricas, que permite el funcionamiento entre redes a través de diferentes redes.

¿Cómo ocurrirá esta transición? Inicialmente, el acceso será discontinuo. Los usuarios serán conectados y desconectados de los servicios muchas veces en un día, cada vez que cambia el tipo de la red de acceso disponible y restablece la conectividad. Luego, con la adopción más amplia de las tecnologías de movilidad de la capa IP como IP Móvil, el usuario móvil será permanentemente capaz de acceder a los servicios sin la necesidad de reconectarse a un ambiente multi-acceso. El conductor de esto estará en las aplicaciones y los servicios, los cuales requerirán accesibilidad permanente de la capa IP para ser soportados (manteniendo constante la dirección IP, por ejemplo). Hasta entonces, el *roaming* global a nivel IP (proporcionado vía protocolos RADIUS o DIAMETER o basado en certificaciones digitales) espera cubrir mayores necesidades de movilidad.

11.1.1 Aspectos de Servicio

Los sistemas están evolucionando hacia una red central común basada en IP para soportar servicios multimedia. Sin embargo, el soporte de multimedia no es la única meta de los servicios basados en IP. Más bien, la meta es la integración de datos y otros medios sobre un sistema uniforme *de manejo de sesión*.

La arquitectura de todos los sistemas basados en IP, o de los Subsistemas Multimedia IP (IMSs), mostrada en la figura 11.1, está basada en el Servidor del Suscriptor Local (HHS, *Home Subscriber Server*). Como una mejora de la base de datos HLR, los servidores HHS soportan los datos del suscriptor relacionados con los subsistemas IMS en base al Protocolo de Inicio de Sesión (SIP, *Session Initiation Protocol*), servidores que controlan los medios para el establecimiento de las sesiones y los *gateways* utilizados para funcionar con otros sistemas como la red PSTN y los sistemas móviles legados.

El HSS incluirá la funcionalidad previamente asociada con el HLR, que incluye control del acceso a la red inalámbrica y administración del perfil del suscriptor, así como datos de suscripción a servicios multimedia e información de registro basado en IP. La información de registro inicia un mapeo entre las identidades públicas del usuario y los servicios que el usuario tiene activados (por ejemplo, apodos (*nicks*) de los servicios de conferencia multimedia), la identidad privada del usuario (como el IMSI), y la dirección IP actual utilizada para alcanzar al usuario. El registro del usuario a los servicios depende de la autenticación explícita, la suscripción, y posiblemente la verificación del crédito. Las interfaces al servidor HHS en los sistemas 3GPP están basadas en MAP (para el control del acceso a la red de acceso inalámbrico) y DIAMETER, mientras que en los sistemas 3GPP2 están basadas sólo en DIAMETER.

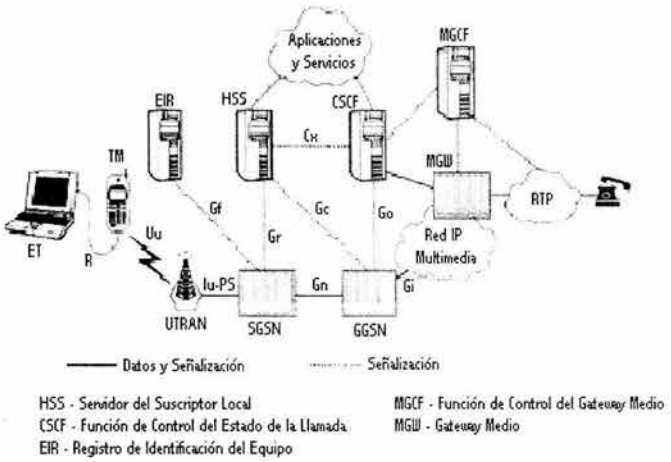


Figura 11.1 Arquitectura simplificada del subsistema IMS

La figura 11.2 explica el proceso de registro para un suscriptor que accede a servicios IMS en redes 3GPP. El suscriptor equipado con una terminal conveniente primero se enlaza a una red UMTS. Entonces un contexto del Protocolo de Paquetes de Datos (PDP) es instalado por un APN permitido por el subsistema IMS (asociado a una red IPv6 que recibe a los servidores del IMS). Entonces utiliza los servicios de un *proxy* CSCF (*Call Session Control Function*) para registrarse con el servidor HSS en la red local. En este proceso, la red local asigna al suscriptor a una CSCF de Servicio (S-CSCF, un servidor SIP definido en la arquitectura del IMS de 3GPP para ofrecer a los suscriptores control del servicio y control de la sesión). La S-CSCF está localizada en la red local, y puede entregar la misma mirada y sensación de los servicios independientemente de la localización actual del usuario y de la red de servicio.

El IMS utiliza servicios basados en paquetes. En este tiempo, los servicios basados en paquetes no incluyen un soporte eficiente de *multicast*, lo cual es soportado actualmente mediante la réplica de la información *multicast* sobre portadores *unicast* en los nodos *gateway* (GGSN). Una serie de especificaciones está siendo alistada para la liberación R6 de 3GPP, de modo que la interfaz de radio será capaz de entregar servicios *multicast y broadcast*.

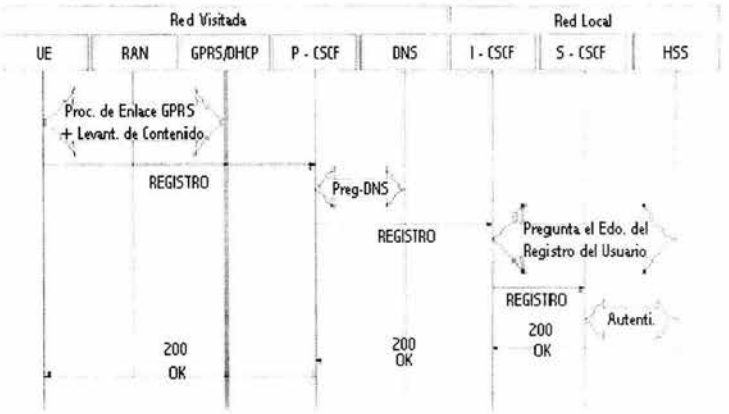


Figura 11.2 El registro del suscriptor del subsistema IMS en 3GPP.

Esto creará una demanda por redes de distribución de contenido *multicast y broadcast*, las cuales necesitarán rastrear la movilidad del usuario. Esto conducirá a un nuevo tipo de MVPNs, llamadas *MVPNs multicast*, donde el tráfico es enviado solo una vez hacia algún punto de acceso de la red IP y el punto de acceso tiene al menos un miembro del grupo *multicast*. Esto también puede ser realizado simplemente extendiendo los actuales protocolos de ruteo *multicast*, o utilizando túneles *multicast* entre el *gateway* de distribución *multicast* y los puntos de acceso.

IMS estará basado en IPv6, y potencialmente ayudará a la introducción en gran escala del protocolo IPv6 en las redes de los portadores.

Finalmente, la habilidad de entregar flujos de medios entra en 3GPP, recientemente 3GPP2 empezó alguna actividad en esto también, con la habilidad de atar a un portador de la red de UMTS a la sesión relacionada de los medios vía un mecanismo de control de la política basada en COPS-PR [RFC3084] que utiliza la entrega de símbolos de autorización de los medios a los puntos finales de la sesión. Estos símbolos entonces se utilizan durante la petición de la asignación de portador para validar la asociación del portador a los medios y para instalar los filtros asociados de paquetes, permitiendo así que los proveedores de servicio facturen simplemente en base a la duración o contenido de la sesión de los medios y no por el servicio de portador. Esta característica es soportada por la interfaz Go entre el nodo GGSN y la función de control de paquetes de la CSCF.

11.1.2 Movilidad Basada en IP

El soporte de la movilidad IP es un método para mantener una estación móvil conectada a Internet mientras que cambia el punto de enlace a Internet. Sin embargo, algunas veces una estación móvil no requiere estar permanentemente accesible en la capa IP, así que este tipo de soporte de la movilidad quizá no sea parte de la evolución de los sistemas móviles.

El Grupo de Trabajo de la Movilidad Continua del IETF ha redactado una propuesta diferente para manejar esta cuestión. La estación móvil no estaría involucrada explícitamente en el registro con el HA; más bien, la red la rastrea de tal manera que la estación móvil siempre este accesible en un servidor de rastreo, el cual entonces llama a la estación móvil cuando alguna entidad necesite comunicarse con ella.

Existe una necesidad urgente para poner disponibles algunos métodos para la autenticación del usuario móvil en una red basada en IP para intercambiar información de autenticación, con el punto de acceso que actúa como un servidor de acceso a la red. En el IETF, el Grupo de Trabajo

PANA (*Protocol for Carrying Authentication for Network Access*) ha sido formado para manejar esta cuestión. Muchas propuestas están sobre la mesa –algunas que reusan la autenticación DHCP y otras que extienden EAP para estar basado en IP. El Grupo de Trabajo PANA promete desarrollar un protocolo universal para autenticación que pueda ser usado en cualquier red que permita *roaming* universal.

11.1.3 Facturación Para los Servicios Inalámbricos de Datos

Originalmente, la facturación de los servicios inalámbricos de datos en las redes celulares estuvo basada en el concepto de la facturación basada en el volumen. Este modelo fue más atractivo para el consumidor que el modelo tradicional basado en la medición del tiempo de uso, el cual mantenía una conexión continua y la utilizaba sólo cuando era necesario para transmitir y recibir los datos.

Sin embargo, más allá de su uso en el modo-i, el cobro en base al volumen en general no se considera una opción atractiva para los consumidores y las corporaciones. De hecho, a menos que los honorarios de volumen se hagan suficientemente bajos, no hay ninguna aceptación de pagar fuertes cantidades de dinero para transferir documentos o multimedia sobre el enlace inalámbrico. En muchas ocasiones, el costo de esto puede superar la ganancia de productividad o el valor de tiempo de tener acceso ubicuo a la información, haciendo este modelo comercial no viable, ya que los usuarios prefieren esperar a tener acceso a la información hasta que ellos estén en alguna posición que les permita usar una tecnología de acceso de red alterna que satisfaga mejor sus necesidades.

Finalmente, la administración del crédito mediante cuentas con tarjetas de prepago o de crédito tal vez pueda ser extendida con la integración de servicios financieros o de depósito ofrecidos por el portador inalámbrico.

11.2 El Futuro de los Servicios y Sistemas Inalámbricos

Consideremos los posibles escenarios de servicios, descritos en la figura 11.3, así como las tecnologías y los actores que los permitirían. Un requerimiento crítico de los servicios basados en IP es la capacidad de entregar un ambiente en el que el usuario se sienta cómodo y atraído. Este ambiente puede ser creado mediante la interacción hombre-máquina: una interfaz gráfica de usuario (GUI) bien definida, opciones de servicio fáciles de usar, personalización de la interfaz, y auto adaptación a los perfiles de uso del cliente. Esto también puede involucrar recibir comunidades de interés, donde grupos de individuos puedan compartir emociones, experiencias, ideas, e información. Estos requerimientos deben ser satisfechos por servicios de datos persona-a-persona y persona-a-máquina ofrecidos por los sistemas inalámbricos, pero sin duda, no por aplicaciones máquina-a-máquina.

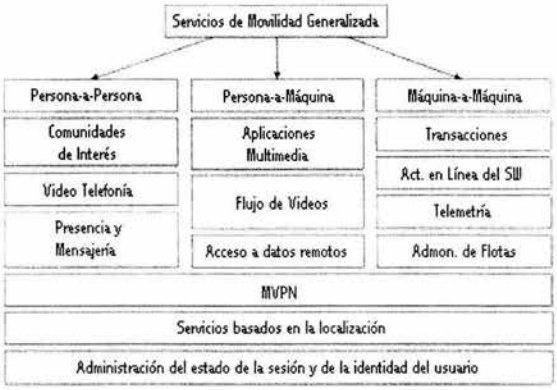


Figura 11.3 Ejemplos de servicios móviles del futuro

11.2.1 Servicios Persona-a-Persona

En la telefonía tradicional, las interacciones entre dos o más usuarios usualmente ocurren después de que algún reconocimiento mutuo ha sido establecido y después del intercambio de los números telefónicos mediante canales. Nos referimos a esto como un "método fuera de banda". Este modelo aún es válido hoy en día, con la excepción de las aplicaciones consumidor-a-negocio (por ejemplo, llamadas libres, marcación de un número buscado en la sección amarilla) y negocio-a-consumidor (por ejemplo, aplicaciones de *telemarketing* y encuestas a los clientes) donde sólo una parte conoce a la otra. Los servicios de fecha quitaron la necesidad de intercambiar números telefónicos fuera de banda, aunque algunos de ellos dependen del intercambio de información basado en el servicio SMS.

En los servicios persona-a-persona de la siguiente generación, los números telefónicos dejarán de ser la única identidad a través de la cual el usuario será conocido. Más probablemente, los usuarios se suscribirán a comunidades que usan una identidad pública. Establecerán contactos con miembros de esas comunidades, creando un ambiente cómodo y fomentando la demanda de otros servicios de telecomunicaciones móviles. Por ejemplo, un usuario puede crear una comunidad virtual que involucre a todos los miembros de su comunidad con el propósito de intercambiar mensajes de texto, imágenes, videos, y conversaciones de voz. Las comunidades corporativas de interés también serán establecidas para ofrecer servicios de mensajería y servicios de diseminación de información. La información distribuida dentro de estas comunidades corporativas puede ser privilegiada o restringida. Los derechos de los miembros de la comunidad serán críticos en este tipo de ambiente. La administración de los servicios de la comunidad se convierte en una parte importante de un negocio del portador inalámbrico, frecuentemente asociado con la administración VPN para la seguridad y la privacidad.

Los miembros de la comunidad pueden ser avisados mediante una interfaz basada en íconos cuando los otros están accesibles. En este escenario, las llamadas tendrán lugar sólo cuando otro usuario este disponible; de otra manera, otros mensajes pueden ser dejados en el buzón de correo del usuario. Los usuarios serán capaces de señalar selectivamente su disponibilidad para los otros miembros dependiendo de, por ejemplo, el tiempo del día y el estado comercial. En este enfoque, una serie de direcciones estarían almacenadas localmente en un directorio telefónico; más bien, una lista de amigos o identidades organizadas en base a la comunidad serían almacenadas en la red. Este modelo ofrece nuevas formas que permiten a los individuos interactuar a través de dispositivos móviles y no móviles. Esto incrementará significativamente la cantidad de información intercambiada mediante otros medios (como la mensajería gráfica, ya desarrollado en Europa vía el Servicio Multimedia de Mensajería (MMS)), y consecuentemente los ingresos del proveedor de servicio.

Otro aspecto importante de este nuevo modelo de interacción del usuario es la entidad que actúa como la terminal de la comunidad. Los usuarios de hecho pueden ser capaces de suscribirse a comunidades recibidas por las partes con excepción del proveedor de servicio inalámbrico. Sin embargo, el proveedor de servicio inalámbrico puede ofrecer mucho más valor agregado que animaría a los clientes a usar comunidades recibidas en su ambiente, ya que el portador inalámbrico tiene la oportunidad de integrar a su ambiente otros servicios valiosos como información basada en la localización, servicios de voz *push-to-talk*, información relacionada a la sesión y contratación sencilla. Entonces, las comunidades recibidas por los proveedores inalámbricos pueden resultar muy competitivas y altamente diferenciadas con respecto a lo que terceros pueden ofrecer.

Otro servicio que promete convertirse en un generador importante de ingresos en los sistemas 3G es la video-telefonía. Sin embargo, mientras no mejore significativamente la comunicación interpersonal, las cuestiones de los precios quizá prohíban su éxito. Históricamente, la video-telefonía no ha tenido éxito en el ambiente alámbrico, que parece ser el caso aún ahora, cuando muchas casas y negocios pueden estar equipados para comunicaciones de alta velocidad que no son caras. Quizá la movilidad y la necesidad de asociar una voz con una cara entre los individuos involucrados en una conversación puede demostrar fomentar este servicio, con la capacidad de distribuir una imagen de una localización actual al tiempo que toma lugar la sesión de voz mejorada con video.

Inicialmente, por lo menos, el acceso a la comunidad no debe ser atado a ninguna carga excepto que un honorario modesto de la suscripción, para fomentar el crecimiento de los servicios asociados a ellas. Al igual que con muchos otros servicios de telecomunicación, las comunidades sufren de la exterioridad de la red, donde el valor del servicio mismo está ligado a la existencia de otros suscriptores que utilizan el mismo servicio. Las barreras de acceso deberían ser minimizadas a fin de atraer a los usuarios a comunidades donde ellos pueden usar muchos servicios, que juntos constituirán una corriente de ingresos significativa. La creación de comunidades y la capacidad de manejar listas "de amigos" y perfiles de usuario personalizados dentro de ellas es imperativa para la atracción y retención del cliente, ya que los aspectos sociales de tales servicios únicos tendrán un efecto significativo sobre los usuarios. Animarán por lo tanto más probablemente a los portadores inalámbricos a crear comunidades mutuamente incompatibles que reciben ambientes, similares a los servicios de mensajería inmediata ofrecidos por actores como *MSN, Yahoo, y AOL*.

11.2.2 Servicios Persona-a-Máquina

Un servicio persona-a-máquina ofrecido por los portadores inalámbricos no exige sincronismo, interacción en tiempo real entre las personas. Para esta serie de servicios, las personas interactúan con terminales de datos o aplicaciones multimedia, que abarcan entretenimiento, recuperación de información, y aplicaciones para transacciones. Estos servicios están basados en la disponibilidad del contenido al que las personas quieren tener acceso.

Los usuarios que pertenecen a comunidades virtuales pueden ellos mismos generar algún contenido, mediante el intercambio persona-a-persona de imágenes, videos cortos, texto y contenido Web. No obstante, se espera que la mayoría del contenido sea proporcionado por los socios y recibido en las redes de los socios o sobre las instalaciones del portador inalámbrico. Esto requerirá el uso de MVPNs para hacer cumplir el servicio exclusivamente y proteger contra ataques de negación de servicio y acceso no autorizado.

El éxito de los servicios basados en contenidos depende enormemente de la amigabilidad para el usuario y de la claridad del lenguaje utilizado.

Los servicios persona-a-máquina son usados en las redes de hoy en productos de información como reportes de las condiciones del tráfico y sistemas interactivos de respuesta a la voz utilizados para obtener información del estado de cuenta o para actualizar información, como el número de una tarjeta de crédito, en los perfiles de los suscriptores. Claramente, las máquinas son mejor

accedidas a través de interfaces basadas en señale-y-de *click* más que mediante la interacción a base de voz, aunque haya en efecto algunas aplicaciones basadas en *Voice XML*, un lenguaje similar a aquellos usados para crear páginas Web que está optimizado para la navegación a base de voz y recoge la entrada de voz y ejecuta comandos de voz. Cuando los dispositivos móviles estén equipados con gráficas mejoradas y entrada señalar-y-seleccionar, será posible una mejor interacción persona-máquina. Una de las cuestiones que deben ser consideradas es cómo el usuario ingresa la información mientras interactúa con las máquinas.

Las comunidades pueden convertirse en un vehículo para los servicios persona-a-máquina. Una comunidad puede tener derecho para recibir información de la máquina reservada sólo para sus miembros; por ejemplo, una comunidad puede estar definida como un grupo de clientes de una institución bancaria y cualquier miembro puede ser dirigido con noticias del banco o bienvenida para interactuar con miembros virtuales, los cuales son simplemente máquinas que ofrecen servicio de ayuda o que actúan como asistentes virtuales.

El servicio de acceso a Internet es otro buen ejemplo de aplicación persona-máquina. En el futuro cercano es más probable que esté ligado con la oferta de servicio inalámbrico de datos y no probablemente para generar ingresos significantes basados en honorarios por volumen de tráfico. Por otra parte, el acceso inalámbrico puede generar una clase de nuevos servicios en Internet, y estos servicios pueden en cambio usar información derivada accediendo a los datos disponibles de interfaces como las que los proveedores inalámbricos ofrecen a terceros, vía *gateways* OSA o interfaces Web.

Otra aplicación que es tratada por muchos como un conductor potencial de los servicios 3G es el flujo de video. En general, se espera que el flujo de video sea ofrecido en la forma de clips de corta duración que satisfagan la curiosidad de los usuarios acerca de nuevos artículos o eventos, o acerca de la localización actual de los usuarios, como noticias históricas, información cultural, e información turística. La entrega de larguísimos vídeos de entretenimiento o clips de entretenimiento que puede estar fácilmente disponible en casa mediante acceso de banda ancha o servicio de cable no puede ser esperado prácticamente en el futuro inmediato principalmente por las limitaciones de ancho de banda y otras razones obvias como el tamaño de la pantalla del dispositivo y la corta vida de la batería.

11.2.3 Servicios Máquina-a-Máquina

El espacio para este tipo de aplicación es muy amplio. Ejemplos incluyen a los fabricantes de móviles que permiten actualizar remotamente el software del microteléfono vía la interfaz inalámbrica, que usan al móvil como una señal de autenticación y autorización para propósitos de pago en lugar de la tradicional tarjeta de crédito, o que liga las capacidades de la terminal inalámbrica hacia una máquina y le permite interactuar con los recursos o información centralizados.

Otro ejemplo, las aplicaciones de telemetría, involucran el monitoreo remoto de dispositivos y eventos. Con el advenimiento de los servicios basados en la localización, nuevos tipos de aplicaciones de administración de una flota pueden aparecer como una extensión y mejoramiento de los servicios de telemetría que existen. Esto puede requerir la integración de la aplicación en ambientes de redes corporativas, que asocian la aplicación basada en la localización con un servicio basado en comunidad donde el miembro de la comunidad es un vehículo que pertenece a la flota, todos soportados sobre una MVPN asociada con la compañía dueña de la flota. Los posibles clientes para tales servicios incluyen compañías de transportación y servicios de radio taxi. Otras aplicaciones puede incluir el aprovisionamiento de línea de respaldo para ambientes de misión crítica en caso de que falle una conexión alámbrica en algunos ruteadores de acceso, así como monitoreo remoto.

11.3 Operador de Red Virtual Móvil

El uso de Operadores de Red Virtual Móviles (MVNOs) es un concepto reciente. Desde el punto de vista del cliente, no existe diferencia entre los servicios proporcionados por un MVNO y un portador inalámbrico tradicional, mientras que en realidad los servicios son proporcionados mediante alguna forma de acuerdo entre el MVNO y el operador actual de las redes celulares. Con el advenimiento de proveedores alternativos de red de acceso inalámbrico, como los proveedores de servicio de Internet WLAN, o WISPs,, los MVNOs pueden ofrecer servicio mediante una variedad de medios de acceso. Además, existen diferentes clases de MVNOs dependiendo de su nivel de contrato en las operaciones físicas de la red. El MVNO ligero es diferente en base al cliente único y a la marcación, mientras que el MVNO completo no solo se enfoca en la marcación sino que también opera algunos elementos críticos de la red.

11.3.1 MVNO Ligero

Un MVNO ligero enfoca su actividad en la adquisición y retención del cliente móvil, campañas de publicidad, cuidado del cliente, y la marcación. Este operador no desea adentrarse en los aspectos técnicos de los servicios de administración, y cree que los servicios ofrecidos mediante la red de un socio, o múltiples socios, son suficientes para satisfacer las necesidades de su cliente. Típicamente, estos operadores arrendan espacio en el registro HLR y los servidores AAA del portador existente y utilizan la infraestructura o los acuerdos de *roaming* del portador. Alternativamente, los MVNOs pueden usar sus propios HLRs y servidores AAA y simplemente tener acuerdos de *roaming* con todos los portadores nacionales.

Estos operadores no requieren enormes inversiones, y pueden invertir todos sus esfuerzos en la satisfacción y el desarrollo del suscriptor. Los MVNOs también pueden definir sus propias aplicaciones para diferenciarse a sí mismos aún más de la competencia y los servicios proporcionados por un portador inalámbrico cuya infraestructura están utilizando.

11.3.2 MVNO Completo

Un MVNO completo agrega valor a la conectividad de la red de acceso operando algunos elementos en la red central. En un sistema definido por 3GPP, por ejemplo, el MVNO puede querer operar el HLR, los servidores AAA, y el nodo GGSN o las particiones lógicas de los GGSNs (GGSNs virtuales). En los sistemas definidos por 3GPP2 pueden operar partes de los grupos de HAs, el nodo PDSN, y los servidores AAA. Los MVNOs completos pueden operar aplicaciones conjuntamente con los proveedores ASP y usar éstas y otras relaciones similares para dirigir el mercado corporativo mediante servicios VPN de administración y aplicaciones de servicios de datos. Un portador alámbrico tradicional que atiende a un número significante de clientes de negocios puede decidir añadir soporte de acceso inalámbrico para extender su línea de productos y actuar como MVNO. Esta clase de MVNOs quiere competir por los elementos técnicos de la entrega de servicio, porque ellos creen que su experiencia les da una ventaja competitiva o porque ellos saben como manejar la base de clientes existente.

11.3.3 MVPN en un Ambiente MVNO

Está claro que la existencia de MVNOs necesita ser tomada en cuenta cuando son definidas las soluciones técnicas de MVPN, ya que el mismo MVNO puede ser un tipo especial de negocio de portador inalámbrico.

El MVNO puede preguntar al proveedor inalámbrico para ofrecer un servicio MVPN sobre el cual el MVNO implementa un portal cautivo donde sus suscriptores son autenticados y donde ellos seleccionan los servicios a los que desean suscribirse o que desean usar durante una sesión particular. Esta VPN puede proporcionar el acceso a múltiples áreas asociadas con paquetes de tales servicios. El MVNO puede preguntar al portador inalámbrico para construir otras VPNs adicionales para soportar redes de aplicaciones específicas que sólo los suscriptores a esas

aplicaciones tienen derecho de acceso. Adicionalmente, si el MVNO ligero tuvo que soportar redes corporativas, ellos preguntarían al socio para administrar completamente los aspectos técnicos del SLA y de la integración del servicio, quizá junto con un tercer socio técnico, quien puede tener una relación con un número de clientes de la empresa que el MVNO podría proveer.

Alternativamente, el MVNO podría arrendar GGSNs o GGSNs virtuales (o HAs en los sistemas 3GPP2) del portador inalámbrico y administrarlos de acuerdo a la serie de reglas acordadas en el contrato que define esta relación de negocios. También puede manejar completamente los servicios de integración y soporte del cliente corporativo. En este caso, la posesión del nodo *gateway* implica que el MVNO puede manejar libremente la VPN que ellos ofrecen a sus clientes, y el MVNO debe operar también el servidor DNS necesario para las redes para resolver los APNs para las direcciones IP en los GGSNs que opera.

En otro escenario, el MVNO podría ofrecer a sus clientes servicio de MVPN voluntaria basada en un cliente VPN IPSec o IP Móvil, para proporcionar el soporte de múltiples tecnologías de acceso y para terminar la conexión IPSec en una *gateway* VPN o un HA que reside en la central de datos del MVNO antes de entregar el tráfico a la red cliente adecuada. Este escenario hace uso de plataformas especializadas para manejar un gran número de túneles IPSec y para soportar el servicio de VPN GW virtual de tal modo que a cada red cliente se le asigna un VPN GW virtual, o para aplicar conmutación entre la interfaz virtual de ingreso y egreso en base a la identidad de la red cliente y no en base al ruteo IP.

11.4 Convergencia WLAN/Celular y MVPN

En esta sección se considera el principal mecanismo que se usa para crear MVPNs convergentes que integran tecnologías y sistemas inalámbricos de paquetes de datos como WLAN, GPRS, UMTS, y CDMA2000.

11.4.1 Integración de WLAN y un Sistema Celular

WLAN no es un sistema estandarizado; no incluye el manejo de los datos del suscriptor, administración de la localización, o administración de la movilidad para la macro-movilidad, *handover* rápido, *roaming*, autenticación del usuario, y otros atributos tradicionalmente asociados con un sistema de telecomunicaciones como GSM. Por otra parte, desde la perspectiva de uso residencial y aplicación a negocios la integración de WLAN y los sistemas celulares tiene sentido. Si está integrado correctamente, WLAN puede complementar un sistema celular 2G o 3G de muchas formas. Las tasas de rendimiento de WLAN son superiores a las de los últimos sistemas inalámbricos de paquetes de datos como UMTS. Además, el equipo WLAN es significativamente más barato y más fácil de instalar y soportar. Mientras satisface las necesidades de ancho de banda, WLAN puede al mismo tiempo aligerar la carga de la infraestructura celular atendiendo a suscriptores en áreas altamente congestionadas. WLAN combinado con los sistemas celulares puede servir como la base para nuevos servicios de datos generadores de ingresos como acceso MVPN de alta velocidad y otros servicios inalámbricos de datos que requieren portador de alto rendimiento.

Estos factores recientemente estimularon una nueva clase de operadores de WLAN sin licencia conocidos como proveedores de servicio de Internet Inalámbrico, quiénes instalan WLANs en posiciones estratégicas, donde probablemente se requiera tener acceso a datos de alta velocidad. Estas posiciones también llamadas zonas críticas, o *WLAN hot spot*, ganan popularidad rápido con los usuarios de datos móviles y pueden ser formadas, sobre fusiones y adquisiciones o federaciones de ISPs inalámbricos, en una red de ubicaciones capaces de cubrir una amplia área, sobre todo cuando es combinado con un sistema celular basado en paquetes de datos bien desarrollado.

11.4.2 Métodos de Integración WLAN

La integración WLAN/celular es un fenómeno relativamente reciente, pero existen ya un número de mecanismos disponibles que permitirían la integración más o menos continua entre los dos. 3GPP SA1 recientemente ha puesto un requerimiento para el interfuncionamiento de WLAN con las redes UMTS y para generar los estándares que lo gobernarían. Como consecuencia, 3GPP2 SA2 está trabajando en la definición de la arquitectura y los aspectos del sistema de la integración de WLAN y los sistemas celulares. Otro grupo, ETSI BRAN (*Broadband Radio Access Networks*), estaba trabajando con los mecanismos específicos para definir HiperLAN/2. Este documento también intenta clasificar los métodos de integración WLAN/GPRS definiendo dos opciones de integración: *ligera y firme* (ver figura 11.4).

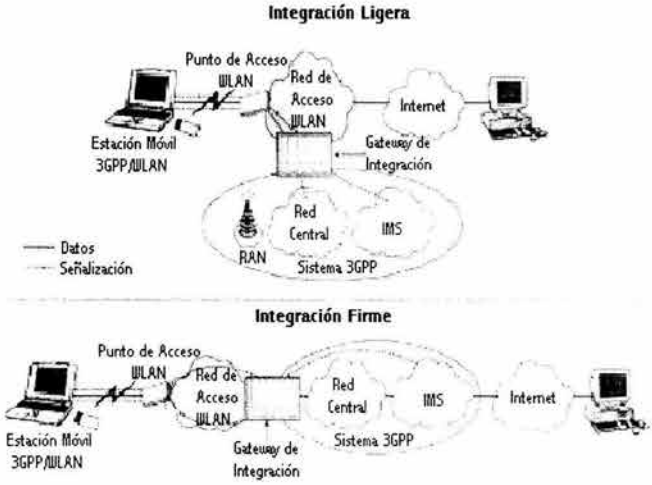


Figura 11.4 Opciones de integración WLAN/celular

La integración ligera se refiere a un escenario donde el tráfico WLAN no atraviesa la central GPRS y en vez de eso es encaminado directamente hacia Internet, así que la únicas funciones compartidas por los dos sistemas son la autenticación y la contabilidad.

La integración firme se refiere a un escenario donde el tráfico WLAN es manejado por los elementos en la red central de GPRS o en el dominio PS de UMTS, como el nodo GGSN, el nodo SGSN, y la función CGF (*Charging Gateway Function*). Esta clasificación solo es aplicable en el marco de los sistemas GPRS y UMTS.

La integración puede permitir los mismos servicios inalámbricos de datos a través de diferentes tecnologías de acceso, así como la entrega de los mismos servicios MVPN (en los escenarios de la integración firme utilizando el mismo APN en los nodos GGSN usados por el suscriptor en la red celular; o en los escenarios de la integración ligera, utilizando acceso a la red basado en IP Móvil o soluciones basadas en *tunneling* voluntario).

11.4.2.1 Autenticación Basada en IMSI Para la Integración WLAN

El mecanismo basado en IMSI asume que el dispositivo WLAN del usuario puede ser autenticado por la infraestructura común de los sistemas celulares de la misma forma que cualquier dispositivo celular. Por ejemplo, en GPRS la estación móvil es autenticada mediante una tarjeta con chip (SIM, *Subscriber Identity Module*), así que el primer requerimiento para la autenticación WLAN/GPRS

basada en IMSI es el soporte de un lector del SIM en la terminal móvil del equipo WLAN. Un buen ejemplo, es la tarjeta PCMCIA WLAN con un lector del SIM fabricado por *Nokia*, la cual introdujo un dispositivo GPRS/WLAN basado en SIM que maneja muchas cuestiones de integración y compatibilidad del lado del usuario. Hoy, sobre el enlace de radio, esto requiere el uso de un mecanismo propietario. Por esta razón, el IEEE o el Grupo de Trabajo PANA del IETF están desarrollando un enfoque para llevar a cabo esta funcionalidad de manera estándar.

El soporte de red para este escenario requiere transportar material de autenticación del sistema celular estándar desde el *gateway* WLAN de acceso hacia un *gateway* intermedio donde el material de autenticación del suscriptor es descargado de la base de datos HLR. Esto puede ser dirigido mediante la introducción de un nuevo elemento de red que integre las infraestructuras WLAN y GPRS y puentear el protocolo AAA usado por WLAN, como RADIUS, con la señalización MAP o TIA y los protocolos AAA usados en las redes celulares. Por simplicidad nos referiremos a este dispositivo como un *gateway* de integración. Este *gateway*, ilustrado en la figura 11.4, puede incluir otras funcionalidades que dependen del grado de la integración WLAN con la infraestructura celular.

En un escenario de integración fuertemente conectado, el *gateway* de integración puede actuar en los sistemas 3GPP como un nodo SGSN desde el punto de vista del sistema celular, comunicando a la CGF y al GGSN y al SGSN que atienden a la red celular de radio acceso. El acceso MVPN obligatoria en este caso será soportado por la infraestructura GPRS en una manera similar a la utilizada por los usuarios terminales de GPRS. En la integración ligera, el *gateway* de integración puede ser implementado como equipo independiente. En este caso sólo el protocolo AAA de WLAN y la señalización MAP o TIA y los protocolos AAA usados en las redes celulares están trabajando, y el tráfico es directamente entregado hacia Internet.

La principal función del *gateway* de integración en los sistemas combinados WLAN/GPRS es convertir los datos de contabilidad basados en RADIUS de WLAN a un formato de facturación de GPRS y conectar la autenticación RADIUS con acceso basado en MAP hacia la información almacenada en el HLR. El sistema de facturación de GPRS puede ser mejorado para ser capaz de identificar la fuente de los CDRs (*Charging Data Records*) a fin de facturar exactamente al cliente por el uso de WLAN vs GPRS.

La autenticación basada en IMSI no es directamente aplicable en el ambiente de CDMA2000, ya que la autenticación en CDMA2000 no está basada en una tarjeta SIM. Actualmente, la autenticación y la contabilidad en CDMA2000 hechas por el nodo PDSN y el HA (en el caso de IP Móvil) están basadas en RADIUS. Debido a que la autenticación RADIUS también es utilizada en WLAN, la tarea de integración WLAN es relativamente recta. El único requerimiento en este caso sería para convertir los parámetros de contabilidad de WLAN a la forma especificada para los sistemas CDMA2000 por la TIA [IS835]. En CDMA2000 estos consisten de los parámetros específicos de radio colectados por la red de radio acceso y los parámetros específicos de la red central colectados por el nodo PDSN. Entonces el PDSN forma un Registro de Datos Usados (UDR) que consiste de ambos parámetros, el cual es enviado hacia un servidor AAA local y posiblemente comunicado sobre la infraestructura AAA.

11.4.2.2 Autenticación Basada en NAI e IP Móvil

En contraste con el enfoque basado en IMSI, este método se integra más fácilmente con los ambientes ISP y AAA – aunque ello requiere del operador celular en los sistemas GPRS/UMTS para operar un servidor AAA basado en RADIUS compatible con el protocolo AAA de WLAN.

Existen dos posibles escenarios para los sistemas de autenticación basada en NAI:

- La estación móvil no está permitida para *handoff* hacia el sistema celular, y viceversa, sin perder la continuidad de la sesión. Por lo tanto, la integración es solo en el nivel AAA, y se espera que la movilidad del usuario esté limitada. Sin embargo, este modelo no parece

sufrir de las limitaciones de movilidad, ya que en la mayoría de los casos, los usuarios WLAN usan *laptops* en zonas críticas y son por lo tanto bastante estáticos.

- El *handoff* intersistemas está permitido por el soporte de IP Móvil en la infraestructura celular y en la infraestructura WLAN. La infraestructura WLAN/celular basada en IP Móvil requeriría el agente FA de IP Móvil para ser soportado por el punto de acceso de WLAN o en los *gateways* intermedios que atienden a un grupo de APs (ver figura 11.5).

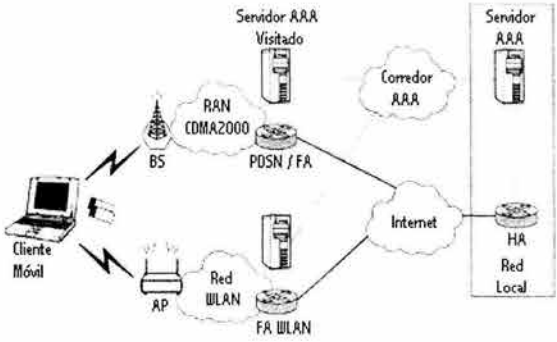


Figura 11.5 Integración WLAN/Celular basada en IP Móvil

En el caso de CDMA2000, cuando es utilizado el método de acceso de IP Móvil, IP Móvil es sin duda soportado nativamente. Los usuarios equipados con *laptops* que soporten acceso WLAN y CDMA2000 –por ejemplo, vía dos tarjetas PCMCIA- pueden vagar casi continuamente entre dos tipos diferentes de tecnologías de acceso inalámbrico, mientras preservan la dirección IP de usuario y las comunicaciones extremo-a-extremo que incluyen *tunneling* voluntario o la sesión TLS hacia una red privada. La autenticación basada en NAI tiene la ventaja de ser soportada por muchos tipos de equipo WLAN estándar y protocolos estándar basados en IP y por consiguiente por software cliente.

En el caso de UMTS y GPRS, un operador celular que ofrece integración WLAN basada en IP Móvil es requerido para desplegar un nodo GGSN que integra la funcionalidad del FA de IP Móvil. Esto requiere configurar la terminal para solicitar los APNs soportados por esos GGSNs, y para almacenar la información de suscripción en el HLR que permite al usuario acceder a esos APNs.

CAPÍTULO 12

RESULTADOS Y CONCLUSIONES

La proliferación y el desarrollo de los sistemas celulares de voz ha expuesto a través de los años las capacidades y la eficacia de las comunicaciones inalámbricas y, así, ha pavimentado el camino para las aplicaciones inalámbricas de datos en amplias áreas. La demanda para tales aplicaciones está experimentando actualmente un aumento significativo y, por lo tanto, hay una llamada fuerte para las tecnologías móviles avanzadas y eficientes de datos.

Las comunicaciones inalámbricas de datos están llegando a ser tan comunes como sus contrapartes alámbricas. La necesidad de comunicaciones inalámbricas de datos se presenta parcialmente debido a la necesidad de computadoras móviles y parcialmente debido a la necesidad de aplicaciones específicas, tales como servicios de envío automatizados y gerencia móvil de flotas. La computación móvil, que apunta para emigrar el mundo de la computación hacia un ambiente móvil, es afectado principalmente por dos componentes: portabilidad y conectividad.

Con respecto a la conectividad, es decir, la capacidad de conectarse con los recursos externos y de tener acceso a los datos externos, la tecnología inalámbrica de datos juega un papel importante porque puede ofrecer la conectividad ubicua, es decir, conectividad en cualquier lugar, en cualquier momento. Por esta razón, la tecnología inalámbrica de datos puede ser de valor real al mundo de los negocios puesto que los usuarios de la computadora son más productivos cuando explotan las ventajas de la conectividad.

La movilidad y la seguridad se están convirtiendo en los temas dominantes para el Internet del nuevo siglo. Estos factores presentan muchos desafíos y muchas oportunidades. La movilidad incrementa la necesidad de seguridad, justamente esto trae consigo la necesidad de aplicar otras tecnologías como descubrimiento del servicio, administración de la localización, *tunneling*, y administración de los datos remotos. Estas tecnologías representan una reestructuración fundamental de los enfoques previos para continuar con el crecimiento del Internet.

El *tunneling* solo es lo suficientemente poderoso para efectuar tal reestructuración, pero los diseñadores de redes rara vez crean soluciones que involucren *tunneling* puro. En vez de eso, la administración de túneles está equipada con muchas y diversas tecnologías para decidir cuando permitir, iniciar, y detener el uso de un túnel. Todas estas técnicas significan una expresión de algunas políticas, las cuales están motivadas por el problema que la solución de *tunneling* intenta resolver.

Dos regímenes de políticas de *tunneling* muy prominentes son IP Móvil y VPNs. La intención es crear rutas útiles de tal manera que los datos puedan ser entregados de manera segura hacia cualquier dominio exterior que el nodo móvil visite. Las técnicas de movilidad son adaptadas para cubrir las necesidades de los dispositivos cuyas comunicaciones son protegidas por VPNs. Esto crea el concepto de MVPNs (*Mobile VPNs*).

Estamos en la etapa en la que las tecnologías de las comunicaciones inalámbricas de datos han alcanzado la madurez al menos tienen estabilidad en los estándares. Los sistemas inalámbricos de la tercera generación, los cuales definen nuevos servicios y proporcionan soporte de datos a alta velocidad y multimedia, han sido estandarizados y están siendo desplegados rápidamente por todo el mundo. Todos estos sistemas incluyen soporte para comunicaciones de datos por conmutación de paquetes. Los aspectos importantes de estos sistemas incluyen no solo transmisiones más altas, sino también disponibilidad, capacidades permanentes, eficiencia más alta, y una gran base para la entrega de nuevos servicios. Los datos por paquetes, efectivamente contribuyeron a que las redes inalámbricas fueran más cercanas –en funcionalidad, transmisión, y utilización de los

recursos- a las redes de datos alámbricas mientras que preservan y mejoran una de las más importantes características de las comunicaciones inalámbricas: *la movilidad*.

Adicionalmente, el avance en las tecnologías de las redes privadas virtuales permitió el fácil uso de las infraestructuras alámbricas públicas compartidas, como Internet, para transmitir de manera segura el tráfico de datos privados, extendiendo así el alcance de las redes privadas permitiendo a los usuarios remotos conectarse a los recursos, a la información y a los servicios remotos.

El siguiente paso obvio es aplicar los beneficios de las tecnologías VPN tradicionales a los ambientes inalámbricos, para crear las MVPNs que permitan comunicaciones privadas seguras sobre una variedad de redes móviles compartidas ofrecidas por los operadores inalámbricos y los proveedores se servicio de Internet inalámbrico.

"Privacidad" es justamente la palabra clave del concepto de VPN, sistema que permite a dos o más redes privadas conectarse sobre otra red que puede ser de acceso público. Se puede definir a una red privada virtual (VPN) como la simulación de un enlace dedicado entre dos entidades a través de Internet, utilizando equipos o software que se comunican entre sí mediante reglas para conseguir privacidad. Una red privada virtual es una red privada que se extiende, mediante un proceso de encapsulación, y en su caso, de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. Pero no es el único tipo de VPN que existe. También se puede tratar de redes privadas virtuales que utilizan el protocolo IP (IP VPN), ya sea sobre Internet o sobre la *backbone* de un operador. Asimismo, una VPN puede habilitarse sobre una red empresarial que utilice otros protocolos de conectividad como Frame Relay, ATM o X.25, según lo requiera la empresa usuaria.

Las VPN se clasifican por tipo de uso: conexión sitio a sitio (de matriz a sucursales), acceso remoto (con enlaces *dial-up*) y extranet (modalidad de sitio a sitio que conecta la matriz con clientes y proveedores). Pero las VPN más populares en la actualidad y cuya tendencia de crecimiento es exponencial, son las IP VPN. ¿La principal razón? Reducción de costos de operación y mantenimiento. Otros beneficios de las IP VPN son: facilidad de administración (centralizada), desempeño garantizado, escalabilidad y posibilidad de utilizar aplicaciones de convergencia de comunicaciones.

Inseguridad ¿Mito o realidad? El incremento en el uso de la red de redes es, sin duda, uno de los impulsores de las comunicaciones a través del protocolo IP. Pero la idea de que las VPN sólo utilizan Internet como medio de transporte ha creado la percepción equivocada de que son inseguras. Quizás en sus inicios lo fueron, sobre todo en la parte de intrusión y desempeño. Sin embargo, al detectarse tales problemas, rápidamente se desarrollaron tecnologías que hoy hacen que las VPN sean igualmente seguras que las redes tradicionales.

El mayor reto de la seguridad es tener simplicidad en un modelo complejo, y para ello se requiere una integración de todas las herramientas. Después de la creación de Internet, las VPN han sido uno de los desarrollos tecnológicos que mayor influencia han tenido en el aumento de la productividad y la reducción de costos de las empresas, así como en el incremento de la seguridad en operaciones bancarias y de información confidencial.

La tecnología de túneles (*Tunneling*) es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPNs es conceptualmente parecido al *log-in* en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de

identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya entrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de *hashing* para derivar un valor incluido en el mensaje como *checksum*. Cualquier desviación en el *checksum* indica que los datos fueron alterados en la transmisión o interceptados y modificados en el camino.

Una de las principales necesidades que llegaron a cubrir las IP VPN en el mercado de conectividad es la incorporación de más servicios. Esto es posible gracias al protocolo MPLS, que transmite información IP a través de la *backbone* de un portador, aunque también trabaja con Frame Relay y ATM. Esta tecnología etiqueta los diferentes paquetes para identificarlos, lo que permite a los operadores ofrecer calidad de servicio (QoS), como la prioridad de datos. Las tecnologías de encriptación y transporte son las que hacen seguras a las VPN. El principal protocolo en esta materia es *IP Security (IPSec)*, desarrollado para soportar un intercambio seguro de paquetes sobre Internet a través de dos modos de encriptación: de transporte y por túnel. El primero encripta la parte de datos de cada paquete, mientras que el segundo protege los dos extremos de la conexión. Su característica principal es que es compatible con la mayoría de hardware y software para VPN. El estándar de encriptación de datos DES, con más de 20 años de creado, ha evolucionado en 3DES, que encripta un mensaje tres veces con diferentes combinaciones de llaves, por lo cual es mucho más seguro que el primero.

Otro protocolo utilizado en redes privadas virtuales es SOCKS 5, que intercepta un requerimiento de servicio y lo revisa en una base de datos de seguridad. Si la petición está permitida, el servidor autentifica al usuario que lo solicitó.

L2TP surge por la necesidad de transmitir tráfico seguro por una red de capa 2, donde se dan las comunicaciones en una LAN, a diferencia de IPSec, que se mueve en la capa 3.

Asimismo, existen dos sistemas criptográficos básicos: simétricos y asimétricos. Los primeros tienden a ser más rápidos en la entrega de información y se usan para intercambiar paquetes grandes de datos entre dos puntos reconocidos. Los asimétricos, por su parte, son más complejos pues requieren un par de llaves relacionadas matemáticamente (una pública y una privada) para ser accesados.

La principal ventaja de usar una VPN es que permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder. El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de una computadora en esa red privada, pudiendo acceder a la información publicada para esa red privada: bases de datos, documentos internos, etc. a través de un acceso público. Al mismo tiempo, todas las conexiones de acceso a Internet desde la computadora cliente VPN se realizarán usando los recursos y conexiones que tenga la red privada.

Entre los inconvenientes podemos citar: una mayor carga en el cliente VPN puesto que debe realizar la tarea adicional de encapsular los paquetes de datos una vez más, situación que se agrava cuando además se realiza encriptación de los datos que produce un mayor retardo de la mayoría de las conexiones. También se produce una mayor complejidad en el tráfico de datos que puede producir efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (*proxy*, servidor de correo, permisos basados en nombre o número IP)

Es un hecho que los beneficios de contar con una VPN son muchos, más aunque el concepto esté de moda, es preciso comprender sus alcances y analizar si responde a las necesidades específicas de una empresa.

Las oportunidades de negocio que las tecnologías 3G representan para proveedores, operadores, fabricantes de equipo y desarrolladores de aplicaciones son interesantes. En primer lugar, se incrementa el número de abonados, los cuales reciben nuevos servicios y aplicaciones. En segundo lugar, los usuarios actuales obtiene servicios de valor agregado. Los jóvenes, el mercado corporativo y los profesionistas.

Sin embargo, dada la situación económica de México, el *boom* de los servicios 3G no será tan impresionante como en otros países. Si bien no podemos compararnos con Corea, es probable que en México tengan éxito algunas aplicaciones desarrolladas en países asiáticos o en Brasil, por ejemplo, como es la banca móvil.

Entre los retos que la tecnología 3G tiene en México están:

- Definir estrategias hacia el cliente final
- Diseñar servicios adecuados de valor agregado
- Implementar esquemas de facturación que alienten el consumo de servicios 3G, sobre todo si se considera que por primera vez se tiene la oportunidad de cobrar no por el tiempo de conexión sino por la cantidad de Kbps transmitidos
- Atender al mercado corporativo
- Crear servicios personalizados

En términos generales, se concluye que las VPNs representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro; el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

De manera personal puedo decir que los alcances de este trabajo son muchos porque no solo resalta la importancia que las redes privadas virtuales móviles tienen a nivel empresarial, sino que profundiza en todos los detalles de su clasificación y funcionamiento, explica la implementación de las MVPNs dentro de los sistemas inalámbricos de segunda y tercera generación, explica tecnologías como IP *tunneling*, seguridad, direccionamiento, las tecnologías de *tunneling* y etiquetado, y los servicios inalámbricos que proporcionan los proveedores de servicio. De alguna manera nos permite ver como ha evolucionado la tecnología de los sistemas y dispositivos inalámbricos y como está cambiando la forma de vida y trabajo de las personas.

Este trabajo constituye una buena referencia para todas aquellas personas que deseen conocer y entender la tecnología de las redes privadas virtuales.

ACRÓNIMOS

AAA	Authentication, Authorization, and Accounting
AAL5	ATM Adaptation Layer
ADM	Add/Drop Multiplexer
AH	Authentication Header
AMPS	Advanced Mobile Phone System
ANSI	American National Standards Institute
AP	Access Point
APN	Access Point Name
ARIB	Association of Radio Industries and Businesses
ARP	Address Resolution Protocol
ARQ	Automatic Repeat Request
AS	Autonomous System
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
AuC	Authentication Center
AVP	Attribute-Value Pair
BCP	Best Current Practice
BER	Bir Error Rate
BG	Border Gateway
BGP	Border Gateway Protocol
BHCA	Busy Hour Call Attempts
BSC	Base Station Controller
BSS	Basic Service Set
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CAMEL	Customized Applications for Mobile Network Enhanced Logic
CAP	CAMEL Application Part

CDMA	Code-Division Multiple Access
CdPA	Called Party Address
CDR	Charging Data Record
CE	Customer Edge
CEPT	Conference of European Posts and Telecommunications Administrations
CF	CompactFlash
CGF	Charging Gateway Function
CgPA	Calling Party Address
CHAP	Challenge Handshake Authentication Protocol
CK	Cipher Key
CLP	Cell Loss Priority
CN	Core Network (UMTS)
COPS	Common Open Policy Service
COPS-PR	Common Open Policy Service for Provisioning
CoS	Class of Service
CP	Control Plane
CPCS	Common Part Convergence Sublayer
CPE	Customer Premise Equipment
CRC	Cyclical Redundancy Check
CRL	Certificate Revocation List
CS	Circuit Switched
CSCF	Call State Control Function
CSD	Circuit-Switched Data
CSE	CAMEL Service Environment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DNS	Domain Name System

DoS	Denial of Service
DP	Detection Point
DPC	Destination Point Code
DRX	Discontinuous Reception
DS0	Digital Signal Level 0
DSSS	Direct-Sequence Spread Spectrum
DWDM	Dense Wavelength-Division Multiplexing
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data Rates for GPRS Evolution
EDP	Event Detection Point
EGPRS	Enhanced GPRS
EIR	Equipment Identity Register
EMS	Element Management System
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
ETSI-BRAN	ETSI Broadband Access Network
FA	Foreign Agent
FDD	Frequency Division Duplex
FDM	Fequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FEC	Forwarding Equivalence Class
FHSS	Frequency Hopping Spread Spectrum
FQDN	Fully Qualified Domain Name
FSK	Frequency-Shift Keying
FSM	Finite State Machine
FTP	File Transfer Protocol
Ga	Interface between SGSN and CGF or GGSN and CGF
Gb	Interface between the BSS and SGSN (2G GPRS)

GBN	GPRS Backbone Network
GBS	GPRS Backbone System
Gc	Interface between GGSN and HLR
G-CDR	GGSN-CDR
GERAN	GSM/EDGE Radio Access Network
Gf	Interface between SGSN and EIR
GGSN	Gateway GPRS Support Node
Gi	Reference Point between the GGSN and External Networks
GMM	GPRS Mobility Management
Gn	Interface between GGSN and SGSN or between SGSNs within a PLMN
Gp	Interface between GGSN and SGSN in different PLMNs
G-PDU	GTP Protocol Data Unit
GPRS	General Packet Radio Service
GPRS-CSI	GPRS CAMEL Subscription Information
GPRS SSF	GPRS Service Control Function
GPRS SS	GPRS Service Switching Function
Gr	Interface between SGSN and HLR
GRE	Generic Routing Encapsulation
GRX	GPRS Roaming Exchange
Gs	Interface between SGSN and MSC/VLR
GSM	Global System for Mobile Communications
GSM CCF	GSM Service Control Function
GSN	GPRS Support Node
GT	Global Title
GTP	GPRS Tunneling Protocol
GTP-C	GPRS Tunneling Protocol-Control Plane
GTP-U	GPRS Tunneling Protocol-User Plane
GTT	Global Title Translation

GUI	Graphical User Interface
HA	Home Agent
HLR	Home Location Register HPLMN – Home PLMN
HPMN	Home Public Mobile Network
HSCSD	High-Speed Circuit-Switched Data
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IBGP	Internet Border Gateway Protocol
ICMP	Internet Control Message Protocol
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identifier
IMS	IP Multimedia Subsystem
IMSI	International Mobile Station Identifier
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPLMN	Interrogating PLMN
IPSec	IP Security
IPv4	Internet Protocol Version 4.0
IPv6	Internet Protocol Version 6.0
IREG	International Roaming Expert Group
ISD	Insert Subscriber Data
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITU	International Telecommunications Union
ITU-T	ITU-Telecommunication Standardization Sector

Iu-cs	Interface between the RNC and UMTS Circuit Core Network
Iu-ps	Interface between the RNC and UMTS Packet Core Network
Iur	Interface between RNCs
IWF	Interworking Function
IW-MSC	Interworking MSC
IXC	Internet Exchange
L2F	Layer Two Forwarding
L2TP	Layer Two Tunneling Protocol
LA	Location Area
LAC	L2TP Access Concentrator
LAI	Location Area Identifier
LAN	Local Area Network
LAU	Location Area Update
LDAP	Lightweight Directory Access Protocol
LER	Label Edge Router
LLC	Logical Link Control
LMDS	Local Multipoint Distribution Services
LNS	L2TP Network Service
LSP	Label Switched Path
LSR	Label Switching Router
MAC	Media Access Control
MAP	GSM Mobile Application Part
MCC	Mobile Country Code
MIB	Management Information Base
MM	Mobility Management
MN	Mobile Node
MNC	Mobile Network Code
MNRF	Mobile Not Reachable Flag

MNRG	Mobile Not Reachable for GPRS Flag
MNRR	Mobile Not Reachable Reason
MoU	Memorandum of Understanding
MPLS	Multi-Protocol Label Switching
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Station ISDN
MT	Mobile Terminal
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
MVPN	Mobile Virtual Private Network
NAI	Network Access Identifier
NAPT	Network Address Port Translation
NAS	Network Access Server
NAT	Network Address Translation
NAT-PT	Network Address Translation-Protocol Translation
NAT-T	NAT-Transversal
NCP	Network Control Protocol
NEBS	National Equipment Building Specification
NI	Network Identifier
NIC	Network Interface Card
NM	Network Management
NMT	Nordic Mobile Telephone System
NNI	Network-to-Network Interface
N-PDU	Network Layer Protocol Data Unit
NSAP	Network Services Access Point
NSAPI	Network Services Access Point Identifier
NTP	Network Time Protocol

OA&M	Operations, Administration, and Maintenance
OFDM	Orthogonal Frequency-Division Multiplexing
OHG	Operators Harmonization Group
OSA	Open System Architecture
OSI	Open Systems Interconnection
PANA	Protocol for Carrying Authentication for Network Access
PAP	Password Authentication Protocol
PC	Personal Computer
PCF	Packet Control Function
PCMCIA	Personal Computer Memory Card International Association
PCO IE	Protocol Configuration Options Information Element
P-CSCF	Proxy CSCF
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDP	Packet Data Protocol
PDSN	Packet Data Serving Node
PDU	Protocol Data Unit
PE	Provider Edge
PIN	Personal Identity Number
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMM	Packet Mobility Management
PN N-PDU	Number Present Flag (in the GTP R99 header)
PPF	Paging Proceed Flag
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PRD	Public Reference Document
PS	Packet Switched

PSCN	Packet-Switched Core Network
PS-CP	Packet-Switched Control Plane
PSPDN	Packet-Switched Public Data Network
PSTN	Public Switched Telephone Network
PS-UP	Packet-Switched User Plane
P-TMSI	Packet TMSI
PVC	Permanent Virtual Circuit
QNC	Quick Net Connect
QoS	Quality of Service
R4	UMTS Release 4
R5	UMTS Release 5
R99	UMTS Release 99
RA	Routing Area
RAB	Radio Access Bearer
RAC	Routing Area Code
RADIUS	Remote Authentication Dial-In User Service
RAI	Routing Area Identifier
RAN	Radio Access Network
RANAP	Radio Access Network Application Part
RAS	Remote Access Server
RAU	Routing Area Update
RFC	Request for Comments
RIL3	Radio Interface Layer 3 Protocol
RLC	Radio Link Control
RNC	Radio Network Controller
RPDU	Relay Protocol Data Unit
RR	Radio Resource
RRC	Radio Resource Control

RRP	Registration Response
RRQ	Registration Request
RTOS	Real-Time Operating System
RTP	Real-Time Protocol
SA	Security Association
SAAL	Signaling ATM Adaptation Layer
SAD	Security Association Database
SAP	Service Access Point
SCCP	Signaling Connection Control Part
S-CDR	SGSN-CDR
SCP	Service Control Point
S-CSCF	Serving CSCF
SCTP	Simple Control Transmission Protocol
SDH	Synchronous Digital Hierarchy
SDO	Standard Definition Organization
SDU	Service Data Unit
SEP	Signaling End Point
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLIP	Serial Line Internet Protocol
SMC	Short Message Control
SMC-GP	Short Message Control-GPRS
SM-CP	Short Message Control Protocol
SMG	Special Mobile Group
SMR	Short Message Relay
SM-RP	Short Message Relay Protocol

SMS	Short Message Service
SMS-CI	SMS CAMEL Subscription Information
SMS-SC	SMS Service Center
SNDCP	Sub-Network Dependent Convergence Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPD	Security Policy Database
SRNC	Serving Radio Network Controller
SRNS	Serving Radio Network Subsystem
SSCF-NNI	Service-Specific Coordination Function at the Network Node Interface
SSCOP	Service-Specific Connection-Oriented Protocol
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSN	Sub-System Number
STP	Signal Transfer Point
TACS	Total Access Communication System
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TE	Terminal Equipment
TEID	Tunnel Endpoint Identifier
TFT	Traffic Flow Template
TI	Transaction Identifier
TIA/EIA	Telecommunications Industries Association/Electronic Industries Association
TID	Tunnel Identifier
TLD	Top Level Domain
TLS	Transport Level Security

TMSI	Temporary Mobile Subscriber Identifier
T-PDU	Payload of a GTP PDU
TPDU	Transfer Protocol Data Unit
TRNC	Target Radio Network Controller
TSG	Technical Standardization Group
TTA	Telecommunications Technology Association
TTC	Telecommunication Technology Committee
UDP	User Datagram Protocol
UDR	Usage Data Record
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
UMTS-CS	UMTS-Circuit Switched Domain
UMTS-PS	UMTS-Packet Switched Domain
UNI	User-to-Network Interface
UP	User Plane
URA	UTRAN Registration Area
USIM	UMTS Subscriber Identification Module
USSD	Unstructured Supplementary Services Data
UTRAN	UMTS Terrestrial Radio Access Network
Uu	Interface between MT and UTRAN
UWCC	Universal Wireless Communications Consortium
V&V	Verification and Validation
VC	Virtual Circuit
VHE	Virtual Home Environment
VLR	Visitor Location Register
VoIP	Voice over IP
VPLMN	Visited PLMN
VPN	Virtual Private Network

VSA	Vendor-Specific Attribute
WAN	Wide Area Network
WAP	Wireless Application Protocol
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wireline Equivalent Protocol
WG	Working Group
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN
WWW	World Wide Web

BIBLIOGRAFÍA

Libros

Black, U.
PPP and L2TP: Remote Access Communications
Prentice Hall
2000

Daoud Yacoub, M.
Wireless Technology. Protocols, Standards and Techniques
CRC PRESS
2002

Garg, V.
Wireless Network Evolution: 2G to 3G
Prentice Hall
2002

Goleniewski, L.
Telecommunications Essentials
Addison-Wesley
2003

Goodman, D.
Wireless Personal Communications Systems
Addison-Wesley
1997

Hjelm, J.
Designing Wireless Information Services
John Wiley
2000

Ibe, O. C.
Redes y Servicios de Acceso Remoto
John Wiley

Schiller, Jochen H.
Mobile Communications
Addison-Wesley
2000

Shneyderman, A. and Casati A.
Mobile VPN
John Wiley
2003

Stallings, W.
Data and Computer Communications
Prentice Hall
1988

Yuan, R., and T. Strayer.
Virtual Private Networks: Technologies and Solutions.
Addison-Wesley
2001

Artículos

Gupta, V., and S. Gupta
"Securing the Wieless Internet"
IEEE Communications Magazine, Volume 39, Issue 12
2001 (December)

Juha Ala-Laurilla, J., J. Mikkonen, and J. Rinnemaa
"Wireless LAN Access Network Architecture for Mobile Operators"
IEEE Communications Magazine,, Volume 39, Issue 11
2001 (August)

Park, J.
"Wireless Internet Access for Mobile Subscribers Based on the GPRS/UMTS Network"
IEEE Communications Magazine, Volume 40, Issue 4
2002 (April)

www

biblioteca.dgsca.unam.mx/cu/productos/boletines/msg00003.html

emisnet.bmv.com.mx/informes/infoanua_6024_2003.pdf

es.gsmbox.com/gsm/roaming/sp-roaming.gsmbox

m-trilogix.com/security/PDF/VPN.pdf

www.34t.com/box-docs.asp?area=76&suba=08&doc=635

www.amazon.com

www.computer.org/internet/v4n4/vpn.htm

www.estandaresabiertos.com/modules.php

www.ieee.org

www.infosol.com.mx/press/pr_virt/pk/micromuse.doc
www.itu.int

www.iusacell.com

www.lagnetwireless.net/modules.php

www.monografias.com/trabajos12/monvpn/monvpn.shtml

www.netmedia.info/business/articulos.php

www.sci.uma.es/sistemas/servinst/vpn/

www.servired.com.mx/modules.php

www.t1msn.com.mx/tecnologia/software/art287softdescwiless/Default.asp

www.telcel.com

www.telcel.net.ve/download/tecno/CDMA.pdf

www.telefonica.com

www.telefonos-moviles.com/articles/item.asp

www.unefon.com

www.uv.es/ciuv/cas/vpn/

www.uv.es/~montanan/redes/trabajos/VirtualPrivateNetwork.PDF