CAPÍTULO 6 – REDES PRIVADAS VIRTUALES

6.1.- Introducción.

Las tecnologías de información en Internet han cambiado la forma como las compañías se mantienen comunicadas con sus clientes, socios de negocios, empleados y proveedores. Inicialmente las compañías eran conservadoras con la información que publicaban en Internet, tal como, productos, disponibilidad de los mismos u otros ítems comerciales.

Pero recientemente, con el auge que ha tenido Internet, debido al cada vez menor costo que los usuarios tienen que pagar para acceder a esta gran red y con el significado que ésta ha adquirido como el principal medio mundial de comunicación, las redes privadas virtuales han hecho su aparición con más fuerza que nunca y se han ganado un espacio dentro del tan cambiante mundo de las redes de información.

Tradicionalmente, un enlace privado se ha hecho por medio de tecnologías WAN como X.25, Frame Relay, ATM, o enlaces conmutados. Ahora con el gran crecimiento de Internet, es posible usar un protocolo como IP, sin importar la tecnología WAN que lo soporte, para disfrutar de los servicios y ventajas que ofrecen las redes privadas. Y mientras que las tradicionales redes privadas se han hecho fuertes en las conexiones LAN-to-LAN, no han sido capaces de atacar el mercado de los usuarios individuales o pequeñas oficinas sucursales, y es aquí principalmente donde han surgido con fuerza las soluciones basadas en VPNs sobre IP, pues su implementación resulta sencilla y bastante económica.

Además el hecho de que las VPNs se construyan sobre infraestructuras públicas ya creadas ha hecho que las empresas ahorren más del 50% del costo que antes tenían que pagar en llamadas de larga distancia y en equipos físicos de acceso remoto o en alquiler de enlaces privados o dedicados.

6.2.- Descripción de una VPN.

Una VPN es una conexión que tiene la apariencia y muchas de las ventajas de un enlace dedicado pero trabaja sobre una red pública. Para este propósito usa una técnica llamada entunelamiento (tunneling), los paquetes de datos son enrutados por la red pública, como por ejemplo Internet, en un túnel privado que simula una conexión punto a punto. Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura. También hace universales para su transporte los diferentes protocolos LAN entre los que se encuentran IP, IPX, Appletalk y Netbeui, de ahí la característica de multiprotocolo que hace sumamente universal la tecnología de las redes virtuales privadas.

Las técnicas de entunelamiento básicamente consisten en encapsular los paquetes de datos que salen de una LAN o del equipo del usuario remoto dentro de protocolos que trabajan a nivel 2 de la torre OSI.

Los componentes básicos de un túnel son:

- Un iniciador del túnel
- Uno o varios dispositivos de enrutamiento
- Un conmutador de túneles (opcional)
- Uno o varios terminadores de túneles

El inicio y la terminación del túnel pueden ser hechos por una amplia variedad de equipos o software. Un túnel puede ser empezado, por ejemplo, por un usuario remoto con un ordenador portátil equipado con un modem analógico y un software de conexión telefónica para hacer una VPN, también puede haber un enrutador de una extranet en una oficina remota o en una LAN pequeña. Un túnel puede ser terminado por otro enrutador habilitado para tal fin, por un switch con esta característica o por un software que haga tal fin.

Adicionalmente y para completar una solución VPN deben existir uno o más dispositivos o paquetes de software que brinden cifrado, autenticación y autorización a los usuarios del túnel. Además muchos de estos equipos ofrecen información sobre el ancho de banda, el estado del canal y muchos más datos de gestión y de servicio.

La figura 6.1 muestra un diagrama detallado de una VPN dial-up usando PPTP como protocolo de entunelamiento. Se aprecian los trayectos en los cuales el protocolo que encapsula los datos es PPP y la parte del recorrido que es tunelizada usando PPTP.

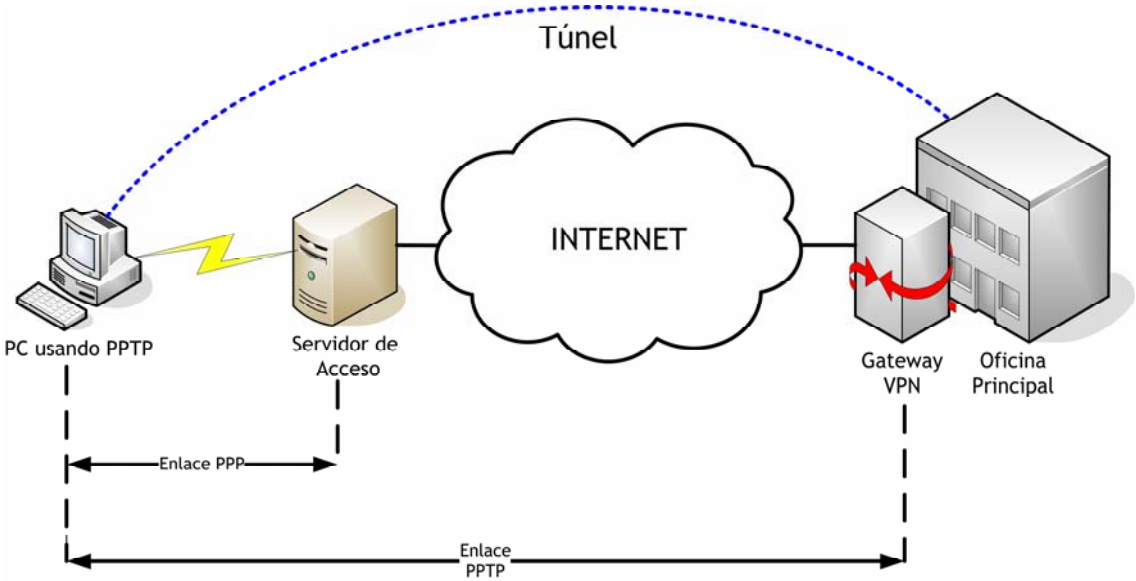

Figura 6.1: Esquema genérico VPN PPTP.

Una buena solución VPN requiere la combinación de tres componentes tecnológicos críticos: seguridad, control de tráfico y manejo empresarial.

Seguridad: Dentro de este punto destacan,

- el control de acceso, para garantizar la seguridad de las conexiones de la red
- el cifrado, para proteger la privacidad de los datos.
- la autenticación, para poder verificar acertadamente tanto la identidad de los usuarios como la integridad misma de la información.

Control de tráfico: que garantice solidez, calidad del servicio y velocidad. Las comunicaciones en Internet pueden llegar a ser excesivamente lentas, lo que las convertirían en soluciones inadecuadas en aplicaciones de negocios donde la rapidez es casi un imperativo. Aquí es donde entran parámetros como la prioridad de los datos y la garantización de ancho de banda.

Manejo empresarial: El componente final crítico en una VPN es el manejo empresarial que esta tenga. Se mide en una adecuada integración con la política de seguridad de la empresa, un manejo centralizado desde el punto inicial hasta el final, y la escalabilidad de la tecnología.

Las tres grandes arquitecturas VPN son las siguientes:

- **VPN de acceso remoto**

Éste es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

- **VPN punto a punto (LAN-to-LAN)**

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales.

- **VPN interna**

Es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo acceso remoto pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas.

Un ejemplo muy clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de habilitado pueda acceder a la información.

El objetivo final de una VPN es brindarle una conexión al usuario remoto como si este estuviera disfrutando directamente de su red privada y de los beneficios y servicios que dentro de ella dispone, aunque esta conexión se realice sobre una infraestructura pública.

6.3.- Tecnologías VPN

Básicamente, y desde el punto de vista de la torre OSI, se puede crear una VPN usando tecnologías de capa 2 (enlace) y de capa 3 (red). Dentro de la primera categoría están PPTP, L2F y L2TP, y en la segunda se encuentra IPSec. MPLS tiene características de las dos al ser una red conmutada que usa etiquetas para enrutar paquetes.

Para entender como funciona el proceso, es necesario tener en mente que lo que se persigue es poder encapsular protocolos en IP. Por ejemplo, en el caso de los protocolos de nivel 2, operan encapsulando la capa 2 de la torre OSI sobre IP. Es la forma de trabajar de PPP (Point to Point Protocol), normalmente usado para transportar IP y otros protocolos sobre enlaces serie entre un cliente y un host remoto. Se emplean PPTP, L2F y L2TP para crear túneles de conexiones PPP sobre Internet hasta un cliente remoto.

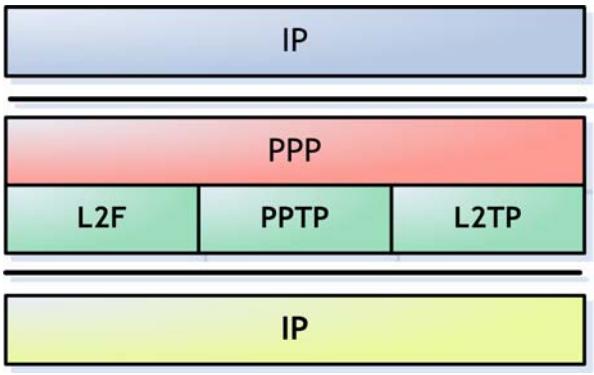

Figura 6.2: Torre tecnologías basadas en nivel 2.

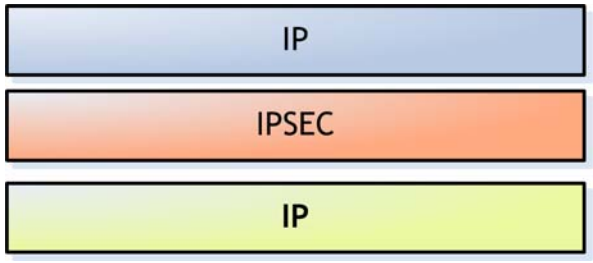

Figura 6.3: Torre tecnologías basadas en nivel 3.

6.3.1 PPTP (Point-to-Point Tunneling Protocol).

Es quizá el protocolo más sencillo de entunelamiento de paquetes. Usado, en general, por pequeñas empresas para realizar sus VPNs LAN-to-LAN, y en topologías de acceso remoto, para trabajadores teleconmutados, tales como vendedores externos o trabajadores que se mantienen en constante movimiento por fuera de sus oficinas.

El protocolo PPTP fue propuesto por el PPTP Forum, compuesto por 3Com, Ascend (ahora Lucent), Microsoft, ECI Telematics y USRobotics.
Debido a la integración que hizo Microsoft en sus sistemas operativos Windows NT, y luego en Windows 98 y posteriores, PPTP tuvo una gran acogida en el mercado mundial, de tal forma que un protocolo de capa 2 lanzado por Cisco Systems al mismo tiempo, prácticamente no llegó a conocerse, L2F (Layer-2-Forwarding)

El protocolo más comúnmente usado para acceso conmutado a Internet es el protocolo punto-a-punto (PPP).

PPTP soporta toda la funcionalidad que PPP le brinda a un acceso conmutado para construir sus túneles a través de Internet. PPTP encapsula paquetes PPP usando una versión modificada del protocolo GRE (Generic Routing Encapsulation). Dado lo anterior, PPTP no sólo es capaz de encapsular paquetes IP, sino IPX y NETBEUI, los protocolos de red local más usados.

La figura 6.4 muestra una conexión PPP entre un cliente y un RAS (Servidor de Acceso Remoto). Como se puede ver, es una conexión sencilla punto a punto donde lo primero que se realiza es una autenticación previa al envío y recibo de tramas PPP de datos.

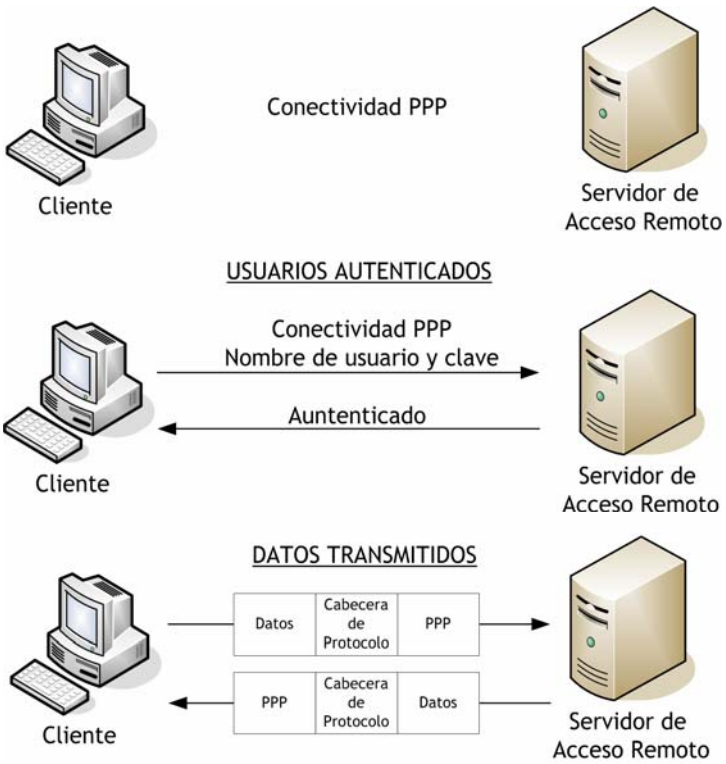

Figura 6.4: Conexión PPP entre un cliente un RAS

PPTP utiliza los mecanismos de autenticación que generalmente están asociados a PPP tales como PAP, EAP, CHAP, una versión mejorada de CHAP llamada MS-CHAP y desarrollada por Microsoft se encuentra en sus sistemas operativos Windows NT, 2000 y XP. Otra mejora que le ha hecho Microsoft al protocolo PPTP es la incorporación del método de cifrado MPPE (Microsoft Point-to-Point Encription).

Una de las ventajas que tiene PPTP por ser un protocolo de nivel 2, es que puede transmitir protocolos diferentes a IP en sus túneles, a diferencia de IPSec que se restringe a trabajar solamente con paquetes IP.

6.3.1.1.- Relación entre PPP y PPTP

PPP es el protocolo más comúnmente usado para acceso a Internet, prácticamente el único, puesto que SLIP casi ha desaparecido. PPP trabaja en la capa 2 de la torre OSI, la capa de enlace de datos, e incluye métodos para encapsular varios tipos de datagramas para ser transferidos sobre enlaces serie.

PPP tiene dos juegos de protocolos:

- Protocolo de Control de Enlace (LCP) que se encarga de las labores de establecimiento, configuración y prueba de la conexión

- Protocolos de Control de Red (NCPs) para el establecimiento y configuración de los diferentes protocolos de capa 3.

PPP es capaz de encapsular paquetes IP, IPX y NETBEUI en tramas PPP y enviar estos paquetes encapsulados de extremo a extremo (entre dos ordenadores, por ejemplo).

Para el establecimiento de una comunicación, cada extremo de un enlace PPP primero envía paquetes LCP para configurar y probar el enlace de datos; cuando un enlace PPP ha sido establecido, el usuario normalmente es autenticado (es una fase opcional en PPP, pero generalmente siempre es implementada).

La autenticación es un paso previo para comenzar la fase de control de protocolos de red. En PPP, la autenticación puede ser implementada mediante los siguientes protocolos: PAP, CHAP, MS-CHAP, MS-CHAPv2, EAP. Cabe resaltar que PAP envía las claves a través del enlace en texto plano, mientras que CHAP es un protocolo de autenticación un poco más robusto ya que el usuario interactúa con el sistema que le autentica respondiendo correctamente a algo que espera el host remoto, estos sistemas de autenticación son llamados de tres vías.

Después de que el enlace ha sido establecido y varias opciones han sido negociadas por el protocolo LCP, PPP envía paquetes NCP para escoger y configurar uno o más protocolos de capa de red. Después de que cada uno de

los protocolos de capa de red han sido configurados, los datagramas de cada uno de ellos pueden ser enviados sobre el enlace.

PPTP depende del protocolo PPP para crear la conexión conmutada entre el cliente y el servidor de acceso a la red. PPTP confía las siguientes funciones a PPP:

- Establecimiento y finalización de la conexión física.
- Autenticación de los usuarios.
- Creación de datagramas PPP.

Una vez que el enlace PPP es creado, el protocolo PPTP define dos tipos de paquetes diferentes: paquetes de control y paquetes de datos, cada uno de los cuales es asignado a diferentes canales lógicos. PPTP separa los canales de control y de datos, usando un flujo de control que corre sobre TCP y un flujo de datos que está encapsulado con cabeceras IP usando GRE. La conexión TCP es creada entre el cliente y el servidor PPTP. Esta conexión es usada para intercambiar mensajes de control.

Los paquetes de control son enviados periódicamente para indagar sobre el estado del enlace y las señales de manejo entre el cliente y el servidor PPTP. Los paquetes de control también se usan para enviar información de control básica del dispositivo y de configuración. Los mensajes de control establecen, mantienen y finalizan un túnel PPTP.
Los paquetes de datos contienen los datos del usuario, es decir, los datagramas del protocolo de capa de red usado.

Después de que el túnel PPTP se ha establecido, los datos del usuario son transmitidos entre el cliente y el servidor PPTP. Estos datos son transmitidos en datagramas IP contenidos dentro de los paquetes PPP. Los datagramas IP son creados usando una versión modificada del protocolo GRE (Generic Routing Encapsulation); esta modificación consiste en incluir un identificador de los hosts que puede ser usado para controlar los privilegios de acceso y la capacidad, la cual es usada para monitorizar la tasa de transferencia a la que los paquetes están transmitiéndose en el túnel.

La cabecera GRE es usada para encapsular el paquete PPP dentro del datagrama IP. La información útil del paquete es esencialmente el paquete PPP original enviado por el cliente. Dado que PPTP opera con un protocolo de capa 2, debe incluir una cabecera que depende del medio en el cual el túnel está transmitiendo, ésta puede ser Ethernet, Frame Relay o PPP. La figura 6.5 muestra la estructura en los diferentes sitios de un túnel de un paquete IP usando encapsulación PPTP desde el sistema cliente hasta la LAN corporativa.

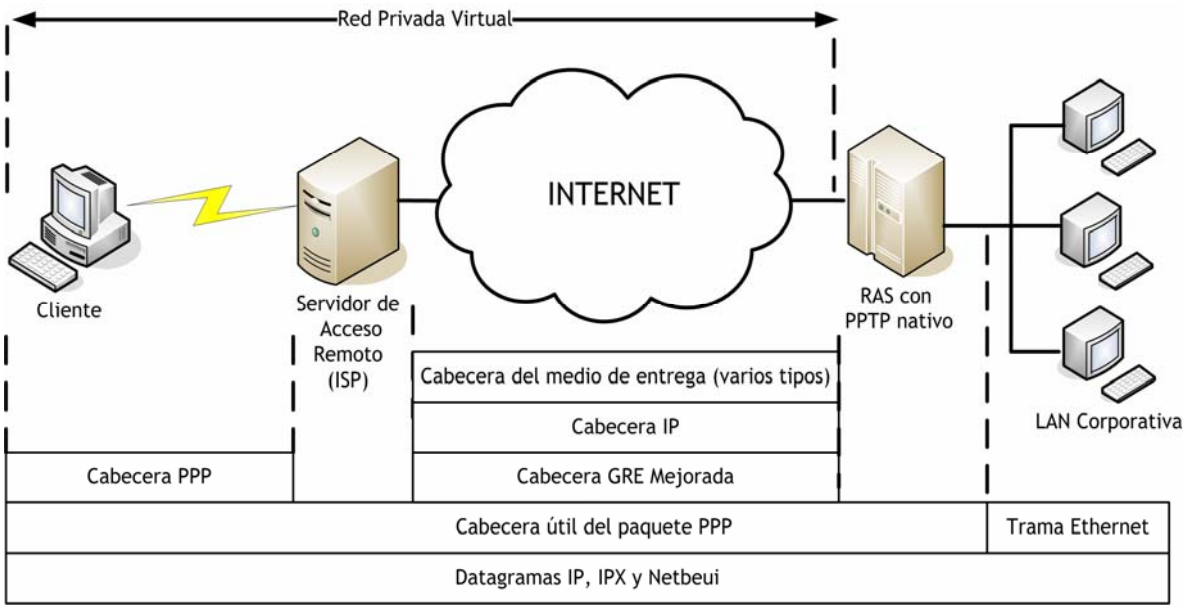

Figura 6.5: Formato paquetes entre las distintas partes de una VPN PPTP.

6.3.1.2.- Túneles.

PPTP permite a los usuarios y a los proveedores de servicios (ISPs, Internet Service Providers) crear varios tipos de túneles, basados en la capacidad del ordenador o equipo del usuario final y en el soporte del ISP para implementar PPTP. De esta manera, el ordenador del usuario final determina el lugar de terminación del túnel, bien sea en su propio equipo, si está ejecutando un cliente PPTP, o en el servidor de acceso remoto del ISP, si su máquina sólo soporta PPP y no PPTP. En este segundo caso el servidor de acceso del ISP debe soportar PPTP, a diferencia del primer caso, donde el proveedor de servicios no se involucra en ningún proceso de entunelamiento de datos.

Dado lo anterior, los túneles se pueden dividir en dos clases: voluntarios y permanentes.
Los túneles voluntarios son creados por requerimiento de un usuario y para un uso específico.
Los túneles permanentes son creados automáticamente sin la acción de un usuario y no le permiten escoger ningún tipo de privilegio.

En los túneles voluntarios, la configuración del mismo depende del usuario final, cuando se usan túneles de este tipo, el usuario puede simultáneamente acceder a Internet y abrir un túnel seguro hacia el servidor PPTP. En este caso el cliente PPTP reside en el equipo del usuario. Los túneles voluntarios proveen más privacidad e integridad de los datos que un túnel permanente. La figura 6.6 muestra un escenario de túneles voluntarios creados desde dos clientes distintos a un mismo servidor PPTP a través de Internet.

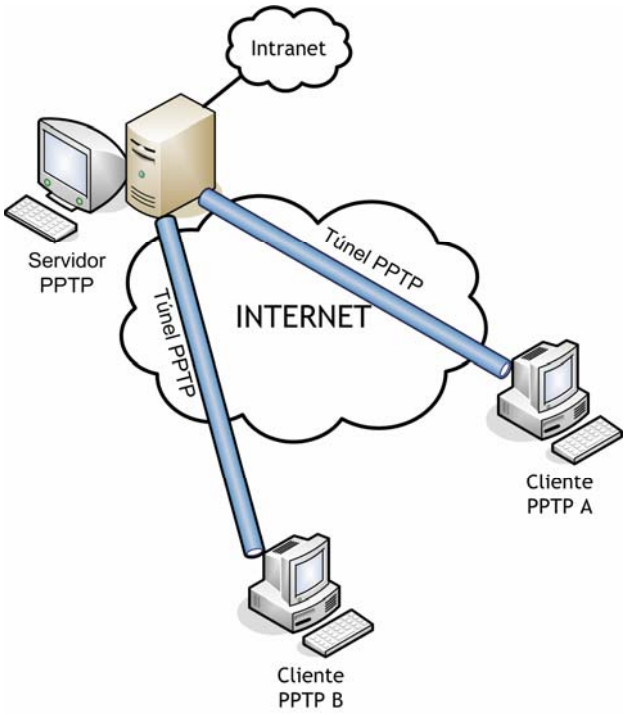

Figura 6.6: Túneles PPTP a un mismo servidor.

Los túneles permanentes son creados sin el consentimiento del usuario, por lo tanto, son transparentes para el mismo. El cliente PPTP reside en el servidor de acceso remoto del ISP al que se conectan los usuarios finales. Todo el tráfico originado desde el ordenador del usuario final es reenviado por el RAS sobre el túnel PPTP. En este caso la conexión del usuario se limita sólo a la utilización del túnel PPTP, no hay acceso a la red pública (Internet) sobre la cual se establece el túnel. Un túnel permanente PPTP permite que múltiples conexiones sean transportadas sobre el mismo túnel. La figura 6.7 muestra un túnel permanente entre un RAS con capacidad para encapsular sesiones PPP usando PPTP y por medio del cual van multiplexadas dos sesiones de clientes A y B.

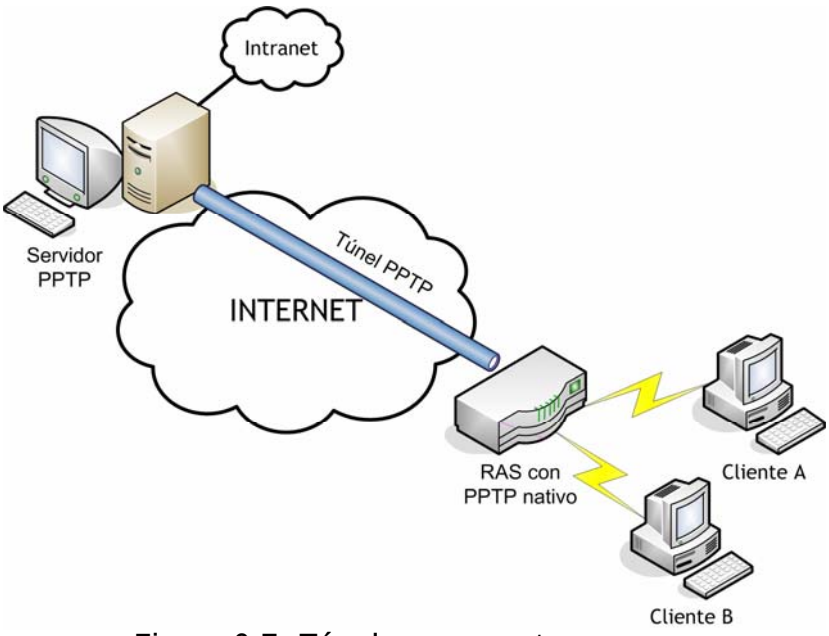

Figura 6.7: Túnel permanente.

Dado que los túneles permanentes tienen predeterminados sus puntos finales y que el usuario no puede acceder a Internet, estos túneles ofrecen mejor control de acceso que los túneles voluntarios. Otra ventaja de los túneles permanentes, es que reducen el ancho de banda utilizado, ya que múltiples sesiones pueden ser transportadas sobre un único túnel, a diferencia de los túneles voluntarios donde cada sesión tiene que trabajar con cabeceras independientes que ocupan un ancho de banda.
Una desventaja de los túneles permanentes es que la conexión inicial, es decir, entre el usuario final y el servidor de acceso que esta actuando como cliente PPTP, no hace parte del túnel, por lo tanto, puede ser vulnerable a un ataque.

Los túneles permanentes se dividen en estáticos y dinámicos.

Los túneles permanentes estáticos, son aquellos que requieren equipos dedicados y su configuración es manual. En este tipo de túneles el usuario final tiene a su disposición varios RAS, los cuales tienen establecidos diferentes túneles a diferentes servidores PPTP. Por ejemplo, si un usuario necesita hacer una VPN a su oficina regional ubicada en la ciudad A tiene que marcar un número X, pero si ese mismo usuario quiere hacer una VPN con su oficina en una ciudad B, tiene que marcar un número Y.

Los túneles permanentes dinámicos, usan el nombre del usuario para determinar el túnel asociado con él, es decir que se encargan de aprovechar mejor los recursos y el usuario puede marcar al mismo número para establecer túneles a diferentes sitios.
La información asociada con cada usuario puede residir en el servidor Radius en el que el servidor de acceso está autenticando todas las conexiones.

Claramente se observa que los túneles permanentes estáticos son más costosos que los dinámicos, ya que involucran un servidor de acceso por cada destino que un cliente VPN quiera alcanzar.

6.3.1.3. Tunneling LAN-to-LAN

Originalmente PPTP fue desarrollado pensando en brindar soluciones de acceso remoto VPN, es decir, proveer acceso conmutado seguro a redes locales corporativas vía Internet. Los túneles LAN-to-LAN no fueron soportados en un comienzo. Solo hasta el año 1997 cuando Microsoft introdujo su servicio de enrutamiento de acceso remoto (RRAS) para servidores NT 4.0, se pudieron implementar topologías LAN-to-LAN usando PPTP como protocolo de entunelamiento.

La implementación de Microsoft para entunelamiento LAN-to-LAN exige la presencia de dos servidores PPTP que tienen la función de hacer de gateways seguros de las dos redes locales.
Sin embargo, la gran desventaja de usar PPTP en topologías LAN-to-LAN es la inseguridad inherente a la arquitectura del protocolo. En efecto, la

autenticación y el cifrado son controlados por protocolos que ofrecen un nivel muy bajo de confiabilidad, como CHAP o MS-CHAP. La figura 6.8 muestra una topología de red LAN-to-LAN entre una pareja de servidores PPTP usando un túnel PPTP sobre Internet, para los usuarios tanto de la LAN corporativa A como de la B el túnel es transparente, y a nivel lógico se trabaja como en una única red local.

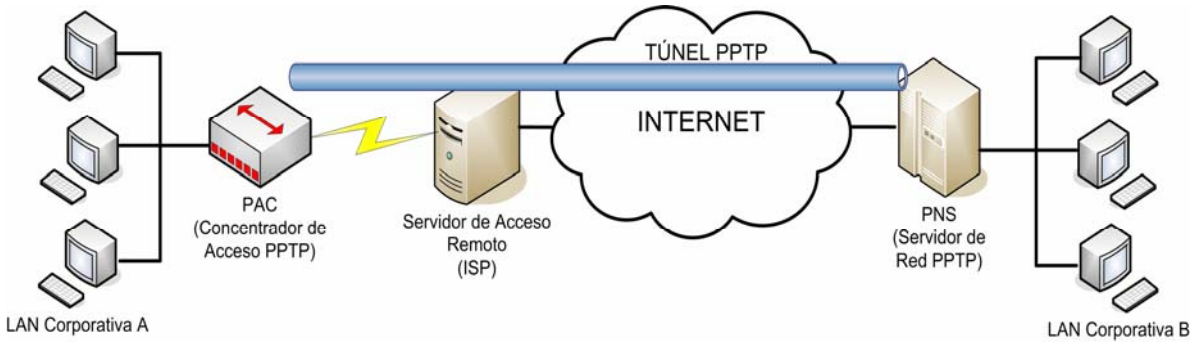

Figura 6.8: Topología LAN-to-LAN.

Para crear un túnel entre dos sitios, un servidor PPTP es autenticado por el otro usando contraseñas simples, algo similar a un usuario conmutado. En este caso, uno de los sitios actúa como el servidor PPTP y el otro como un cliente PPTP, de esta manera, un túnel voluntario es creado entre los dos extremos y por el mismo pueden existir varias sesiones.
Dado que un túnel PPTP puede encapsular varios protocolos de capa de red, los usuarios no tendrán acceso a los recursos, que cada protocolo le provee hasta que sus privilegios sean validados por el correspondiente protocolo.

6.3.1.4.- Componentes de una VPN PPTP.

Servidores PPTP.

Un servidor PPTP tiene dos funciones básicas: actuar como el punto final del túnel PPTP y reenviar los paquetes hacia y desde el ordenador en la red privada. Para reenviar los paquetes al ordenador destino, el servidor desencapsula el paquete PPTP obteniendo el nombre del computador o la dirección IP privada que se encuentra dentro de este.

Una de las características de los servidores PPTP es la de poder filtrar únicamente el tráfico PPTP dependiendo de si esta condición aparece o no en el perfil del usuario, de esta manera, se puede restringir a un usuario para que se conecte a la red local o se conecte a Internet.

En algunos casos el servidor PPTP está ubicado dentro de la red privada y está protegido por un cortafuegos o firewall. Cuando esto ocurre, es necesario abrir el puerto TCP 1723, o si el firewall permite filtrar no por puerto sino por protocolo, se deberá permitir el protocolo GRE.

Software cliente PPTP.

Como se dijo anteriormente, si el servidor de acceso a Internet del proveedor de servicios soporta PPTP no se necesita ningún software o hardware adicional en el extremo final del cliente, solamente que éste pueda establecer una conexión PPP.
Por otro lado, si el ISP no soporta PPTP, el cliente deberá utilizar un software cliente PPTP en su computador para poder crear el túnel. Para esto primero deberá establecer una conexión PPP marcando vía módem, y una vez esté establecida, deberá realizar una segunda conexión PPTP usando un puerto virtual proporcionado por el software cliente PPTP.

Todos los sistemas operativos Windows 95, Windows 98, Windows NT/2000/XP cuentan con un cliente PPTP nativo. También existen clientes PPTP para Linux.

Servidores de Acceso de Red.

Los servidores de acceso a la red (NAS), también llamados servidores de acceso remoto o concentradores de acceso, son los encargados de soportar las conexiones PPP de una gran cantidad de clientes que se conectan a este por medio de enlaces telefónicos conmutados.
Sus funciones van desde el establecimiento de la conexión física (modulación, demodulación, compresión de datos, corrección de errores, etc.) hasta labores de enrutamiento presentes en la capa 3 de la torre OSI.

Dentro de un túnel PPTP se pueden encontrar NAS actuando como clientes PPTP o simplemente como un concentrador de acceso PPP.
PPTP permite que las funciones realizadas por un servidor de acceso a la red sean separadas usando una arquitectura cliente-servidor. Comúnmente, las siguientes funciones son implementadas por un NAS:

- Brindar una interfaz física entre la red telefónica pública conmutada y los módems. Esto incluye conversiones A/D y D/A, conversiones síncronas a asíncronas y manipulaciones de flujos de datos.
- Terminación lógica de enlaces PPP.
- Autenticación de enlaces PPP.
- Multiplexión de canales (protocolo multilink PPP).
- Terminación lógica de protocolos de control de red (NCP).
- Enrutamiento multiprotocolo y bridging.

PPTP divide estas funciones entre los dos componentes que se definen en el protocolo, que son PAC y PNS.

El PAC o concentrador de acceso PPTP es el responsable de las dos primeras funciones y algunas veces de la tercera.

El PNS o servidor de red PPTP, es el responsable del resto de las funciones.

El protocolo PPTP es única y exclusivamente implementado entre el PAC y el PNS. Un PAC puede atender muchos PNSs. Un único PNS puede ser asociado a muchos PACs.

6.3.1.5.- Estructura del Protocolo.

PPTP define una conexión de control entre cada pareja PAC-PNS la cual opera sobre TCP; y un túnel IP operando sobre la misma pareja PAC-PNS el cual es usado para transportar paquetes PPP con encapsulamiento GRE.

Conexión de control.

Antes que el entunelamiento PPP ocurra entre un PAC y un PNS, una conexión de control debe ser establecida entre ellos. La conexión de control es una sesión TCP que mantiene control sobre la llamada e intercambia mensajes de información. Por cada pareja PAC-PNS debe existir una conexión de control y un túnel. La conexión de control es la responsable por el establecimiento, el manejo y la liberación de las sesiones que existen en el túnel.

El PNS y el PAC establecen la conexión de control usando los mensajes *Start-Control-Connection-Request* y *Start-Control-Connection-Reply*. Esos mensajes son también usados para intercambiar información básica entre los dos extremos del túnel. La conexión de control puede comunicar cambios entre las dos partes con un mensaje *Set-Link-Info*. Una sesión puede ser liberada por el PAC o por el PNS.

La conexión de control es mantenida por mensajes de eco *keep-alive*. Esto asegura que un fallo en la conectividad entre el PNS y el PAC pueda ser detectada con rapidez. Otras tipos de fallo pueden ser reportadas por mensajes *Wan-Error-Notify*.

PPTP define un conjunto de mensajes enviados como datos TCP en la conexión de control entre un PNS y un PAC. La sesión TCP es establecida en el puerto 1723. El puerto origen es asignado a cualquier número de puerto que no esté siendo usado en el momento del establecimiento del túnel.
Cada mensaje en la conexión de control PPTP comienza con una cabecera fija de ocho octetos, ésta cabecera contiene la longitud total del mensaje, un indicador del tipo de mensaje PPTP y una “magic cookie”.

Los tipos de mensajes de control de conexión definidos por el protocolo PPTP son: mensajes de control y mensajes de gestión; éstos últimos aún no se encuentran definidos y se han reservado para aplicaciones futuras.

La "magic cookie" es la constante 0x1A2B3C4D. Su función básica es asegurarle al receptor que está sincronizado con el flujo de datos TCP. La pérdida de sincronización no conlleva a una resincronización, sino a un cierre inmediato de la sesión TCP de la conexión de control.

Los mensajes de control definidos por el protocolo PPTP son:

Gestión de la conexión de control:
Start-Control-Connection-Request
Start-Control-Connection-Reply
Stop-Control-Connection-Request
Stop-Control-Connection-Reply
Echo-Request
Echo-Reply

Gestión de la llamada:
Outgoing-Call-Request
Outgoing-Call-Reply
Incoming-Call-Request
Incoming-Call-Reply
Incoming-Call-Connected
Call-Clear-Request
Call-Disconnect-Notify

Reporte de errores:
WAN-Error-Notify

Control de la sesión:
PPP Set-Link-Info

Comportamiento del túnel.

PPTP necesita el establecimiento de un túnel por cada pareja PNS-PAC.

Este túnel se utiliza para transportar todos los paquetes PPP de las diferentes sesiones involucradas en la pareja PNS-PAC. Una clave que se encuentra presente en la cabecera GRE indica qué paquetes PPP pertenecen a qué sesión.

De ésta manera, los paquetes PPP son multiplexados y desmultiplexados sobre un único túnel existente entre una pareja PNS-PAC. El valor del campo Clave es definido dentro del proceso de establecimiento de la llamada.

La cabecera GRE también contiene información de reconocimiento y de secuencialización con la cual se realiza control de congestión y detección de errores en el túnel.

Los datos del usuario transportados por el protocolo PPTP son esencialmente paquetes de datos PPP. Los paquetes PPP son transportados entre el PAC y el PNS, encapsulados en paquetes GRE los cuales a su vez son transportados sobre IP. Los paquetes encapsulados PPP son esencialmente

paquetes de datos PPP sin ningún elemento de tramado de medio específico. Los paquetes IP transmitidos sobre los túneles entre un PAC y un PNS tienen la estructura general que se muestra en la figura 6.9.

Figura 6.9: Estructura paquetes entre PAC y PNS.

Cabecera mejorada GRE

La cabecera GRE usada por PPTP es una versión ligeramente mejorada de la especificación estándar del protocolo GRE. La principal diferencia es la definición de un nuevo campo de reconocimiento de número (Acknowledgment Number), usado para determinar si un paquete particular GRE o un conjunto de paquetes han llegado al lado remoto del túnel.
Esta capacidad de reconocimiento no es usada en conjunto con ningún tipo de retransmisión, en vez de eso, se usa para determinar la tasa de transferencia a la cual los paquetes de datos del usuario son transmitidos sobre el túnel.

6.3.2 L2TP (Layer 2 Tunneling Protocol).

L2TP fue creado como el sucesor de PPTP y L2F. Las dos compañías abanderadas de cada uno de estos protocolos, Microsoft por PPTP y Cisco por L2F, acordaron trabajar en conjunto para la creación de un único protocolo de capa 2 y así lograr su estandarización por parte del IETF(Internet Engineering Task Force).

L2TP es usado por los Proveedores de Servicios de Internet (ISP) para permitir trabajar con VPNs sobre Internet. L2TP emerge de la fusión de las mejores características de los protocolos de túneles PPTP y L2F. L2TP es un protocolo de comunicación entre dispositivos de datos y es transparente a las aplicaciones de usuario.

Al igual que PPTP, L2F fue diseñado como un protocolo de entunelamiento usando para ello encapsulamiento de cabeceras. Una de las grandes diferencias entre PPTP y L2F, es que el entunelamiento de éste último no depende de IP y GRE, permitiéndole trabajar con otros medios físicos por ejemplo Frame Relay.
Paralelamente al diseño de PPTP, L2F utilizó PPP para autenticación de usuarios que accedan vía telefónica conmutada, pero también incluyó soporte para TACACS+ y Radius. Otra gran diferencia de L2F con respecto a PPTP es que permite que un único túnel soporte más de una conexión.

En L2F existen dos niveles de autenticación del usuario:

- Por el ISP antes de crear el túnel

- Por la pasarela o gateway corporativa cuando la conexión está configurada.

Todas las anteriores características de L2F han sido transportadas a L2TP. Como PPTP, L2TP utiliza la funcionalidad de PPP para proveer acceso conmutado que puede ser tunelizado a través de Internet a un sitio destino. Sin embargo, como se ha mencionado anteriormente, L2TP define su propio protocolo de entunelamiento basado en L2F permitiendo transporte sobre una amplia variedad de medios de empaquetamiento tales como X.25, Frame Relay y ATM.

Dado que L2TP es un protocolo de capa 2, ofrece a los usuarios la misma flexibilidad de PPTP de soportar otros protocolos aparte de IP, tales como IPX y NETBEUI.

Puesto que L2TP usa PPTP en enlaces conmutados, incluye mecanismos de autenticación nativos de PPP como PAP y CHAP.

Microsoft incluye L2TP a partir del sistema operativo Windows 2000, ya que las mejoras de L2TP con respecto a PPTP son muchas.

6.3.2.1 Componentes básicos de un túnel L2TP.

Concentrador de acceso L2TP (LAC)

Un LAC es un nodo o dispositivo físico que se añade a los elementos de interconexión de la red conmutada, o bien se coloca con un sistema de terminación PPP capaz de gestionar el protocolo L2TP, y se encuentra en un punto extremo de un túnel L2TP. El LAC se ubica entre un LNS (Servidor de red L2TP) y un sistema remoto, y reenvía los paquetes hacia y desde cada uno de esos elementos. Los paquetes enviados desde el LAC hasta el LNS van tunelizados. El LAC es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes. En algunas ocasiones el sistema remoto actúa como un LAC, esto ocurre cuando cuenta con un software cliente LAC.

Servidor de Red L2TP (LNS)

Un LNS es un nodo que se encuentra en un punto extremo de un túnel L2TP y que interactúa con el LAC, o punto final opuesto. El LNS es el punto lógico de terminación de una sesión PPP que está siendo tunelizada desde un sistema remoto por el LAC. El LNS también se conoce como Home Gateway (HGW).

Túnel

Un túnel existe entre una pareja LAC-LNS. El túnel consiste de una conexión de control y de ninguna o más sesiones L2TP. El túnel transporta datagramas PPP encapsulados y mensajes de control entre el LAC y el LNS.

6.3.2.2.- Topología L2TP.

La figura 6.10 describe un escenario típico L2TP. El objetivo es tunelizar tramas L2TP entre un sistema remoto o un cliente LAC y un LNS localizado en la LAN corporativa.

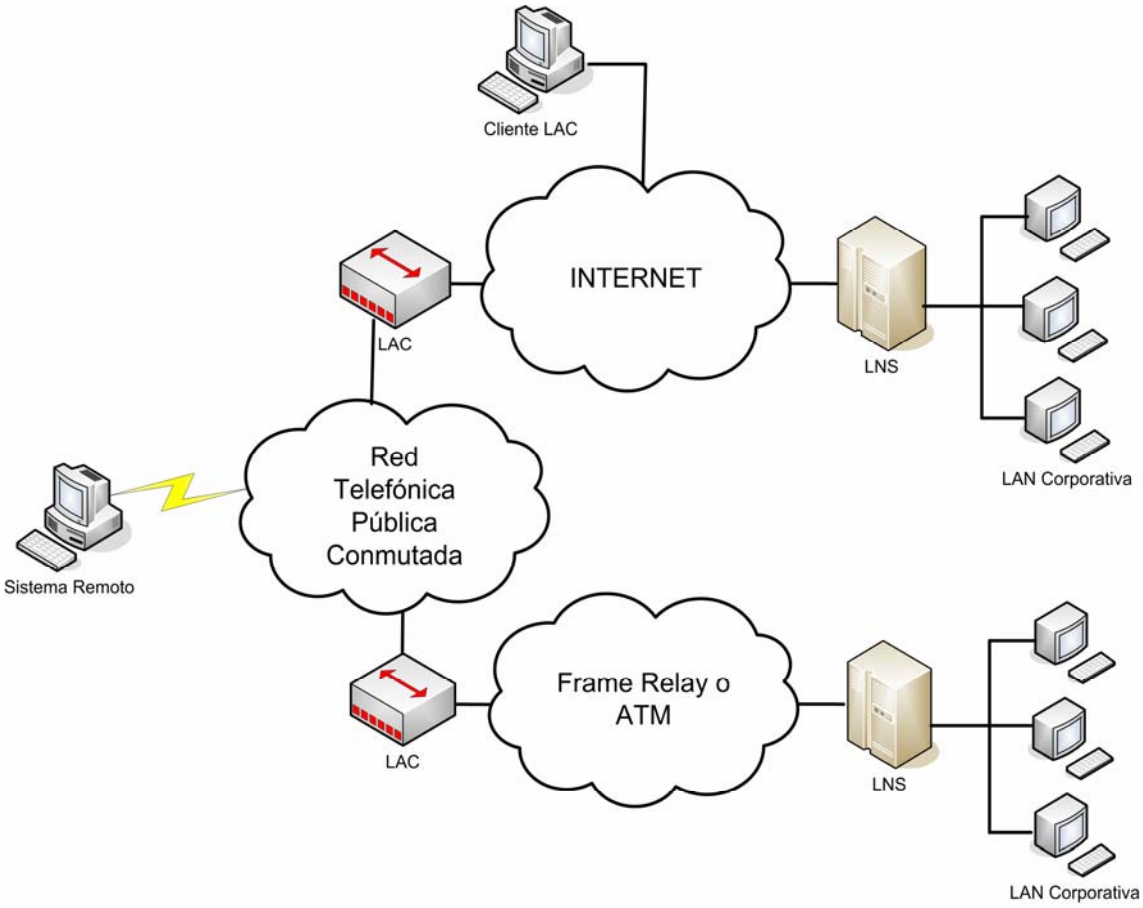

Figura 6.10: Escenario L2TP.

La conexión entre un usuario remoto, el LAC del ISP y el LNS en la red de área local usando un túnel L2TP se establece mediante los siguientes pasos:

1) El sistema remoto inicia una conexión PPP a través de la red telefónica conmutada a un LAC.

2) El LAC en el ISP acepta la conexión y se establece el enlace PPP.

3) El LAC autentica parcialmente al usuario remoto, por ejemplo, mediante CHAP o PAP. El nombre de usuario, nombre de dominio o el número marcado de identificación de servicio (DNIS, Dialed Number Identificación Service) se usa para determinar si el usuario es un cliente VPN. Si no lo es, la autenticación continúa y el cliente tendrá acceso a Internet o cualquier otro servicio contratado. Si se trata de un usuario VPN se mapeará un determinado punto de terminación (concretamente el LNS destino)

4) Los puntos finales del túnel, LAC y LNS, se autentican entre ellos antes de que se intente crear una sesión en el túnel. Alternativamente, el LNS puede aceptar la creación de un túnel sin autenticar otro anterior.

5) Una vez que existe el túnel, se crea una sesión L2TP de la que hará uso el usuario final.

6) El LAC propagará las opciones LCP negociadas (correspondientes al enlace de control) y la autenticación parcial al LNS. Éste transmitirá esa información directamente al interfaz virtual de acceso. Si las opciones configuradas en la interfaz no se corresponden con las opciones del LAC, la conexión fallará y se enviará un mensaje de desconexión al LAC.

7) El resultado final parece que se trata de una negociación directa entre el cliente y el LNS, pero el LAC actúa como dispositivo intermedio.

Un cliente LAC (un host que corre L2TP nativo) puede también crear un túnel hasta la LAN corporativa sin usar un LAC externo. En este caso, el host tiene un software cliente LAC y se encuentra conectado a la red pública. Una conexión PPP virtual es creada posteriormente y el software cliente LAC hace un túnel hasta el cliente LNS. El direccionamiento, la autenticación, la autorización y el accounting pueden ser proporcionados por el dominio de la LAN corporativa remota.

6.3.2.3.- Estructura del protocolo L2TP.

L2TP utiliza dos tipos de mensajes:

- Mensajes de control, usados en el establecimiento, mantenimiento y finalización de túneles y llamadas.

- Mensajes de datos, usados para encapsular tramas PPP que está siendo transportadas sobre el túnel.

Los mensajes de control utilizan un canal de control fiable con el cual L2TP garantiza la entrega. Los mensajes de datos no son retransmitidos cuando ocurren pérdidas de paquetes.

La figura 6.11 muestra la relación de las tramas PPP y los mensajes de control con los canales de datos y control L2TP respectivamente. Las tramas PPP son transportadas sobre un canal de datos no fiable y son encapsuladas primero por una cabecera L2TP y luego por una cabecera de transporte de paquetes que pueden ser UDP, Frame Relay o ATM.

Los mensajes de control son enviados sobre un canal de control L2TP fiable, el cual transmite paquetes en banda sobre el mismo transporte de paquetes. Para esto se requiere números de secuencia que estén presentes en

todos los mensajes de control. Los mensajes de datos pueden usar esos números de secuencia para reordenar paquetes y detectar pérdidas de los mismos.

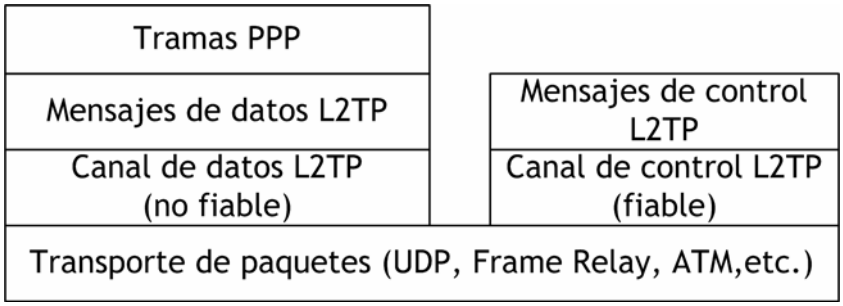

Figura 6.11: Relación tramas PPP con mensajes de control y datos.

Formato de una la cabecera L2TP

Los paquetes L2TP para el canal de control y el canal de datos comparten un formato de cabecera común. La figura 6.12 muestra el formato de una cabecera L2TP. A continuación irían los datos.

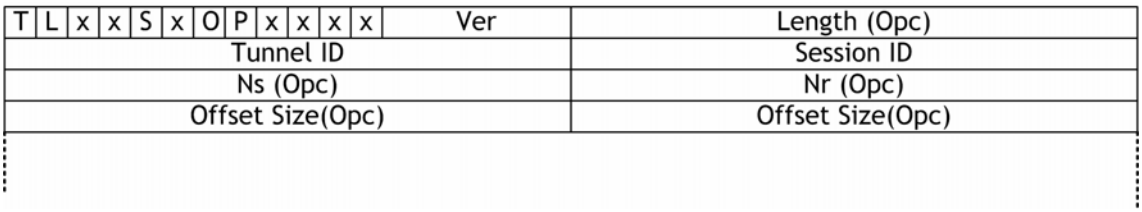

Figura 6.12: Estructura cabecera L2TP

El bit T (tipo), indica el tipo de mensaje, es 0 para un mensaje de datos y 1 para un mensaje de control.

Si el bit L (longitud) es 1, el campo Longitud está presente. Este bit debe estar puesto en 1 para los mensajes de control.

Los bits x son reservados para futuras extensiones. Todos los bits reservados deben ser puestos en 0 para los mensajes salientes y deben ser ignorados por el receptor.

Si el bit S (secuencia) vale 0, los bits Ns y Nr estarán presentes. El bit S debe estar puesto en 1 para los mensajes de control.

Si el bit O (offset) es 1, el campo de tamaño Offset está presente. El bit O debe estar puesto a 0 para los mensajes de control.

Si el bit P (prioridad) es 1, los mensajes de datos deben recibir un trato preferencial en las colas locales y en la transmisión. Las peticiones echo LCP usados como keepalive para el enlace deben generalmente ser enviados con este bit puesto en 1 dado que un intervalo de tiempo grande originado por una conexión local puede originar una demora en los mensajes keepalive ocasionando una pérdida innecesaria del enlace. Esta característica es solamente usada por los mensajes de datos. El bit P debe ser puesto en 0 para todos los mensajes de control.

El campo Ver debe valer '2' e indicar la versión de la cabecera L2TP de los mensajes de datos. Los paquetes recibidos con un campo Ver desconocido deben ser descartados.

El campo Length indica la longitud total del mensaje en octetos.

El campo Tunnel ID sirve como identificador para el control de conexión. Los túneles L2TP son nombrados por identificadores que tienen significado local únicamente.

El campo Session ID indica el identificador para una sesión dentro del túnel. Al igual que los identificadores de túnel, las sesiones L2TP son nombradas por identificadores que tienen únicamente significado local.

El campo Ns indica el número de secuencia para los mensajes de datos y de control.

El campo Nr indica el número de secuencia esperado en el siguiente mensaje de control a ser recibido. En los mensajes de datos el campo Nr está reservado, y si está presente debe ser ignorado.

Si el campo Offset Size está presente, especifica el número de octetos después de la cabecera L2TP, a partir de los cuales la carga útil de datos es esperada a que inicie o a que se encuentre.

Tipos de mensajes de control

El protocolo L2TP define los siguientes tipos de mensajes de control para la creación, mantenimiento y finalización del túnel.

Manejo de la conexión de control

0 (reserved)
1 (SCCRQ) Start-Control-Connection-Request
2 (SCCRP) Start-Control-Connection-Reply
3 (SCCCN) Start-Control-Connection-Connected
4 (StopCCN) Stop-Control-Connection-Notification
5 (reserved)
6 (HELLO) Hello

Manejo de la llamada

7 (OCRQ) Outgoing-Call-Request
8 (OCRP) Outgoing-Call-Reply

9 (OCCN) Outgoing-Call-Connected
10 (ICRQ) Incoming-Call-Request
11 (ICRP) Incoming-Call-Reply
12 (ICCN) Incoming-Call-Connected
13 (reserved)
14 (CDN) Call-Disconnect-Notify

Reporte de errores
15 (WEN) WAN-Error-Notify

Control de la sesión PPP
16 (SLI) Set-Link-Info

Funcionamiento del protocolo

Para tunelizar una sesión PPP con L2TP se necesita llevar a cabo dos pasos:

- El establecimiento de una conexión de control para el túnel.

- El establecimiento de una sesión respondiendo a la petición de una llamada entrante o saliente.

El túnel y su correspondiente conexión de control deben ser establecidos antes que una llamada entrante o saliente sea iniciada. Una sesión L2TP debe ser establecida antes que L2TP pueda empezar a enviar por el túnel tramas PPP. Múltiples sesiones pueden existir a través de un túnel único y múltiples túneles pueden existir entre el mismo LAC y LNS.

La figura 6.13 ilustra la relación que puede existir entre un LAC y un LNS, claramente se notan los puntos terminales de un enlace PPP de una sesión L2TP, de una conexión de control L2TP y del túnel en sí. Muestra cómo se introducen en el túnel tramas PPP usando L2TP

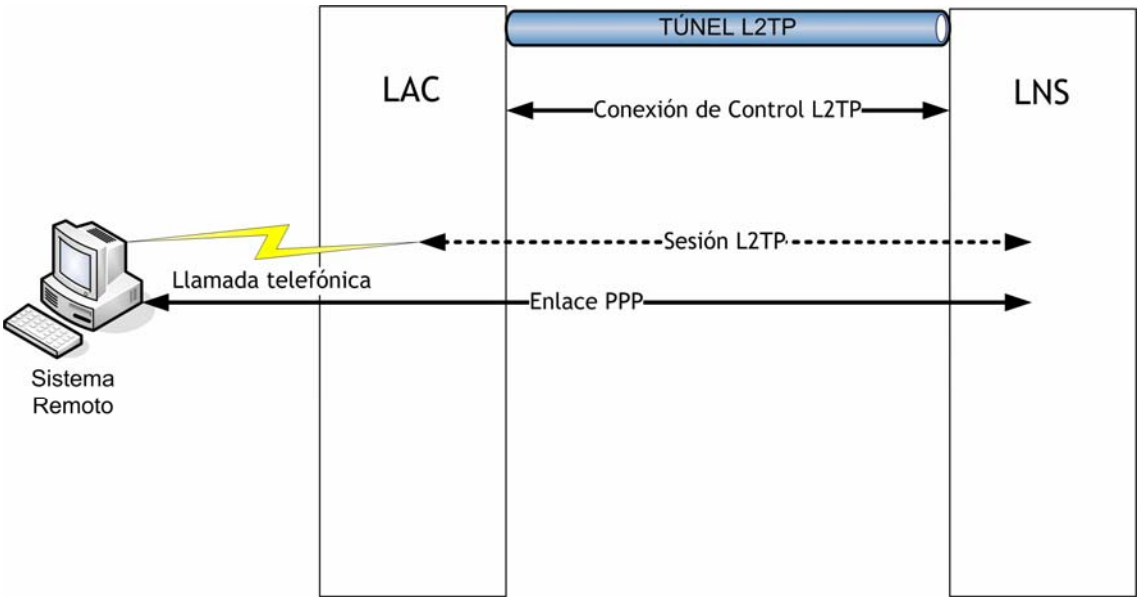

Figura 6.13: Entunelamiento de tramas PPP usando L2TP.

Veamos los distintos pasos por los que atraviesa una conexión L2TP:

- Establecimiento de la conexión de control.

La conexión de control es la conexión inicial que debe llevarse a cabo entre un LAC y un LNS antes que puedan crearse sesiones a través de ésta.

El establecimiento de la conexión de control incluye la verificación de la identidad del extremo remoto entre otros. Un intercambio de tres mensajes como se muestra en la figura 6.14 es utilizado para configurar la conexión de control.

El mensaje ZLB ACK es enviado si no hay más mensajes esperando en cola para ese extremo.

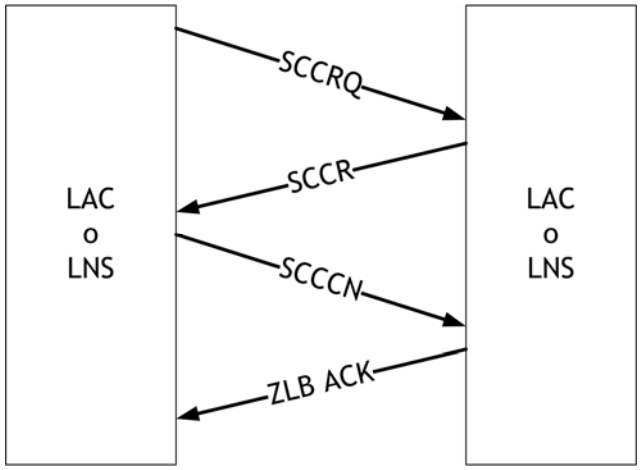

Figura 6.14: Establecimiento de una conexión de control.

- Autenticación del túnel.

L2TP incorpora un sistema de autenticación simple y opcional parecido a CHAP durante el establecimiento de la conexión de control.
Si un LAC o LNS desea autenticar la identidad de su pareja, éste le envía una petición en el mensaje SCCRQ o SCCRP, a lo cual su pareja responde en otro SCCRP o SCCCN respectivamente. Si la respuesta enviada y la respuesta recibida de su pareja no concuerdan, el establecimiento del túnel no será permitido.

- Establecimiento de la sesión.

Después del establecimiento exitoso de la conexión de control, sesiones individuales pueden ser creadas. Cada sesión corresponde a un único flujo PPP entre el LAC y el LNS.
A diferencia del establecimiento de la conexión de control, el establecimiento de la sesión es direccional con respecto al LAC y al LNS. El LAC solicita al LNS aceptar una sesión para una llamada entrante, y el LNS solicita al LAC aceptar una sesión para una llamada saliente.

- Establecimiento de una Llamada Entrante.

La figura muestra la secuencia típica de intercambio de tres mensajes para configurar la sesión.

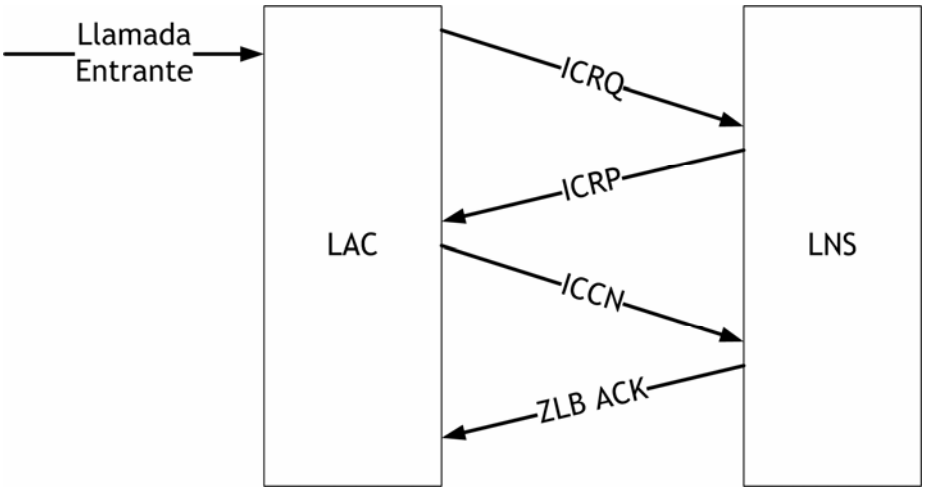

Figura 6.15: Establecimiento de una llamada entrante.

El ZLB ACK es enviado si no hay más mensajes esperando en cola para la pareja remota.

- Establecimiento de una Llamada Saliente.

La figura muestra la secuencia típica de intercambio de tres mensajes para configurar la sesión.

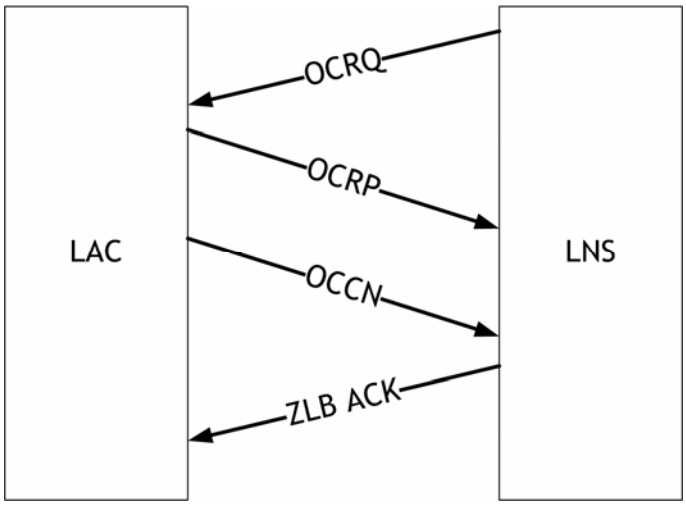

Figura 6.16: Establecimiento de una llamada saliente.

El ZLB ACK es enviado si no hay más mensajes esperando en cola para la pareja remota.

Reenvío de tramas PPP

Una vez que el establecimiento del túnel se ha completado, las tramas PPP desde el sistema remoto son recibidas en el LAC, encapsuladas en L2TP y reenviadas sobre el túnel apropiado. El LNS recibe el paquete L2TP y procesa la trama PPP encapsulada como si fuera recibida en una interfaz PPP local.

El emisor de un mensaje asociado con una sesión y un túnel particular, coloca el identificador de sesión y de túnel en los campos Session ID y Tunnel ID de la cabecera para todos los mensajes salientes. De ésta manera, las tramas PPP son multiplexadas y desmultiplexadas sobre un único túnel entre una pareja LNS-LAC.

El valor '0' para el Session ID y Tunnel ID es especial y no debe ser usado. Para los casos donde el Session ID no ha sido aún asignado (por ejemplo durante el establecimiento de una nueva sesión o túnel), el campo Session ID debe ser enviado como 0, igualmente, para los casos donde el Tunnel ID aún no ha sido asignado desde el nodo remoto.

Uso de números de secuencia en el canal de datos.

Los números de secuencias son definidos en la cabecera L2TP para los mensajes de control y opcionalmente para los mensajes de datos. Estos son usados para proporcionar un transporte fiable a los mensajes de control y una secuencialización opcional para los mensajes de datos. Cada nodo mantiene una secuencia de números diferentes para la conexión de control y para cada sesión de datos individual dentro del túnel.

A diferencia del canal de control L2TP, el canal de datos no usa números de secuencia para retransmitir mensajes de datos perdidos, en vez de éstos, los mensajes de datos pueden usar números de secuencia para detectar paquetes perdidos y/o restaurar la secuencia original de paquetes que se ha perdido durante el transporte.

El LAC, le puede solicitar al LNS que la secuencia de números esté presente en los mensajes de datos. El LNS controla el envío o no de la secuencia de números. S

Si el LAC recibe mensajes de datos sin la secuencia de números presente, éste deberá parar cualquier secuencia de datos futura.

Si el LAC recibe mensajes de datos con una secuencia de números presente, este deberá comenzar a enviar números de secuencia en todos los mensajes de datos salientes futuros.

Estos procesos de habilitar o deshabilitar la secuencia de números puede ocurrir en cualquier momento de la transferencia de paquetes. Es recomendable activar esta característica en todos los LNS para asegurar un correcto ordenamiento de todos los paquetes entrantes.

Keepalive (Hello)

El mecanismo de keepalive es empleado por L2TP para detectar periodos extensos de no control o inactividad de datos en el túnel.

Se realiza enviando mensajes de control Hello después de que un periodo de tiempo específico ha transcurrido desde que el último mensaje de control o de datos fue recibido en el túnel.

Como con cualquier otro mensaje de control, si el mensaje Hello no es recibido oportunamente el túnel es declarado inactivo y es reconfigurado.

Con este mecanismo se asegura que cualquier fallo de conectividad entre el LNS y el LAC sea detectado oportunamente por ambos lados del túnel.

- Terminación de la sesión

Tanto el LAC como el LNS pueden terminar una sesión, esto se logra por medio de un mensaje de control CDN, la figura 6.17 es un ejemplo típico del intercambio de mensajes de control para terminar una sesión.

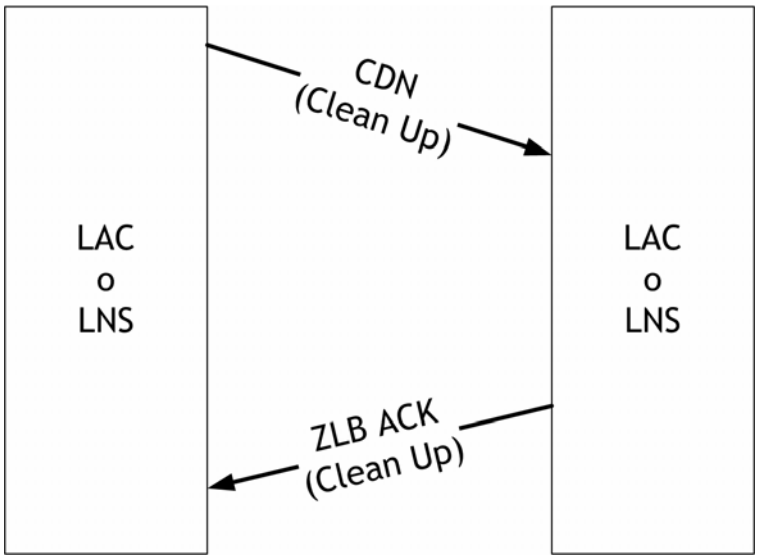

Figura 6.17: Terminación de la sesión.

- Terminación de la conexión de control

Al igual que con una sesión, la conexión de control puede ser finalizada por el LAC o por el LNS, se realiza enviando un mensaje de control StopCCN. La figura 6.18 ilustra el intercambio de mensajes de control entre un LAC y un LNS necesarios para terminar una conexión de control.

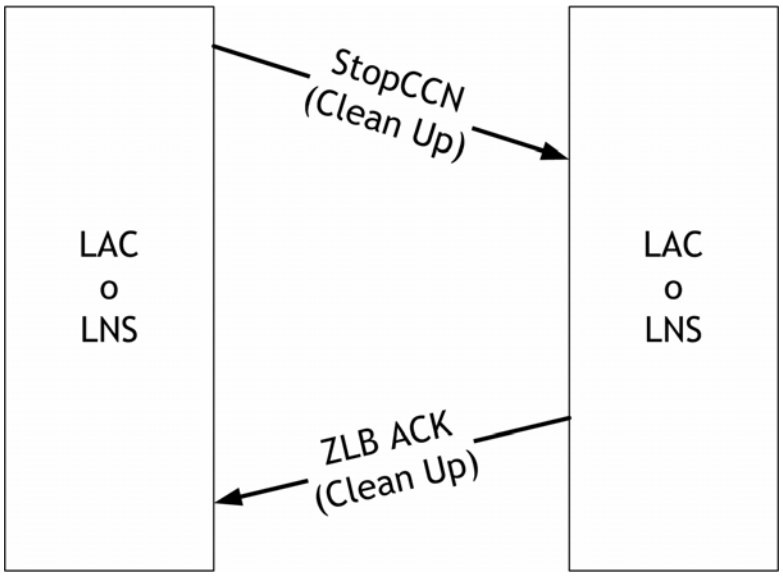

Figura 6.18: Terminación de la conexión de control.

Para terminar el túnel y todas las sesiones en él, es necesario solamente el envío de un StopCCN, no se necesita bajar sesión por sesión individualmente.

6.3.3.- IPSEC.

En IPv4 no se desarrollaron mecanismos de seguridad inherentes al protocolo, por tanto, protocolos y procedimientos adicionales a IPv4 fueron necesarios para brindar servicios de seguridad a los datos.

IPSec (Internet Protocol Security) es un conjunto de protocolos diseñados para proveer una seguridad basada en criptografía robusta para IPv4 e IPv6, de hecho IPSec está incluido en IPv6.

Entre los servicios de seguridad definidos en IPSec se encuentran:
- control de acceso.
- integridad de datos.
- autenticación del origen de los datos.
- protección frente a duplicados.
- confidencialidad en los datos.

Entre las ventajas de IPSec están la modularidad del protocolo, ya que no depende de un algoritmo criptográfico específico.

6.3.3.1 Componentes de IPSec

IPSec está compuesto por tres componentes básicos:

- los protocolos de seguridad (AH y ESP)
- las asociaciones de seguridad (SAs)

- las bases de datos de seguridad

cada uno de los cuales, trabaja sirviéndose de los demás y ninguno le resta importancia al otro.

1) Protocolos de Seguridad

IPSec es un conjunto de protocolos que provee varios servicios de seguridad. Esos servicios de seguridad trabajan gracias a dos protocolos, el Authentication Header (AH) y el Encapsulating Security Payload (ESP), y también al uso de protocolos y procedimientos para el manejo de llaves criptográficas tales como IKE (Internet Key Exchange Protocol).

El éxito de una implementación IPSec depende en gran medida de una adecuada elección del protocolo de seguridad y de la forma en cómo se intercambian las llaves criptográficas.

AH es un protocolo que añade una nueva cabecera justo después de la cabecera IP original. AH provee autenticación del origen de los datos e integridad de los mismos, también provee integridad parcial para prevenir ataques de repetición. Este protocolo es apropiado cuando se requiere autenticación en vez de confidencialidad.

ESP provee confidencialidad para el tráfico IP, al igual que autenticación tal cual como lo hace AH, pero solo uno de estos servicios puede ser proporcionado por ESP al mismo tiempo.

IKE es un protocolo que permite a dos entidades IPSec negociar dinámicamente sus servicios de seguridad y sus llaves de cifrado al igual que la autenticación de la sesión misma.

2) Asociaciones de Seguridad (SAs)

El concepto de asociación de seguridad (SA) es clave en IPSec.

Una SA define las medidas de seguridad que deberían ser aplicadas a los paquetes IP basados en quién los envía, hacia dónde van y qué tipo de carga útil transportan. El conjunto de servicios de seguridad ofrecidos por una SA dependen de los protocolos de seguridad y del modo en el cual ellos operan definidos por la SA misma. La figura 6.19 muestra los dos modos en los cuales un protocolo de seguridad puede operar: transporte y túnel; la diferencia radica en la manera como cada uno de ellos altera el paquete IP original.

El modo de transporte es diseñado para proteger los protocolos de capas superiores tales como TCP y UDP. En modo túnel, el paquete IP original se convierte en la carga útil de un nuevo paquete IP. Esto le permite al paquete IP inicial, "ocultar" su cabecera IP para que sea encriptada, considerando que el paquete IP externo sirve de guía a los datos a través de la red.

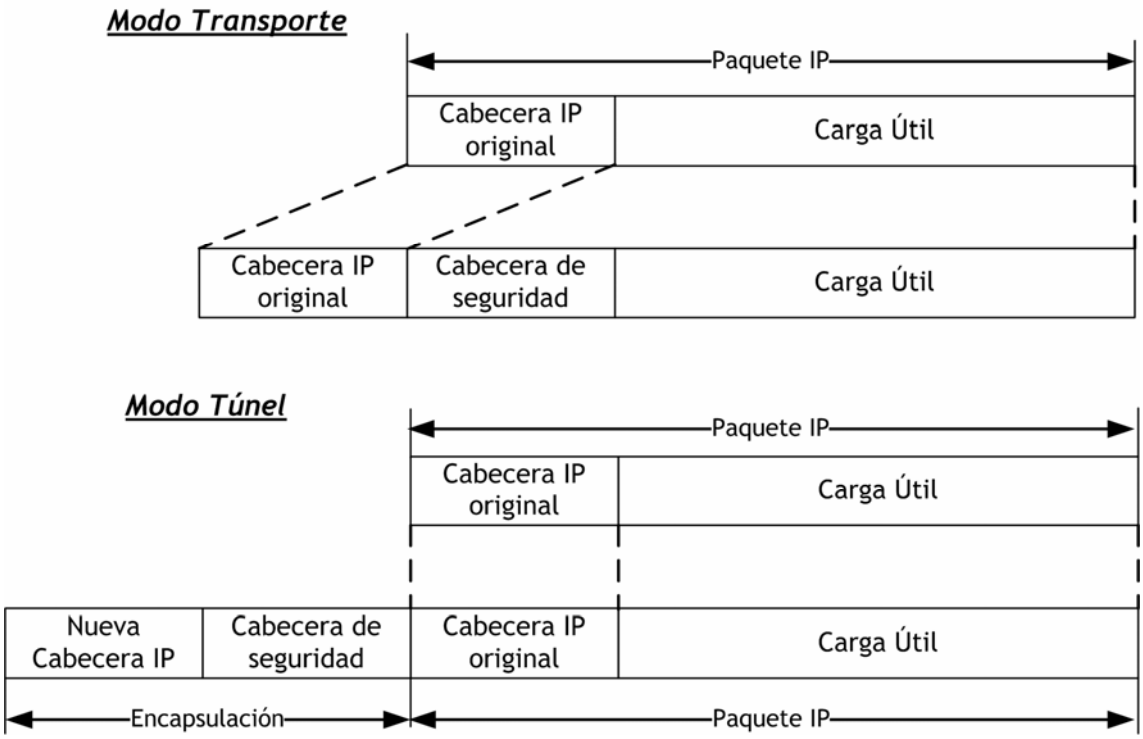

Figura 6.19: Estructura paquete IP en modos transporte y túnel.

Las SAs pueden ser negociadas entre dos entidades IPSec dinámicamente, para lo cual se basan en políticas de seguridad dadas por el administrador del sistema o estáticamente especificadas por el administrador directamente.

Una SA es únicamente identificada por tres parámetros:
- una dirección IP de destino.
- un identificador del protocolo de seguridad.
- un índice del parámetro de seguridad (SPI).

La dirección IP de destino es aquella por la cual se identifica el punto final de la SA, el SPI es un número de 32 bits usualmente escogido por el punto final de destino de la SA y que solo tiene significado local dentro de ese punto destino.

El identificador del protocolo de seguridad es un número con el cual se define cada uno de ellos, 51 para AH y 50 para ESP.

La dirección IP del origen no se usa para definir una SA, una SA se define entre dos host o gateways para datos enviados en una sola dirección, de aquí que, si dos dispositivos necesitan intercambiar información en ambas direcciones usando IPSec, requerirán de dos SAs, una para cada sentido.

En modo de transporte, la cabecera IP original se mantiene intacta y una cabecera de seguridad es colocada entre la cabecera IP misma y su carga

útil. La cabecera IP original es modificada para que el receptor del paquete entienda que antes de la carga útil se encuentra una cabecera de seguridad.

En modo túnel, el paquete IP original se convierte en la carga útil de un paquete IP encapsulado. La cabecera IP nueva le indica al receptor del paquete que una cabecera de seguridad se encuentra a continuación de ella.

Varias SAs pueden ser aplicadas en serie para incrementar los servicios de seguridad del tráfico IP. En estas situaciones una SA es encerrada por otra. El protocolo IPSec define dos formas: transporte adyacente y túneles iterados.

En transporte adyacente, se usan tanto AH como ESP y ellos son aplicados por el mismo host. Es necesario hacer notar que trabajar con adyacencias de transporte AH sobre AH o ESP sobre ESP no trae beneficios adicionales. Lo deseable en este caso es aplicar AH después de ESP.

En túneles iterados, se puede combina cualquier cantidad de túneles con lo cual se logra proveer de capas anidadas de seguridad. Los puntos finales del túnel pueden estar en la misma o en diferentes localizaciones. Por ejemplo, un túnel host-to-host puede ser entunelado por un túnel gateway-to-gateway; y un túnel gateway-to-gateway puede de nuevo ser entunelado por otro túnel gateway-to-gateway.

3) Bases de datos de seguridad

IPSec trabaja con dos bases de datos de seguridad, en una se encuentran las políticas de seguridad y en la otra las asociaciones de seguridad, SPD (Security Policy Database) y SAD (Security Association Database) respectivamente.

El administrador de políticas define un conjunto de servicios de seguridad para ser aplicados al tráfico IP tanto entrante como saliente. Esas políticas son guardadas en las SPDs y son usadas por las SAs cuando éstas se crean. Todas las SAs son registradas en la SAD.

- Bases de datos de asociaciones de seguridad (SAD)

  La base de datos de asociaciones de seguridad almacena todos los parámetros concernientes a las SAs, cada una de ellas tiene una entrada en la SAD donde se especifican todos los parámetros necesarios para que IPSec realice el procesamiento de paquetes IP que son gobernados por esa SA. Entre los parámetros que se encuentran en una SAD se encuentran:

  - El índice de parámetro de seguridad.
  - El protocolo a ser usado por la SA (ESP o AH).
  - El modo en el cual el protocolo es operado (túnel o transporte).
  - Un contador numérico secuencial.

- La dirección IP fuente y destino de la SA.
- El algoritmo deautenticación y la llave de autenticación usadas.
- El algoritmo de cifrado y su llave.
- El tiempo de vida de las llaves de autenticación y de cifrado.
- El tiempo de vida de la SA.

Para el procesamiento de los paquetes IP entrantes, se busca una SA en la SAD tal que concuerde con los siguientes tres valores: la dirección IP destino, el tipo de protocolo IPSec y el SPI.
La dirección IP de destino y el tipo de protocolo IPSec son obtenidos de la cabecera IP y el SPI se obtiene de la cabecera AH o ESP. Si una SA es encontrada para el paquete IP entrante, éste es procesado de acuerdo a los servicios de seguridad especificados. Luego se aplicarán al paquete todas las reglas descritas en la SPD para la SA que lo gobierna.

Para el procesamiento de paquetes IP salientes, primero se aplica el procesamiento relacionado con la SPD. Si se encuentra una política para el paquete de salida que especifique un procesamiento IPSec, la SAD es interrogada para determinar si previamente se ha establecido una asociación de seguridad.
Si aparece, el paquete es procesado de acuerdo a la SA. Si por lo contrario no se encuentra ninguna entrada para este paquete, se negocia una nueva SA que será guardada en la SAD.

- Base de datos de políticas de seguridad (SPD)

Una base de datos de políticas de seguridad es una lista ordenada de políticas de seguridad para aplicar a los paquetes IP.
Dichas políticas son, en general, reglas que especifican como los paquetes IP deben ser procesados.
La SPD es mantenida por el administrador del dispositivo IPSec.

Una entrada SPD tiene dos componentes: un juego de selectores y una acción. Un selector es un parámetro y el valor o rango de valores para éste parámetro. Los parámetros generalmente se encuentran dentro de una de éstas dos categorías:

- Aquellos que se encuentran dentro de un paquete IP, tales como, la dirección IP, número de protocolo y números de puertos de capas superiores.

- Aquellos que se derivan de la credencial de autenticación de una entidad de comunicación, tales como, una dirección de correo o un nombre distinguido DN (Distinguished Names) en certificados digitales.

Diferentes operadores lógicos como AND, OR y NOT pueden ser aplicados a las políticas para combinar más de un selector.

Cuando un paquete IP contiene valores que concuerdan con los especificados por algún selector de una entrada, la acción que se especifica en dicha entrada es aplicada al paquete. Hay tres opciones:

- Aplicar el servicio de seguridad IPSec.

- Descartar el paquete IP.

- Permitir que el paquete IP omita el procesamiento IPSec.

La figura 6.20 muestra una entrada en una base de datos de políticas de seguridad para un paquete entrante y saliente, claramente se notan las partes que componen un selector como lo son los parámetros y su correspondiente valor, junto a ellos se encuentra la acción que IPSec tomaría si los paquetes IP concuerdan con los valores de los selectores.

ENTRANTES

Selectores	**Acción**
Dirección_IP fuente = 10.0.0.92 AND Dirección e-mail fuente = info@canil.uk	IPSec (ESP, 3DES, HMAC-SHA-1)
Nombre_distinguido fuente = Andy McHo	IPSec (ESP, 3DES, HMAC-MD5)
Dirección_IP destino = 192.89.0.169	Omitir

SALIENTES

Selectores	**Acción**
Dirección_IP destino = 10.0.0.92	IPSec (ESP, 3DES, HMAC-SHA-1)
Nombre_distinguido destino = Andy McHo	IPSec (ESP, 3DES, HMAC-MD5)
Dirección_IP fuente= 192.89.0.169	Omitir

Figura 6.20: Ejemplos de políticas de seguridad.

Es posible que un paquete IP concuerde con más de una entrada en la SPD. Por esto, se debe tener en cuenta el orden de las entradas en una SPD, ya que la primera concordancia será la política seleccionada. Además, una política por defecto debe ser

aplicada para el nodo y ésta se aplica cuando el paquete IP no concuerda con ninguna de las entradas de una SPD. Usualmente, esta política por defecto es descartar el paquete IP.

La SPD trata al tráfico saliente y entrante de manera separada, esto es, que se deben aplicar políticas de seguridad distintivas de entrada y de salida por cada interfaz de red. Cuando un paquete IP llega a una interfaz de red, IPSec primero busca en la SAD la apropiada SA, cuando la encuentra, el sistema inicia los procesos SAD y SPD. Después del procesamiento SPD, el sistema reenvía el paquete al siguiente salto o le aplica procedimientos adicionales tales como reglas de firewall.

El procesamiento SPD se realiza primero en paquetes salientes. Si la entrada SPD que concuerda especifica que un procesamiento IPSec es necesario, la SAD es consultada para determinar si una SA ha sido previamente establecida, en caso contrario se negocia una nueva SA para el paquete.

Dado que el procesamiento SPD es realizado tanto para los paquetes IP salientes como entrantes, se convierte en el cuello de botella más representativo en una implementación IPSec.

6.3.3.2.- Authentication Header (AH)

El protocolo de cabecera de autenticación AH es usado para propósitos de autenticación de la carga útil IP a nivel de paquete, esto es, autenticación de la integridad de los datos y de la fuente de los mismos.

Como el término autenticación indica, el protocolo AH se asegura que los datos entregados dentro del paquete IP han llegado a su destino sin ninguna modificación.

AH también provee de un mecanismo de protección opcional frente a duplicación de paquetes IP. Sin embargo, AH no protege la confidencialidad de los datos, es decir, no recurre a ningún tipo de cifrado de los mismos.

El protocolo AH define cómo un paquete IP sin protección es convertido en uno nuevo que contiene información adicional y que brinda autenticación.

El elemento fundamental usado por AH es una cabecera de autenticación como se muestra en la figura 6.21. El nuevo paquete IP es formado insertando la cabecera de autenticación, bien sea, después de la nueva cabecera IP o después de la cabecera IP original modificada según sea el modo en el cual trabaje la SA: transporte o túnel.

Cuando la cabecera de autenticación es insertada, la cabecera IP que la precede deberá indicar que la próxima cabecera que se encuentra es la cabecera de autenticación y no la carga útil del paquete original. La cabecera IP realiza esta acción colocando el campo Protocolo al valor ‘51’ (valor de protocolo para AH).

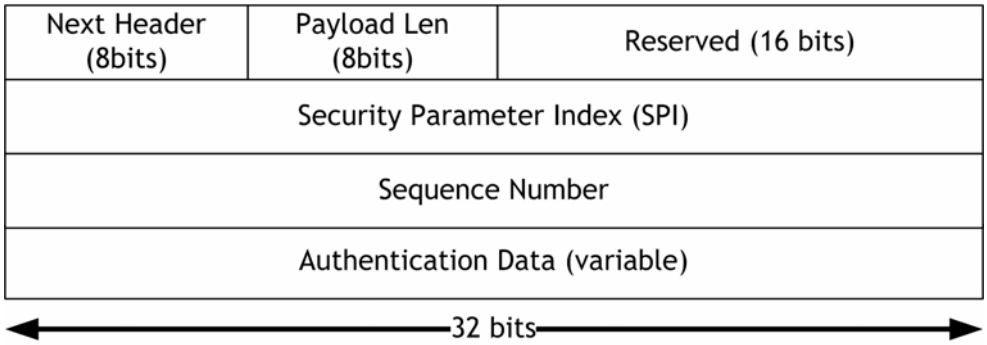

Figura 6.21: Formato de la cabecera de autenticación.

La cabecera de autenticación contiene seis campos:

Next Header: El campo Next Header es un campo de ocho bits que identifica el tipo de protocolo de la carga útil del paquete IP original.

Payload Len: El campo Payload Len es un campo de ocho bits que especifica la longitud de la cabecera de autenticación (no confundir con la cabecera original del paquete IP).

Reserved: El campo Reserved se encuentra reservado para uso futuro, actualmente debe ser puesto a 0.

Security Parameter Index: El campo Security Parameter Index es un número arbitrario de 32 bits. El valor SPI es escogido por el sistema destino cuando la SA es establecida. Para SAs unicast, se utiliza el valor SPI y opcionalmente el tipo de protocolo IPSEC (AH, en este caso), para seleccionar una SA indicada por el receptor. Para SAs multicast, se combina el campo SPI junto la dirección destino y opcionalmente la dirección origen, para seleccionar un SA.

Sequence Number: El campo Sequence Number es un campo de 32 bits que mantiene un control de la secuencia de paquetes IPSec. Comienza en 0 cuando la SA es establecida y se incrementa por cada paquete IP saliente que usa esta SA. Este campo se usa como un mecanismo de protección frente a paquetes duplicados. En la RFC 4302 se explica la posibilidad de utilizar 64 bits en este número de secuencia para comunicaciones de alta velocidad.

Authentication Data: El campo Authentication Data es un campo de longitud variable que contiene el valor de chequeo de integridad ICV (Integrity Check Value) para ese paquete IP. El ICV es calculado con el algoritmo seleccionado por la SA y es usado por el receptor para verificar la integridad del paquete IP entrante. Los algoritmos por defecto requeridos por AH para trabajar son HMAC con MD5 y SHA-1.

Hay que tener en cuenta, que la autenticación no puede ser aplicada sobre la cabecera entera del paquete IP, ya que algunos campos de la cabecera IP original cambian durante el transito por Internet. Esos campos son llamados campos mutables, y son: Type of service (TOS), Fragment offset, Fragmentation flags, Time to live (TTL), Header checksum. Para conocer más detalles sobre estos campos de la cabecera de un paquete IP puede consultarse la RFC 4302.

Para realizar el proceso de autenticación, el emisor calcula el ICV y lo ubica en el campo Authentication Data. El ICV es un valor hash computado sobre todos los campos que la autenticación incluye. La llave secreta es negociada durante el establecimiento de la SA. La autenticación de un paquete recibido es verificada cuando el receptor calcula el valor hash y lo compara con el ICV del paquete entrante. Si el paquete IP no es autenticado exitosamente, es descartado.

6.3.3.2.1.- Modo Transporte.

En modo transporte, la cabecera del paquete IP original es conservada como la cabecera del nuevo paquete IP, y la cabecera de autenticación es insertada entre la cabecera IP y la carga útil original (ver figura 6.22). El único cambio que se realiza en la cabecera IP es el del campo Protocolo que cambia a 51, valor para el protocolo AH. El valor reemplazado en el campo Protocolo pasa a ser el valor del campo Next Header en la cabecera de autenticación. Finalmente el ICV es calculado sobre la totalidad del nuevo paquete IP excluyendo los campos mutables mencionados previamente.

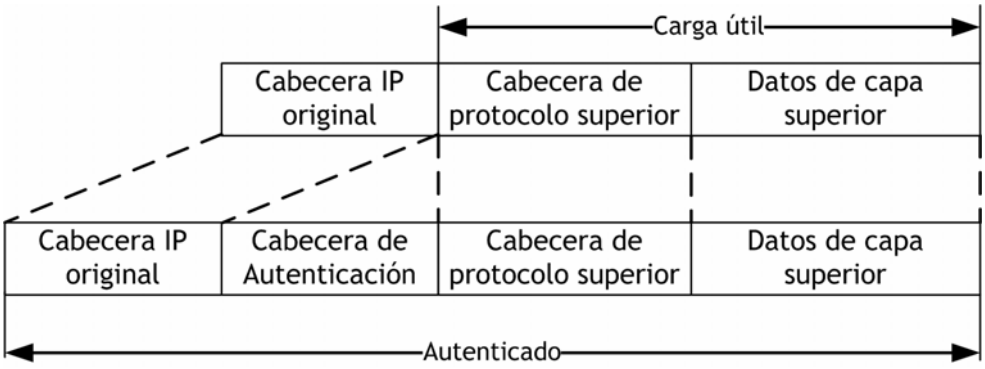

Figura 6.22: Modo transporte AH.

La ventaja del modo transporte es que solo añade unos pocos bytes extra a el paquete IP original. Sin embargo, por conservarse la cabecera IP original como la misma cabecera del nuevo paquete IP, solamente puede ser usado por hosts finales, esta es una limitación grande cuando los dispositivos que están gobernados por esta SA IPSec actúan como pasarelas de otros hosts que se encuentran detrás de ellos.

6.3.3.2.2.- Modo Túnel.

En modo túnel, una nueva cabecera es creada para el nuevo paquete IP y la cabecera de autenticación es insertada entre las cabeceras nueva y original, tal como se muestra en la figura 6.23. El paquete IP original permanece intacto y es encapsulado dentro del nuevo paquete IP. De esta manera, la autenticación se aplica sobre el paquete IP original entero (incluyendo los campos mutables de la cabecera IP original).

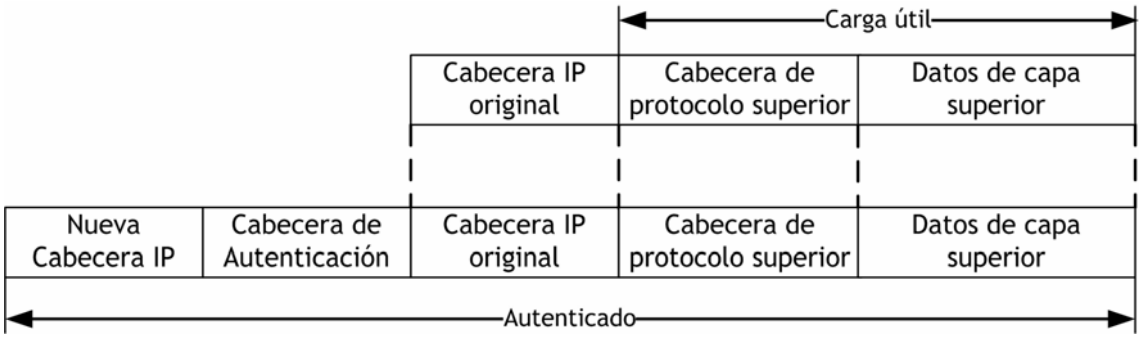

Figura 6.23: Modo túnel AH.

La cabecera IP original permanece completamente inalterada y contiene las direcciones IP tanto de destino como fuente de los dispositivos que emiten y reciben el tráfico IP original. La nueva cabecera IP contiene la dirección IP fuente y de destino de los dispositivos IPSec entre los cuales viaja el nuevo paquete. De esta manera, el modo túnel puede ser usado si los puntos finales de la SA son un host o pasarela de seguridad.

A diferencia del modo transporte, el modo Túnel tiene como desventaja adicionar mas bytes extra por lo cual el throughput efectivo del enlace disminuye al igual que el desempeño de los dispositivos se torna mas lento por el doble procesamiento de cabecera que se necesita.
El valor del campo Protocolo en la nueva cabecera IP es 51 (como en el modo Transporte) y el campo Next Header en la cabecera de autenticación contiene el valor 4, que especifica que la siguiente cabecera es de un paquete de tipo IPv4.

6.3.3.3.- Encapsulating Security Payload (ESP)

El protocolo ESP IPSec provee autenticación, confidencialidad de los datos por medio de cifrado y una protección opcional antirepetición para los paquetes IP. La autenticación y el cifrado son también opcionales, pero al menos una de ellas debe ser empleada; de lo contrario, este protocolo carecería de fundamento.

La confidencialidad es lograda por medio de técnicas de cifrado. Los algoritmos de cifrado empleados a los paquetes IP son definidos por la SA sobre la cual los paquetes son enviados. El algoritmo de cifrado 'Null' en el cual el cifrado no es aplicado, es también un algoritmo válido en este protocolo. En este caso, ESP solamente presta el servicio de autenticación para el tráfico.

Al igual que con AH varios campos adicionales son insertados en el paquete IP para que presten los servicios mencionados anteriormente. Muchos de esos campos tienen el mismo significado que en AH, pero la diferencia es que éstos se encuentran a lo largo del paquete IP, algunos en la cabecera ESP, otros en la cola ESP y otro está en el segmento de autenticación ESP. La figura 6.24 muestra la construcción de un paquete IP después que se ha procesado con el protocolo IPSec ESP, se observan la ubicación de los campos dentro de cada uno de los segmentos del nuevo paquete.

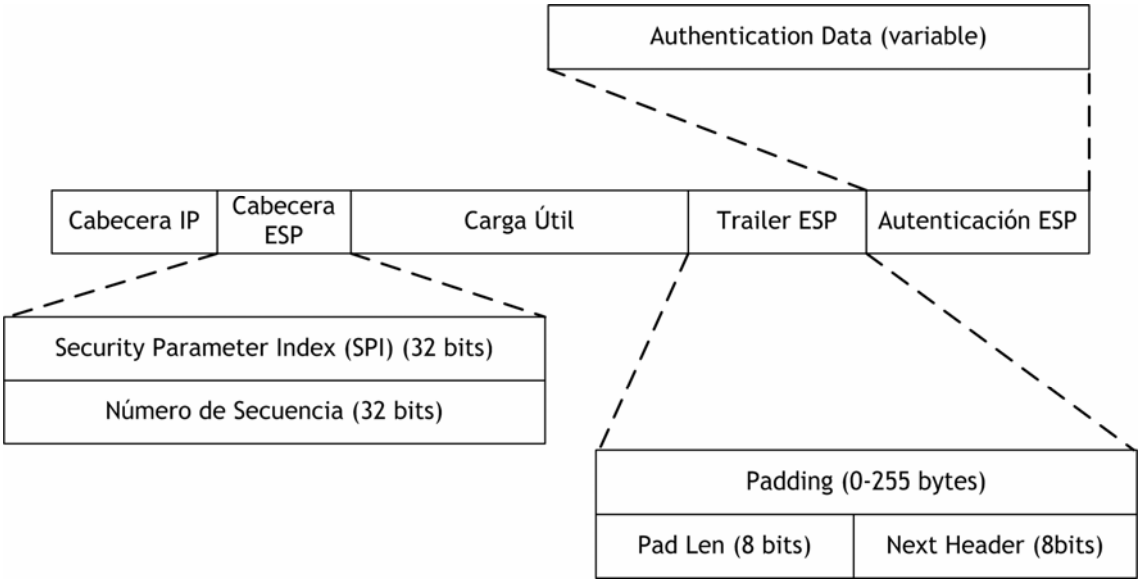

Figura 6.24: Paquete IP procesado con ESP.

La cabecera ESP se encuentra después de la nueva cabecera IP o después de la cabecera IP original modificada, dependiendo del modo que se use. La cola (también llamada trailer) ESP se encuentra al final del paquete IP original y el segmento de autenticación ESP se encuentra después de la cola.

Si la autenticación no es aplicada, el segmento de autenticación ESP no es añadido. Si el cifrado es aplicado, cada una de las partes desde el final de la cabecera ESP hasta el final de el trailer ESP son encriptadas.

Al igual que en el protocolo AH, los campos SPI, Sequence Number, Next Header y Authentication Data, se encuentran definidos a lo largo del nuevo paquete IP. También se encuentran otros dos campos, el campo Padding es usado para rellenar los datos a ser encriptados y completar un límite de 4 bytes, por tanto este campo es de longitud variable. El campo Pad Len especifica la longitud del relleno para poder luego ser eliminado después de que los datos son desencriptados.

Existe un problema cuando la longitud del nuevo paquete IP, debido a la adición de una cabecera ESP y de unos campos de relleno y de autenticación, resulta ser mas grande que el tamaño máximo definido para el paquete (MTU). Cuando esto pasa, los paquetes IP son fragmentados por el dispositivo emisor.

Debido a que el procesamiento ESP debe ser aplicado únicamente a paquetes IP enteros y no fragmentados, si un paquete IP entrante ha llegado fragmentado, la pasarela de seguridad que lo recibe debe reensamblar los fragmentos para formar de nuevo el paquete IP antes de que sean procesados por ESP.

6.3.3.3.1.- Modo Transporte.

En el modo transporte, la cabecera ESP es insertada entre la cabecera IP y la carga útil original, y los segmentos trailer y de autenticación ESP son añadidos si son necesarios.

Si el paquete está siendo sujeto de un segundo proceso de encapsulamiento ESP, la nueva cabecera ESP se añade después de la primera y los segmentos trailer y de autenticación son agregados después de los primeros campos de su mismo ítem. Dado que la cabecera IP original sigue sin alteraciones, el modo de transporte para el protocolo ESP, al igual que en AH, solamente puede ser usado entre hosts.

El modo de transporte es el más usado cuando no es necesario ocultar o autenticar las direcciones IP tanto de la fuente como del destino.

En la figura 6.25 se detalla la construcción del nuevo paquete IP usando ESP en modo transporte, además se muestra la parte del paquete que puede ser encriptada y la parte del paquete que puede ser autenticada.

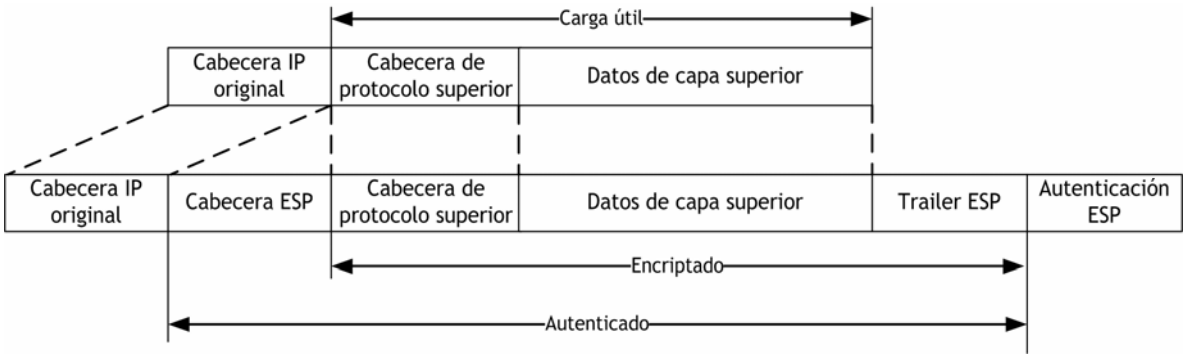

Figura 6.25: Modo transporte ESP.

6.3.3.3.2.- Modo Túnel

En modo túnel, el paquete IP original es encapsulado por completo dentro de un nuevo paquete IP.

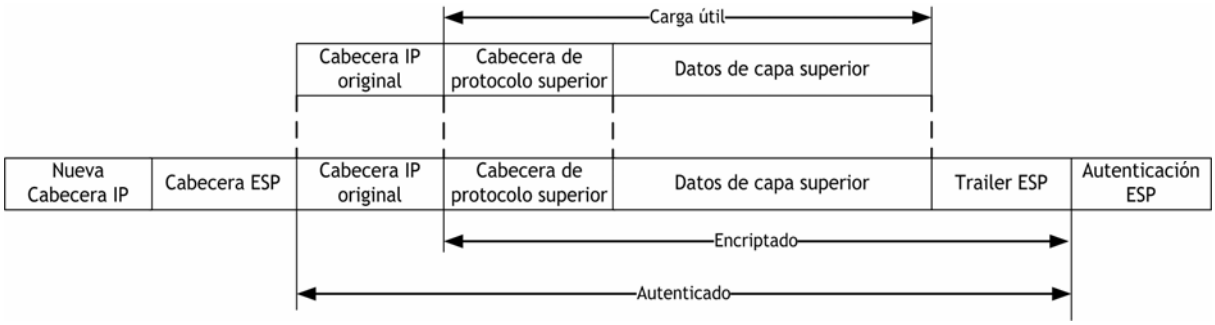

Figura 6.26: Modo transporte ESP.

En la figura 6.26 se muestra como la nueva cabecera IP y la cabecera ESP son puestas al comienzo del paquete IP original, y los segmentos trailer y de autenticación ESP son añadidos al final del mismo.

Si el túnel se encuentra establecido entre hosts, las direcciones IP fuente y de destino, en la nueva cabecera IP pueden ser las mismas que en la cabecera original.

Si el túnel se encuentra establecido entre dos pasarelas o gateways de seguridad, las direcciones en la nueva cabecera IP serán las direcciones de las pasarelas. Ejecutando ESP en modo túnel entre pasarelas de seguridad se puede lograr tanto confidencialidad como autenticación del tráfico en tránsito entre las dos pasarelas.

6.3.3.4.- Internet Key Exchange (IKE)

Los protocolos ESP y AH no explican cómo las asociaciones de seguridad son negociadas, simplemente se refiere a cómo los servicios de seguridad son aplicados a cada paquete IP de acuerdo con lo que le indica la SA.

Las SAs pueden ser configuradas manualmente por el administrador del sistema o pueden ser negociadas dinámicamente por medio de un protocolo de manejo de llaves tal como IKE.

Este último tipo de negociación es muy importante debido a que en una comunicación de datos es imposible saber cuando una nueva SA se tiene que establecer y más cuando los datos a asegurar provienen del exterior del sistema.

La otra razón importante para usar negociación dinámicas de SAs, es que por motivos de seguridad las SAs no pueden tener un tiempo de vida muy largo, dado que se expone a que algún atacante rompa los códigos de seguridad. Para eliminar este riesgo, las SAs se renegocian periódicamente regenerando así todo el material asociado a las llaves mismas.

IKE está basado en el protocolo de manejo de llaves y de asociaciones de seguridad en Internet ISAKMP (Internet Security Association And Key

Management Protocol), que implementa elementos de los métodos de intercambio de llaves Oakley y SKEME (Secure Key Exchange Mechanism).

En este apartado explicaremos IKEv1 recogido en las RFCs 2407, 2408 y 2409, puesto que es el más utilizado actualmente. De todas formas, hay que tener en cuenta que ya existe una nueva versión conocida como IKEv2 y sus especificaciones se recogen en la RFC 4306.

ISAKMP define un conjunto de procedimientos por medio de los cuales se asegura el canal de comunicación entre dos puntos. En otras palabras, es el protocolo encargado de preparar el canal de transporte seguro que luego será usado por las SAs para ser negociadas.
Un mensaje ISAKMP consiste de una cabecera ISAKMP y de uno o más campos de carga útil encadenados dentro de un paquete UDP. Estos paquetes usan el puerto 500. La figura 6.27 muestra el formato de un mensaje ISAKMP compuesto de una cabecera UDP, una cabecera ISAKMP y uno o más campos de carga útil ISAKMP encadenados uno de tras del otro.

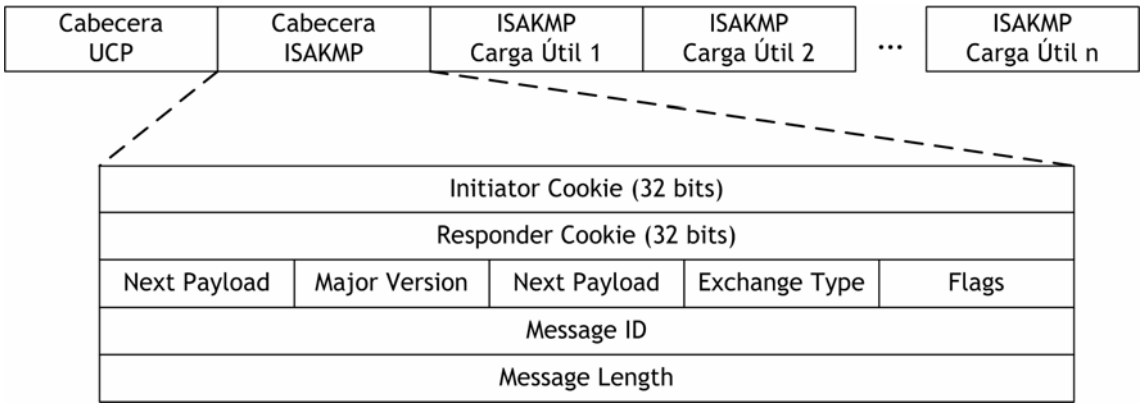

Figura 6.27: Formato de un mensaje ISAKMP.

Dentro de la cabecera ISAKMP se distinguen los siguientes subcampos:

- Initiator Cookie: La cookie de la entidad que comienza el proceso de establecimiento de la SA.

- Responder Cookie: La cookie de la entidad que esta respondiendo a un requerimiento de establecimiento de SA.

- Next Payload: Indica el tipo del primer campo de carga útil en el mensaje. Major Version: Indica el primer dígito de una versión de protocolo ISAKMP. Tiene valor de 1 cuando el protocolo ISAKMP con el cual se trabaja cumple con todas las características descritas en la RFC2408, y valor 0 cuando se trabaja con ISAKMP descrito en RFCs con fechas anteriores.

- Major Version: Indica el segundo dígito de una versión de protocolo ISAKMP. Tiene valor de 0 cuando el protocolo ISAKMP con el cual se trabaja cumple con todas las características descritas en la RFC 2408, y valor 1 cuando se trabaja con ISAKMP descrito en RFCs con fechas anteriores. Por norma, un extremo de la conexión no debería aceptar

paquetes con una Major Version mayor a la que el propio extremo maneja.

- Exchange Type: Indica el tipo de intercambio que esta siendo usando en la negociación del canal seguro, principal, agresivo o rápido. Este campo es importante porque le indica a cada entidad qué mensaje tiene que esperar a continuación.

- Flags: Es un campo de 8 bits pero en la actualidad solo se usan los 3 primeros bits más significativos, el resto son reservados para aplicaciones futuras y deben permanecer siempre a 0.

  - Encryption Flag: Cuando el valor de este bit es 1, todos los campos de carga útil que le siguen al encabezado son encriptados usando el algoritmo de cifrado definido en la ISAMKP SA. Si el valor del bit es 0 la carga útil no viaja encriptada.

  - Commit Flag: Este bit es usado como una señal para sincronizar el intercambio de llaves. Se utiliza para asegurar que los datos a encriptar no sean recibidos antes de completar el establecimiento de la SA. Si el valor del Commit Bit es 1, significa que la entidad que así lo ha configurado, le exige a la otra parte que debe esperar una información de intercambio contenida en el Notify Payload. Aparte de ser usado para asegurar el intercambio de datos encriptados en el momento justo, el Commit Bit se usa para proteger los datos por pérdidas de transmisión debidas a redes no fiables, y así evitar múltiples retransmisiones.

  - Authentication Flag: Este bit se usa para indicar a las partes que a la información útil de los paquetes hay que aplicarle técnicas de chequeo de integridad, pero no de cifrado. Si su valor es de 1 significa que toda la carga útil tiene que ser autenticada.

- Message ID (4 octetos): Es un número único usado para identificar el estado en el que se encuentra el protocolo durante las negociaciones de la fase 2. Es generado aleatoriamente por la parte que inicia la negociación de la fase 2. Sirve para no crear confusiones cuando entre dos entidades se están estableciendo SAs diferentes.

- Message Length (4 octetos): Indica la longitud total del mensaje (cabeceras + cargas útiles) en octetos. El cifrado se puede aplicar sobre el tamaño total del mensaje ISAKMP.

Hay dos fases en la negociación ISAKMP de una asociación de seguridad.

La primera fase es la negociación entre los dos nodos ISAKMP. En esta fase dos nodos se ponen de acuerdo en la forma de proteger las comunicaciones que se establecerán luego entre ellos, se puede decir que en

esta fase se crea una asociación de seguridad ISAKMP. Es muy importante no confundir una ISAKMP SA con las SAs propias de IPSec tratadas anteriormente. Una ISAKMP SA es bidireccional y no trabaja sobre el tráfico IPSec.

En la segunda fase, las asociaciones de seguridad propias de IPSec son negociadas entre los dos nodos ISAKMP. Dado que el canal se ha asegurado en la primera fase, las negociaciones dentro de esta segunda fase se desarrollan de una manera más sencilla. Una misma ISAKMP SA puede ser usada para negociar muchas SAs IPSec reduciendo el número de negociaciones. Lo anterior sucede en aplicaciones IPSec LAN-to-LAN donde una pasarela de seguridad actúa como un nodo ISAKMP en nombre de los hosts que ella protege.

6.3.3.4.1.- Fase 1 IKE

IKE define dos modos de negociación dentro de la fase 1: modo principal y modo agresivo.

El intercambio de mensajes de un modo principal se muestra en la figura 6.28. Se pueden observar tres pasos en este modo.
En el primero, un nodo ISAKMP (el que inicia) propone múltiples SAs al otro nodo (el que responde); este último escoge una de las SAs propuestas y la retorna al emisor.
En el segundo paso, cada nodo envía sus parámetros de intercambio de llaves y un número aleatorio llamado nonce; el uso de los nonces tiene como objetivo proteger a la negociación contra ataques de repetición.
En el tercer paso, toda la información que se intercambia es autenticada usando uno de los siguientes mecanismos de autenticación: secreto compartido, firmas digitales o cifrado de llaves públicas.

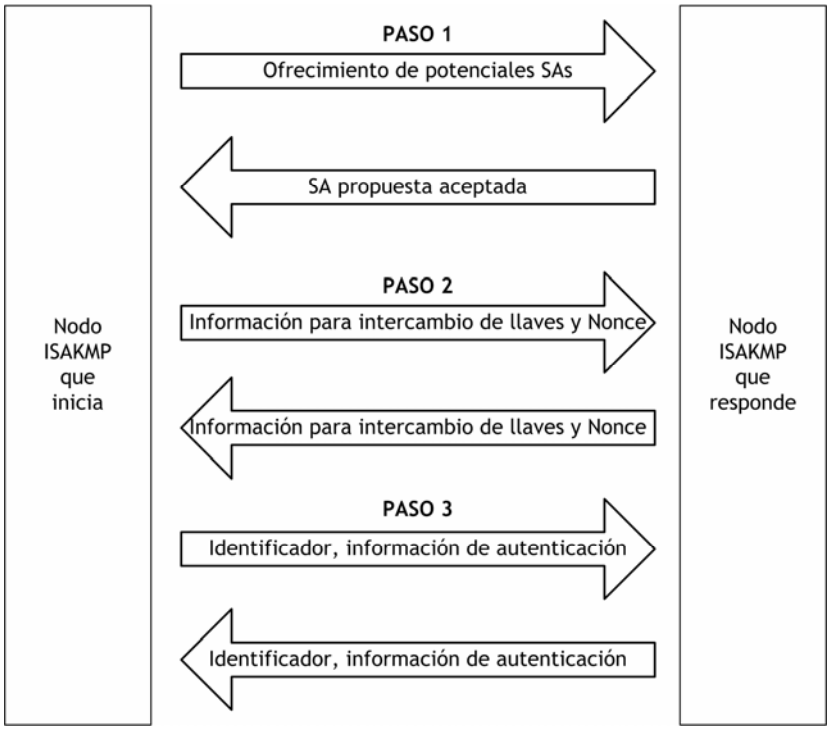

Figura 6.28: Mensajes modo principal, fase 1 IKE.

Cuando se emplea el mecanismo de secreto compartido, los dos nodos usan una llave secreta derivada de un secreto compartido para crear la palabra hash. Esta palabra hash es luego intercambiada entre los dos nodos y sirve como autenticador.

Si se emplea el mecanismo de firmas digitales, la autenticación entre el iniciador y su corresponsal es llevada a cabo usando la firma digital de las entidades de negociación. Los dos nodos intercambian sus identidades, los valores de sus llaves públicas y las SAs propuestas usando mensajes hash firmados digitalmente.

Con el tercer mecanismo, el de cifrado de llaves públicas, los dos nodos intercambian sus IDs y nonces de manera encriptada usando sus llaves públicas.

En el modo agresivo, la SA propuesta, los parámetros de intercambio de llaves, el nonce y la información de su identidad, son intercambiadas todas en un único mensaje, tal como se muestra en la figura 6.29. Adicionalmente, la información de autenticación intercambiada no va encriptada.

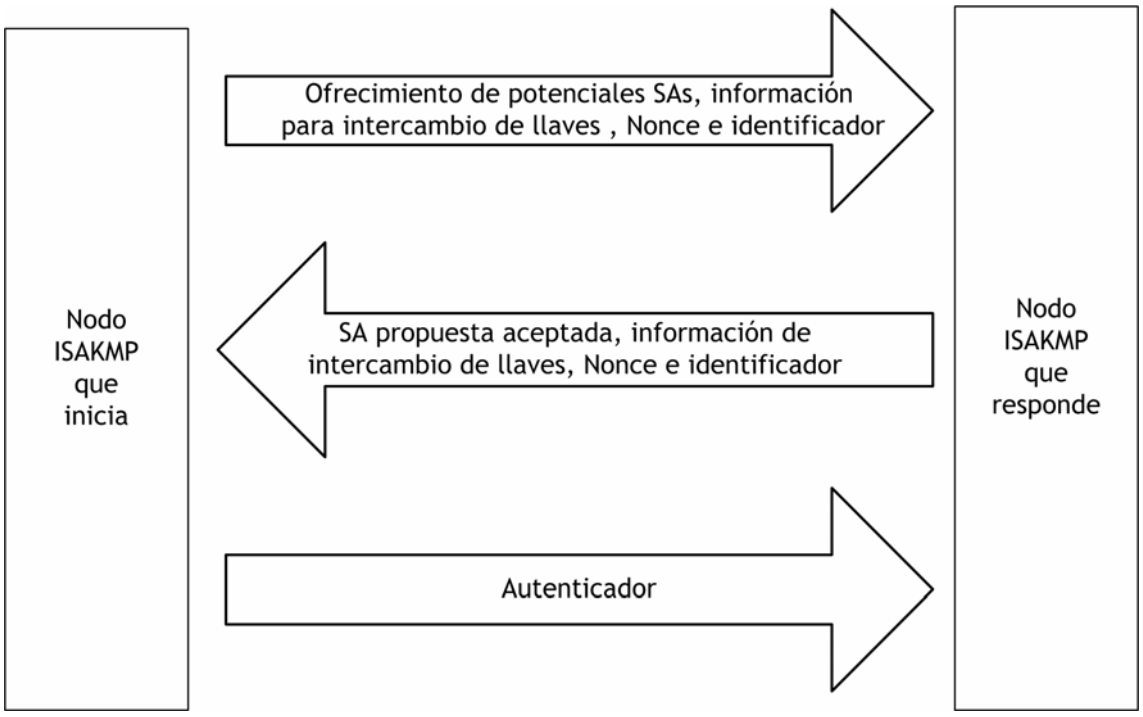

Figura 6.29: Mensajes fase 1 IKE, en modo agresivo.

Una vez se completa la negociación en la fase 1, la ISAKMP SA queda establecida. A partir de este momento todas las negociaciones de las asociaciones de seguridad que se necesiten crear entre los dos nodos viajan en un canal asegurado.

6.3.3.4.2.- Fase 2 IKE.

Durante esta fase, se negocian las asociaciones de seguridad IPSec. Como se dijo anteriormente, la negociación que se realiza en esta fase es más rápida dado que el canal ya se ha asegurado, de aquí que el nombre que toma esta negociación es el de modo rápido.
Los mensajes que se intercambian en modo rápido son mostrados en la figura 6.30.

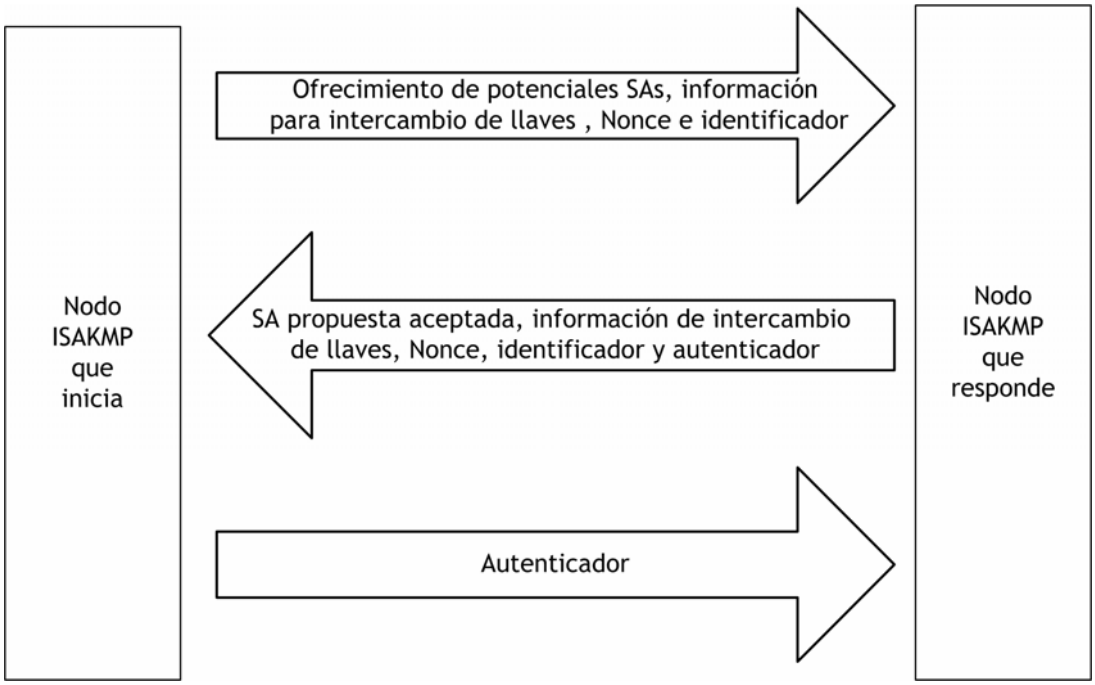

Figura 6.30: Mensajes fase 2 IKE, en modo rápido.

En esta fase las identidades que se pasan de un lado a otro no son las identidades de los nodos IKE sino de los nodos IPSec y más específicamente, de los selectores a ser usados en esta SA y que se encuentra en la base de datos de políticas de seguridad que rige esta comunicación.

Claramente se concluye que para que se lleve a cabo la fase 2 es necesario que haya concluido la fase 1, pero una vez la fase 2 se ha establecido, puede existir independientemente aún si la fase 1 ha desaparecido.

6.3.3.4.3.- Generación de Llaves en IKE.

Las llaves son generadas una vez los parámetros necesarios se encuentran en los nodos ISAKMP.

El algoritmo Diffie-Hellman juega un papel vital en la generación de llaves en IKE. Dicho algoritmo permite que dos partes generen una llave secreta a partir de parámetros públicos, de tal manera que una tercera entidad que tenga la intención de obtener la llave secreta interceptando la comunicación de los dos nodos involucrados sea incapaz de hacerlo.

Sin embargo, el protocolo Diffie-Hellman es vulnerable a ataques en los cuales alguien intercepta los mensajes que se intercambian y suplanta uno de

los nodos. Por lo anterior, en el intercambio IKE, las dos partes involucradas deben ser autenticadas.

La llave secreta Diffie-Hellman generada en la fase 1 es llamada la ISAKMP master key y la llave secreta Diffie-Hellman generada en la fase 2 es llamada la user master key.

Oakley es un protocolo que se usa para determinar llaves y que se basa en el esquema Diffie-Hellman para intercambiar llaves secretas de una manera segura entre dos partes que se han autenticado previamente.

6.3.4.- MPLS (Multi-Protocol Label Switching)

MPLS es una tecnología que modifica el reenvío tradicional de paquetes que analiza la dirección IP de destino contenida en la cabecera de la capa de red de cada paquete y por medio de la cual un paquete viaja desde la fuente hasta su destino final.

6.3.4.1.- Situación anterior al uso de MPLS.

En el análisis tradicional para el reenvío de un paquete IP cada procesamiento es realizado en cada punto de la red. Los protocolos de enrutamiento dinámicos o estáticos construyen una base de datos necesaria, la cual se analiza para tomar una decisión hacia donde va el paquete IP según dirección de destino, dicha tabla se conoce como tabla de enrutamiento.

El reenvío tradicional de paquetes que realiza la capa de red, confía en la información que le proporcionan los protocolos de enrutamiento tales como OSPF (Open Shortest Path First) o BGP (Border Gateway Protocol) o a las rutas estáticas configuradas en cada router, para tomar la decisión de reenvío entre los mismos. Es decir, que la decisión de reenvío está basada única y exclusivamente en la dirección IP de destino. Todos los paquetes para el mismo destino siguen el mismo camino a través de la red si no existen otros caminos de igual costo. Si un router tiene dos caminos de igual costo hacia un mismo destino, los paquetes podrían tomar uno solo o ambos, teniendo como consecuencia una degradación en la velocidad debido al proceso de balanceo de cargas.

Los routers son dispositivos que trabajan a nivel de la capa de red, ellos se encargan de recolectar y distribuir la información de enrutamiento y de la conmutación a nivel 3 basada en el contenido de la cabecera de la capa de red de cada paquete.

Los routers se pueden conectar directamente por medio de enlaces punto-a-punto o redes de área local. También pueden ser conectados a través de switches LAN o WAN. Esos conmutadores de capa 2 no tienen la capacidad de mantener la información de enrutamiento de capa 3 o de seleccionar el camino que debería de tomar un paquete partiendo del análisis de su dirección de destino capa 3. Es decir, los switches de capa 2 no se pueden involucrar en el proceso de reenvío de paquetes a nivel de capa 3.
En el caso de una red WAN el diseñador de la red tiene entonces que establecer trayectos a nivel 2 manualmente a través de toda la red WAN. Por

esos trayectos es por donde los conmutadores que están conectados físicamente a la capa 2, reenvían sus paquetes a nivel de la capa 3.

El establecimiento de un trayecto en una red WAN de capa 2 se realiza por medio de un enlace punto-a-punto, que en la mayoría de redes WAN es llamado un circuito virtual y que se establece únicamente por medio de una configuración manual. Cualquier dispositivo de enrutamiento que se encuentre conectado en los límites de una red de capa 2 y que quiera reenviar sus paquetes a nivel de capa 3 a otro dispositivo de enrutamiento, necesita establecer una conexión directa a través de la red.

Los problemas de escalabilidad que se pueden encontrar en redes de este tipo son:

- Cada vez que un nuevo router es conectado a la red WAN, un circuito virtual debe ser establecido entre este router y cada uno de los demás, si se busca un enrutamiento óptimo.

- En la mayoría de protocolos de enrutamiento, cada router conectado a la red WAN a nivel de capa 2, necesita un circuito virtual dedicado a cada uno de los otros routers. Con esto se logra la redundancia. Como resultado, se obtienen enrutadores con múltiples vecinos y a su vez, cantidades de tráfico de enrutamiento circulando entre ellos.

- Otro problema frecuente es la dificultad que se tiene para hacer el aprovisionamiento de ancho de banda o de circuitos virtuales entre los routers de una red capa 3, ya que es difícil predecir la cantidad exacta de tráfico entre dos routers. Esto conlleva a que algunos proveedores de servicio no opten por ofrecer un servicio de calidad garantizada dado por su red.

Los anteriores problemas, entre otros, han hecho que algunos proveedores de servicios de enlaces capa 2 quieran implementar tecnologías IP usando la infraestructura WAN que ya tienen. También, algunos proveedores de Internet se muestran interesados sobre alguna tecnología que les permita garantizar una calidad en el servicio (QoS) como lo hacen los conmutadores ATM.
Además el rápido crecimiento del ancho de banda ha acelerado la aparición de interfaces ópticas en los enrutadores y que poco a poco puedan emplear tecnologías de alta velocidad como ATM.

En el reenvío de paquetes IP convencional, cualquier cambio en la información que controla el reenvío de paquetes es comunicado a todos los dispositivos que controlan el dominio de enrutamiento. Este cambio, siempre lleva consigo un periodo de convergencia mientras que la información es actualizada en toda la red.

De lo anterior es claramente deseable, un mecanismo que pudiera cambiar el trayecto por el cual se reenvía un paquete sin afectar los demás dispositivos que conforman la red. Para implementar este mecanismo, los dispositivos de enrutamiento no deberían depender de la información que se contiene en la cabecera IP, para lo cual se necesitaría adjuntar una etiqueta

adicional al paquete reenviado que indique el comportamiento que tome el mismo a lo largo de la red. Si las decisiones de reenvío se basan entonces en etiquetas adjuntadas a los paquetes IP originales, cualquier cambio en el proceso de decisión puede ser llevado a cabo únicamente adjuntado nuevas etiquetas y así no modificarían ninguno de los otros dispositivos de enrutamiento que conforman la red.

En una red que trabaja con el mecanismo de reenvío convencional de paquetes, todos los dispositivos de enrutamiento, conocen la información de enrutamiento para alcanzar determinado destino. Esto es necesario, dado que cada paquete es enrutado basado en la dirección destino que esta contenida en su cabecera de capa de red.

Este método tiene implicación de escalabilidad en términos de propagación de rutas, de memoria y CPU utilizadas en los enrutadores del backbone. Un mecanismo que permita a los dispositivos de enrutamiento conmutar los paquetes a través de la red, desde un router destino hasta un router final, sin analizar la dirección destino sería un objetivo a perseguir.

6.3.4.2.- Descripción de MPLS.

MPLS o Conmutación de Etiquetas Multiprotocolo (Multi-Protocol Label Switching) es una tecnología relativamente nueva que se desarrolló para solucionar la mayoría de los problemas que existen en la técnica actual de reenvío de paquetes. El IETF cuenta con un grupo de trabajo MPLS. El objetivo primario de MPLS, es estandarizar una tecnología base que integre el intercambio de etiquetas durante el reenvío con el sistema de enrutamiento actual de redes. Se espera que esta nueva tecnología mejore la relación precio/desempeño del enrutamiento que se realiza en la capa de red, que mejore la escalabilidad de la misma capa, y que provea una gran flexibilidad en la entrega de (nuevos) servicios de enrutamiento.

La arquitectura MPLS describe cómo se realiza la conmutación de etiquetas, la cual combina los beneficios del reenvío de paquetes a nivel de capa 2 con los beneficios del enrutamiento del nivel 3. De forma similar a cómo se hace en las redes de capa 2, MPLS asigna etiquetas a los paquetes para que sean transportados a través de redes basadas en paquetes o en celdas. Este mecanismo de reenvío a través de dichas redes es conocido como intercambio de etiquetas (label swapping), lo cual permite que con una etiqueta pequeña y de longitud fija que se añade al paquete original se pueda enrutar dicho paquete a lo largo de un camino determinado que se crea con la información que cada conmutador tiene de la red y la que existe en cada etiqueta. Esta es la forma como se puede crear una VPN usando MPLS.

En el reenvío de paquetes usando MPLS se puede apreciar una diferencia drástica con el reenvío original de paquetes donde cada paquete es analizado en cada uno de los saltos de la red, se comprueba la cabecera capa 3, y en base a eso se toma una decisión conforme a la tabla de enrutamiento de cada dispositivo de nivel 3.

La arquitectura MPLS se divide en dos componentes:

- El componente de reenvío, también llamado data plane.

- El componente de control, también llamado control plane.

El componente de reenvío, como su nombre lo indica, se encarga de reenviar los paquetes basado en las etiquetas que cada uno de ellos transporta, para esto usa una base de datos de reenvío de etiquetas que es mantenida por un switch de etiquetas (label switch). Haciendo la analogía con el esquema tradicional de reenvío de paquetes, esta base de datos es la tabla de enrutamiento.

El componente de control es el responsable de crear y mantener toda la información de reenvío de etiquetas (también llamadas vínculos) entre un grupo de switches de etiquetas interconectados. De nuevo, haciendo la analogía con el esquema tradicional de enrutamiento, el componente de control es el protocolo de enrutamiento.

La figura 6.31 muestra en un esquema la arquitectura de un nodo MPLS realizando el enrutamiento de un paquete IP. Se detalla la relación entre cada uno de los bloques dentro del mismo nodo y también con nodos adyacentes.

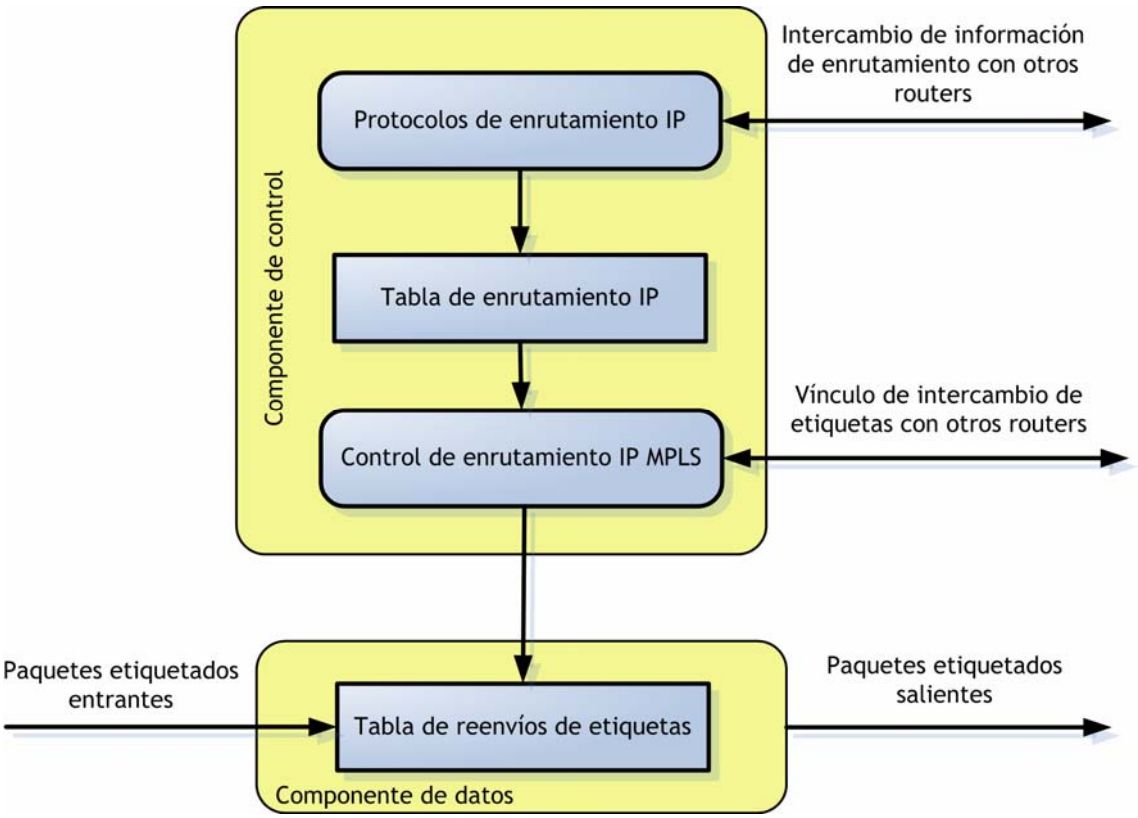

Figura 6.31: Arquitectura de un nodo MPLS.

Como se observa, cada nodo MPLS también es router IP en el componente de control, ya que ejecuta uno o varios protocolos de enrutamiento (o depende de rutas estáticas) para intercambiar información de enrutamiento con otros nodos MPLS en la red.

Tal como en los routers tradicionales, los protocolos de enrutamiento IP son los encargados de mantener la tabla de enrutamiento, en la cual se basan los dispositivos de nivel 3 para tomar la decisión de reenvío del paquete.

En un nodo MPLS, la tabla de enrutamiento es usada para determinar el intercambio de vínculos de etiquetas, dicho intercambio es realizado por el Protocolo de Distribución de Etiquetas o LDP (Label Distribution Protocol).

El componente de control usa las etiquetas intercambiadas con los nodos MPLS adyacentes para construir la Tabla de Reenvío de Etiquetas o LFT (Label Forwarding Table), la cual usa el componente de datos para reenviar los paquetes etiquetados a través de la red MPLS.

6.3.4.3.- Componentes de una red MPLS.

Se conoce por Enrutadores de Conmutación de Etiquetas o LSR (Label Switch Router) a cualquier dispositivo que esté involucrado en el proceso de distribución de etiquetas y que pueda reenviar paquetes. La función básica del proceso de distribución de etiquetas es poder permitirle a cada LSR que distribuya sus vínculos de etiquetas a otros LSRs dentro de la red MPLS.

Existen varios tipos de LSRs que se diferencian por las funciones que cada uno de ellos desempeña, entre ellos están el Edge-LSR, ATM-LSR y ATM Edge-LSR. La diferencia es puramente a nivel de arquitectura, es decir el mismo dispositivo puede ser usado como cualquiera de los otros.

El Edge-LSR es un router que realiza la imposición o extracción de las etiquetas en los límites de la red MPLS. La labor de imposición consiste en añadir al paquete original una etiqueta o un conjunto de etiquetas en el punto de ingreso a la red (en el sentido fuente-destino). La función de extracción es lo contrario, y consiste en quitar la última etiqueta del paquete antes de ser reenviada al siguiente host externo a la red MPLS.

Cualquier LSR que esté contiguo a un nodo no MPLS es considerado un Edge-LSR. Sin embargo, si ese LSR tiene alguna interfaz conectada a un ATM-LSR, entonces toma el nombre de ATM Edge-LSR.

Los Edge-LSR usan la tabla de reenvío IP tradicional para etiquetar paquetes IP o para quitar las etiquetas de los mismos antes de ser enviados a un nodo no MPLS.

Un ATM-LSR es un conmutador ATM que puede actuar como un LSR, es decir, es un dispositivo que realiza enrutamiento IP y asignación de etiquetas en el componente de control, y reenvío de paquetes de datos usando los mecanismos de conmutación de paquetes propios de ATM, para esto usa su matriz de conmutación ATM como su LFT.

6.3.4.4.- Mecanismo de imposición de etiquetas MPLS.

La imposición de etiquetas en MPLS es la acción de añadir una etiqueta a un paquete cuando éste entra a un dominio MPLS.

Esta función se realiza siempre en los límites de la red MPLS y es ejecutada por un Edge-LSR.

En el reenvío tradicional de paquetes IP, cada salto en la red realiza una consulta en la tabla de reenvío IP, y con base en la dirección destino que se encuentra en la cabecera de red, selecciona el siguiente salto y reenvía el paquete hacia éste. Esta iteración se repite en cada salto de la red hasta que el paquete llega a su destino final.

Escoger el siguiente salto para el paquete IP es la combinación de dos funciones. La primera función clasifica todos los paquetes que llegan en determinado momento al router en varios grupos de prefijos IP destino; es decir, agrupa todos los paquetes que pertenecen a una misma subred y que por lo tanto tienen que ser reenviados al mismo destino. La segunda función asocia a cada grupo de paquetes creado en el primer paso a una dirección IP que es su siguiente salto.

Dentro de la arquitectura MPLS, el resultado de la primera función, es decir, los grupos de paquetes con el mismo destino, es llamado un FEC (Forwarding Equivalence Classes). Cada paquete dentro un FEC es reenviado de la misma manera, por lo tanto atraviesan la red usando el mismo camino.

A diferencia del reenvío tradicional de paquetes, el proceso de asignar a un paquete un FEC es realizado sólo una vez y no por cada salto, con lo cual se reduce el procesamiento de cada router dentro de la red. El FEC al cual el paquete es asignado, es codificado como un identificador de tamaño fijo llamado etiqueta.

Cuando el paquete etiquetado llega al siguiente salto dentro del dominio MPLS, el LSR que lo recibe, analiza su etiqueta y lo reenvía al siguiente salto dependiendo de la información que aparece en LFT.

6.3.4.5.- Reenvío de paquetes MPLS.

Los paquetes MPLS entran a la red a través de un LRS de entrada y salen de ella a través de un LSR de salida. El camino que toma un paquete de un lado a otro se denomina LSP (Label Switched Path). Este camino es construido a partir de la información que se toma de una FEC.

Un LSP trabaja en un esquema orientado a conexión, es decir, que el camino tiene que ser formado antes de que cualquier flujo de tráfico empiece a circular por éste.

Cuando un paquete atraviesa la red MPLS, cada LSR cambia la etiqueta entrante por una nueva etiqueta saliente, al igual que el mecanismo usado por ATM, donde los VPI/VCI son cambiados por un par diferente cuando salen del conmutador ATM. Este proceso continúa hasta que el último LSR ha sido alcanzado.

Cada LSR mantiene dos tablas que soportan toda la información relevante al componente de reenvío MPLS. La primera, conocida como LIB (Label Information Base), donde se guardan todas las etiquetas asignadas por este LSR y las correspondencias de esas etiquetas a otras recibidas desde algún LSR vecino. Las correspondencias de estas etiquetas, son distribuidas por medio de protocolos para este uso específico.

La segunda tabla conocida como LFIB (Label Forwarding Information Base) y en la cual son mantenidos únicamente las etiquetas que están siendo actualmente usadas por el componente de reenvío. Las LFIB son el equivalente MPLS de una matriz de conmutación en un conmutador ATM.