Capítulo 5.
Aplicaciones.

Una vez que se ha descrito el funcionamiento y características de la interfaz A-bis, se muestran algunos ejemplos donde se ha aplicado esta como una alternativa para la optimación del ancho de banda.

Aprovechando algunos hechos se pueden mencionar, por ejemplo, el utilizar la infraestructura de TX existente para los diferentes servicios de 2G y 3G. Así. Al optimar la infraestructura actual se tiene mayor capacidad; utilizar el tráfico de GSM (A-bis) como opción para optimar tráfico de 2G; UMTS utiliza actualmente una base ATM para la mayoría de las interfaces; haciendo un manejo estadístico del tráfico de usuario (Iub) se puede usar como candidato para la sobre suscripción, en consecuencia utilizar menores recursos de TX en algunos puntos.

Una de las marcas que proporciona el equipo necesario para la realización de este proceso es la marca TELLABS con su serie 8600. (En el Anexo 2 se pueden ver algunos equipos y sus características)

Algunas ventajas que se obtienen al utilizar este equipo son las siguientes:

- La agregación elimina la necesidad de actualizaciones y/o crecimientos masivos de la red SDH.
- MPLS permite transportar con calidad de servicio sobre enlaces SDH existentes. (evita el reemplazo de equipos SDH existentes).
- Prepara la red para el crecimiento de datos con una tecnología diseñada para datos.

- Permite la agregación y transporte de tráficos TDM, ATM e IP en el mismo equipo.
- Optima el transporte de datos con un factor mínimo de 4:1 con multiplexaje estadístico.

5.1 Introducción a la teoría de MPLS/IP.

MPLS son las siglas de Multiprotocol Label Switching – Multiprotoco de Intercambio de Etiquetas. Es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

MPLS funciona anexando un encabezado a cada paquete. Dicho encabezado contiene una o más “etiquetas”, y al conjunto de etiquetas se le llama pila o “stack”. Cada etiqueta consiste de cuatro campos:

- Valor de la etiqueta de 20 bits.
- Prioridad de Calidad de Servicio (QoS) de 3 bits. También llamados bits experimentales.
- Bandera de “fondo” de la pila de 1 bit.
- Tiempo de Vida (TTL) de 8 bits.

5.1.1 Descripción general.

Como cada paquete de una conexión de protocolo de capa de red se desplaza de un router a otro, cada router toma una decisión independiente en el

reenvío de paquetes. Es decir, cada router de forma independiente elige al próximo salto para el paquete, basado en su análisis de la cabecera del paquete y los resultados de ejecutar el algoritmo de enrutamiento.

Las cabeceras de los paquetes contienen mucho más información de la necesaria, solo para elegir el siguiente salto. Por lo tanto, elegir el siguiente salto puede considerarse como la relación de dos funciones. En la primera, está la función de fragmentos de todo el conjunto de paquetes posible que queda dentro del conjunto de "Clases de Equivalencia de Reenvío (Forwarding Equivalence Classes - FECs)". En la segunda están los mapas de cada FEC a un próximo salto. En la medida en que la decisión de reenvío es concertada, los diferentes paquetes, los cuales consiguen mapearse en el mismo FEC, son indistinguibles. Todos los paquetes que pertenecen a una FEC particular y que viajan de un nodo en particular seguirán el mismo camino (o, si ciertos tipos de enrutamiento multi-ruta están en uso, todos ellos seguirán un conjunto de rutas relacionadas con el FEC).

En el reenvío IP convencional, en un router dado, generalmente se considera que dos paquetes están en la misma FEC si existiera una dirección de prefijo X en las tablas de enrutamiento del router de manera que X es "el juego más largo" para la dirección de destino de cada paquete. A medida que el paquete atraviesa la red, cada salto, a su vez reexamina el paquete y lo asigna a una FEC.

En MPLS, la asignación de un paquete particular a una FEC particular se hace una sola vez, cuando el paquete entra en la red. La FEC a la que el paquete se le asigna se codifica como un valor fijo de corta longitud conocido como una "etiqueta". Cuando un paquete es enviado a su próximo salto, la etiqueta es enviada junto con él; es decir, los paquetes se "etiquetan" antes de que se les reenvíe.

En posteriores saltos, no hay análisis de cabecera de la capa del paquete de la red. Más bien, la etiqueta se utiliza como un índice en una tabla que especifica el

siguiente salto, y una nueva etiqueta. La etiqueta vieja se sustituye con la etiqueta nueva, y el paquete es enviado a su próximo salto.

En el paradigma de reenvío MPLS, una vez que un paquete es asignado a una FEC, no se hace análisis de las cabeceras por los “routers” posterior, todo envío es impulsado por las etiquetas. Esto tiene una serie de ventajas sobre las convencionales en la capa de transmisión de red.

Algunos “routers” analizan la cabecera de un paquete de la capa red no sólo para elegir el siguiente salto del paquete, sino también para determinar "la prioridad del paquete" o "clase de servicio". A continuación, se pueden aplicar diferentes umbrales para descartar o acreditar a los diferentes paquetes. MPLS permite (pero no exige) la prioridad o clase de servicio, total o parcialmente se deduce de la etiqueta. En este caso, se puede decir que la etiqueta representa la combinación de la FEC y la prioridad o clase de servicio.

Un “router” que soporta MPLS es conocido como un "Label Switching Router" o un “Router Intercambiador de Etiquetas” o LSR.

Arquitectura MPLS

Siglas más usadas:

- LER (Label Edge Router): elemento que inicia o termina el túnel (pone y quita cabeceras). Es decir, el elemento de entrada/salida a la red MPLS. Un router de entrada se conoce como Ingress Router y uno de salida como Egress Router. Ambos se suelen denominar Edge Label Switch Router ya que se encuentran en los extremos de la red MPLS.
- LSR (Label Switching Router): elemento que conmuta etiquetas.

- LSP (Label Switched Path): nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del túnel
- MPLS establecido entre los extremos. A tener en cuenta que un LSP es unidireccional.
- LDP (Label Distribution Protocol): un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.
- FEC (Forwarding Equivalence Class): nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

5.1.2 Conceptos básicos.

Etiquetas

Una etiqueta tiene una pequeña longitud fija, es importante a nivel local como identificador, se utiliza para identificar a una FEC. La etiqueta que se coloca a un paquete en particular representa el reenvío de la clase equivalencia la que se le asigna al paquete.

Por lo general, un paquete es asignado a una FEC basándose (total o parcialmente) en su dirección de destino en la capa de red. Sin embargo, la etiqueta no es una codificación de dicha dirección.

Cuando hablamos acerca de paquetes que “están siendo enviados” de un LSR a otro no significa necesariamente que el paquete se ha originado en ese punto ni que ha de terminar en el otro. Esto quiere decir que los paquetes pueden ir de un punto a otro en su camino a un FEC de destino final, incluso que viene desde otro FEC de origen más anteriormente, o sea que van de paso.

El etiquetado de paquetes.

La "etiqueta del paquete" es un paquete en el que una etiqueta se ha codificado. En algunos casos, la etiqueta se encuentra en una cabecera de encapsulación que existe específicamente para este propósito. En otros casos, la etiqueta puede residir en un enlace de datos existentes o encabezado de la capa de red, siempre que hay un campo que está disponible para ese fin. La técnica de codificación particular a ser usada debe ser acordada por ambas entidades, tanto el que codifica la etiqueta como la entidad que decodifica la etiqueta.

Sello de asignación y distribución

En la arquitectura MPLS, la decisión de enlazar a una etiqueta L en especial a una FEC F en particular, se hace por la LSR de carga de bajada con respecto a ese enlace. El LSR de carga de bajada luego informa a la LSR de carga de subida del enlace. Así, las etiquetas son "asignadas para la bajada", y los enlaces de la etiqueta son distribuidos en la dirección "de bajada a subida".

Si un LSR ha sido diseñado de modo que sólo puede buscar etiquetas que caen en un rango numérico determinado, entonces sólo necesita asegurarse de que las etiquetas de enlace se encuentran en ese rango.

Atributos de un enlace de etiquetas

Un particular enlace con la etiqueta L hacia el FEC F, distribuido desde un LSR a otro, pueden tener asociados "atributos". Si el LSR es de subida, e incluso distribuye la etiqueta de enlace a una FEC F, bajo ciertas condiciones, puede ser obligado a distribuir también el atributo correspondiente que recibió del LSR de bajada.

Protocolos de distribución de etiquetas

Un protocolo de distribución de etiquetas es un conjunto de procedimientos por los que un LSR informa a otro de los enlaces etiqueta/FEC ha sido hecho. Dos LSRs que utilizan un protocolo de distribución de etiquetas para etiquetar el enlace de intercambio de información etiqueta/FEC se les conoce como "compañeros de distribución de etiquetas" con respecto al enlace de información en materia de intercambio. Si dos LSRs son pares de distribución de etiquetas, vamos a hablar de la existencia de una "etiqueta de adyacencia de distribución" entre ellos. Dos LSRs pueden ser compañeros de distribución de etiquetas con respecto a algún conjunto de enlaces, pero no con respecto a algún otro conjunto de enlaces.

El protocolo de distribución de etiquetas también abarca las negociaciones en la que dos pares de distribución de etiquetas deben comprometerse con el fin de aprender unas de otras las capacidades MPLS.

Cargas de subida no solicitadas vs. Cargas de bajada en demanda.

La arquitectura MPLS permite a un LSR a solicitar explícitamente, de su próximo salto para un FEC particular, una etiqueta obligatoria para tal FEC. Esto se conoce como distribución de la etiqueta de "cargas de bajada en demanda".

La arquitectura MPLS permite a un LSR distribuir enlaces a LSRs que no han solicitado expresamente nada de ellos. Esto se conoce como distribución de la etiqueta "carga de subida no solicitada".

La pila de etiquetas

Hasta ahora, pareciera como si un paquete etiquetado lleva sólo una sola etiqueta. Pero, es útil tener un modelo más general en el que un paquete etiquetado

lleva un número de etiquetas, organizadas para que la última en entrar, sea la primera en salir de la pila. Nos referimos a esto como la etiqueta de apilamiento.

En MPLS un paquete etiquetado es completamente independiente del nivel de su jerarquía. El tratamiento se basa siempre en la etiqueta superior, sin tener en cuenta la posibilidad de que un cierto número de etiquetas puedan haber estado "por encima" anteriormente, o que un cierto número de etiquetas pueden ser inferiores en la actualidad.

Un paquete sin etiqueta puede considerarse como un paquete cuya etiqueta de apilamiento está vacía (es decir, en cuya etiqueta de apilamiento tiene una profundidad de 0). Si la etiqueta de un paquete de apilamiento es de m de profundidad, nos referimos a la etiqueta en la parte inferior de la pila como etiqueta nivel 1, a la etiqueta encima de ella (si existe) como etiqueta nivel 2 y a la etiqueta en la parte superior de la pila como la etiqueta nivel m.

Selección de ruta

La selección de rutas se refiere al método utilizado para la selección de los LSP para un FEC particular. La arquitectura propuesta para el protocolo MPLS soporta dos opciones para la selección de ruta: enrutamiento salto a salto y enrutamiento explícito.

El enrutamiento salto a salto permite a cada nodo a elegir independientemente el siguiente salto para cada FEC. Este es el modo habitual hoy en día en las redes IP. Un "enrutador LSP salto a salto" es una LSP cuya ruta se selecciona usando el enrutamiento salto a salto.

En un LSP enrutado de manera explícita, cada LSR no elige independientemente el siguiente salto; más bien, un LSR único, generalmente el LSP de ingreso o el LSP

de egreso, especifica varias (o todas) de los LSRs en el LSP. Si un LSR solo especifica el LSP entero, el LSP es "estrictamente" explícitamente enrutado. Si un LSR solo especifica solo algunos de los LSP, el LSP está "vagamente" explícitamente enrutado.

Etiqueta de distribución en el Protocolo de transporte

Un protocolo de distribución de etiquetas se usa entre los nodos de una red MPLS para establecer y mantener las etiquetas de enlaces. Con el fin de que MPLS funcione correctamente, la información de las etiquetas de distribución deben transmitirse de forma fiable, y los mensajes de protocolo de las etiquetas de distribución, relativos a una FEC en particular, deben ser transmitidas en secuencia. El control de flujo es también deseable, como es la capacidad de llevar múltiples etiquetas de mensajes en un solo paquete o datagrama.

5.1.3 Introducción al Protocolo de Internet, versión 6 (IPv6)

El IP versión 6 (IPv6) es la nueva versión del Protocolo Internet, diseñado como el sucesor para el IP versión 4 (IPv4). Los cambios del IPv4 al IPv6 recaen principalmente en las siguientes categorías:

- Capacidades de Direccionamiento Extendido. El IPv6 incrementa el tamaño de dirección IP de 32 bits a128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionables, y una autoconfiguración más simple de direcciones. La escalabilidad del enrutamiento multienvío se mejora agregando un campo "ámbito" a las direcciones multienvío. Y se define un nuevo tipo de dirección llamada "dirección envío a uno de", usado para enviar un paquete a cualquiera de un grupo de nodos.

- Simplificación del Formato de Cabecera. Algunos campos de la cabecera IPv4 se han sacado o se han hecho opcionales, para reducir el costo del caso común de proceso de tratamiento de paquete y para limitar el costo del ancho de banda, de la cabecera IPv6.
- Soporte Mejorado para las Extensiones y Opciones. Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.
- Capacidad de Etiquetado de Flujo. Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cuál el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".

Formato de la cabecera IPv6.

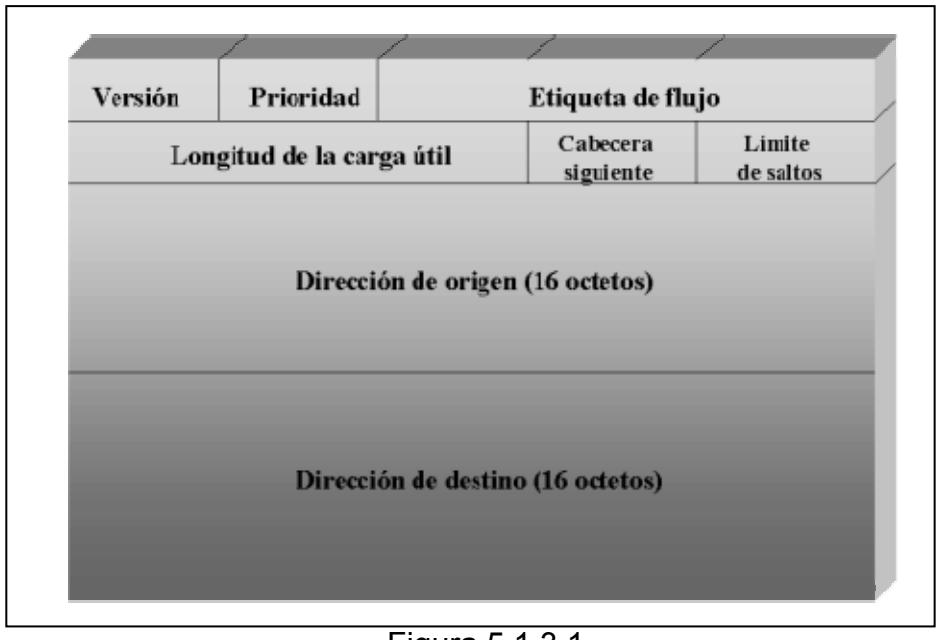


Figura 5.1.3.1

- Versión Número. Es la 6 del Protocolo de Internet de 4 bits.
- Prioridad. Campo de clase de tráfico de 8 bits.

- Etiqueta de Flujo. Etiqueta de 20 bits.
- Longitud de la Carga Útil. Entero sin signo de 16 bits. Es la longitud de la carga útil IPv6, es decir, el resto del paquete que sigue a esta cabecera IPv6, en octetos. Las cabeceras de extensión presente son parte de la carga útil, se incluyen en el conteo de la longitud.
- Cabecera Siguiente. Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6. Utiliza los mismos valores que el campo Protocolo del IPv4
- Límite de Saltos. Entero sin signo de 8 bits. Decrementado en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el Límite de Saltos llega a cero.
- Dirección Origen. Dirección de 128 bits del originador del paquete.
- Dirección Destino. Dirección de 128 bits del recipiente pretendido del paquete (posiblemente no el último recipiente, si está presente una cabecera enrutamiento).

Cabeceras de extensión IPv6.

En el IPv6, la información de capa internet opcional se codifica en cabeceras separadas que se pueden colocar entre la cabecera IPv6 y la cabecera de capa superior dentro de un paquete. Hay un número pequeño de tales cabeceras de extensión, cada una identificada por un valor de Cabecera Siguiente distinto. Un paquete IPv6 puede llevar cero, una, o más cabeceras de extensión, cada una identificada por el campo Cabecera Siguiente de la cabecera precedente.

Una implementación completa del IPv6 comprende la implementación de las siguientes cabeceras de extensión:

- Opciones de Salto a Salto
- Enrutamiento (Tipo 0)

- Fragmento
- Opciones de Destino
- Autenticación
- Seguridad del Encapsulado de la Carga Útil

Orden de las Cabeceras de Extensión

Cuando más de una cabecera de extensión se usa en un mismo paquete, se recomienda que esas cabeceras aparezcan en el siguiente orden:

- Cabecera IPv6
- Cabecera Opciones de Salto a Salto
- Cabecera Opciones de Destino
- Cabecera Enrutamiento
- Cabecera Fragmento
- Cabecera Autenticación
- Cabecera Seguridad del Encapsulado de la Carga Útil
- Cabecera Opciones de Destino
- Cabecera de Capa Superior

Cada cabecera de extensión debe ocurrir solamente una vez, a excepción de la cabecera Opciones de Destino la cual debe ocurrir a lo sumo dos veces (una vez antes de una cabecera Enrutamiento y la otra vez antes de una cabecera de capa superior). A continuación se describen algunas:

- Cabecera Opciones de Salto a Salto. Se usa para llevar información opcional que debe ser examinada por cada nodo a lo largo de la ruta de entrega del paquete.
- Cabecera Enrutamiento. Es utilizada por un origen IPv6 para listar uno o más nodos intermedios a ser "visitados" en el camino hacia el destino del paquete.

- Cabecera Fragmento. Es utilizada por un origen IPv6 para enviar un paquete más grande de lo que cabría en la MTU de la ruta hacia su destino. Para enviarlo, un nodo origen puede dividir el paquete en fragmentos y enviar cada fragmento como un paquete separado, para ser reensamblado en el receptor. El paquete original sólo se reensambla a partir de paquetes fragmento que tienen la misma Dirección Origen, Dirección Destino, e Identificación del Fragmento.
- Cabecera Opciones de Destino. Es usada para llevar información opcional que necesita ser examinada solamente por el(los) nodo(s) destino del paquete.
- Cabecera No Hay Siguiente. En el campo Cabecera Siguiente de una cabecera IPv6 o de cualquier cabecera de extensión indica que nada hay siguiendo esa cabecera. Si el campo Longitud de la Carga Útil de la cabecera IPv6 indica la presencia de octetos más allá del final de una cabecera, esos octetos deben ignorarse, y pasarse inalterados si el paquete se reenvía.

Cuestiones de Tamaño del Paquete.

El IPv6 requiere que cada enlace de Internet tenga una MTU (Unidad Máxima de Transferencia - Maximum Transfer Unit) de 1280 octetos o mayor. En cualquier enlace que no pueda llevarse un paquete de 1280 octetos en una pieza, debe proporcionarse fragmentación y reensamblaje específico al enlace en una capa debajo del IPv6.

Los Enlaces que tienen una MTU configurable deben configurarse para tener una MTU de por lo menos 1280 octetos; se recomienda que sean configurados con una MTU de 1500 octetos o mayor, para alojar posibles encapsulaciones (es decir, tunelizar) sin incurrir en la fragmentación de la capa IPv6.

De cada enlace al cual un nodo se conecta directamente, el nodo debe poder aceptar paquetes tan grandes como la MTU de ese enlace.

Un nodo debe poder aceptar un paquete fragmentado que, después del reensamblaje, sea tan grande como de 1500 octetos. Se permite a un nodo aceptar paquetes fragmentados de tal manera que reensamblan a más de 1500 octetos. Solo si se tiene la certidumbre que el destino es capaz reensamblar paquetes de ese tamaño.

Etiquetas de Flujo.

El campo Etiqueta de Flujo en la cabecera IPv6 puede ser usado por un origen para etiquetar secuencias de paquetes para los cuales solicita un manejo especial por los enrutadores IPv6, tal como la calidad de servicio no estándar o el servicio en "tiempo real".

Clases de Tráfico.

El campo Clase de Tráfico en la cabecera IPv6 está disponible para usarse por nodos originantes y/o enrutadores reenviantes para identificar y distinguir entre las diferentes clases o prioridades de paquetes IPv6.

Se utiliza para distinguir las fuentes que deben beneficiarse del control de flujo de otras. Esta distinción en los flujos permite que los routers reaccionen mejor en caso de congestión.

Cuestiones de Protocolo de Capa Superior.

- Sumas de Verificación de Capa Superior. Cualquier protocolo de transporte u otro de capa superior que incluya las direcciones de la cabecera IP en su cálculo de suma de verificación debe modificarse para el uso sobre el IPv6, para incluir las direcciones IPv6 de 128 bits en lugar de las direcciones IPv4

de 32 bits. A diferencia del IPv4, cuando los paquetes UDP son originados por un nodo IPv6, la suma de verificación UDP no es opcional. Es decir, siempre que se origine un paquete UDP, un nodo IPv6 debe calcular una suma de verificación UDP sobre el paquete y la pseudo cabecera. La versión IPv6 del ICPM (Internet Control Message Protocol - Protocolo de Control de Mensajes de Internet) [ICMPv6] incluye dicha pseudo cabecera en su cálculo de suma de verificación; éste es un cambio a diferencia de la versión IPv4 del ICMP. La razón para el cambio es para proteger al ICMP de una mala entrega o corrupción de aquellos campos de la cabecera IPv6 de los que depende, los qué, a diferencia del IPv4, no son cubiertos por una suma de verificación de la capa internet.

- Tiempo de Vida Máximo de un Paquete. A diferencia del IPv4, no se exigen a los nodos IPv6 cumplir con el tiempo de vida máximo de un paquete. Esa es la razón por la que el campo "Tiempo de Vida" del IPv4 se renombró a "Límite de Saltos" en el IPv6. En la práctica, muy pocas, si algunas, implementaciones IPv4 adoptan el requisito de limitar el tiempo de vida de un paquete, así que esto no es un cambio en la práctica.
- Contestando a Paquetes que Llevan Cabeceras Enrutamiento. Cuando un protocolo de capa superior envía uno o más paquetes en contestación a un paquete recibido que incluía una cabecera Enrutamiento, el(los) paquete(s) respuesta no debe(n) incluir una cabecera Enrutamiento que se derivó automáticamente "invirtiendo" la cabecera Enrutamiento recibida a menos que se hayan verificado la integridad y autenticidad tanto de la Dirección Origen como de la cabecera Enrutamiento recibida.

5.2 VPN

La Red Privada Virtual (RPV), en inglés Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Una VPN no es más que una estructura de red corporativa implantada sobre una red de recursos de carácter público, pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas, al fin y al cabo no es más que la creación en una red pública de un entorno de carácter confidencial y privado que permitirá trabajar al usuario como si estuviera en su misma red local.

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación.

Funcionamiento

La comunicación entre los dos extremos de la red privada a través de la red pública se hace estableciendo túneles virtuales entre esos dos puntos y usando sistemas de encriptación y autenticación que aseguren la confidencialidad e integridad de los datos transmitidos a través de esa red pública. Debido al uso de estas redes públicas, generalmente Internet, es necesario prestar especial atención a las cuestiones de seguridad para evitar accesos no deseados.

La tecnología de túneles (Tunneling) es un modo de envío de datos en el que se encapsula un tipo de paquetes de datos dentro del paquete de datos propio de algún protocolo de comunicaciones, y al llegar a su destino, el paquete original es desempaquetado volviendo así a su estado original.

En el traslado a través de Internet, los paquetes viajan encriptados, por este motivo, las técnicas de autenticación son esenciales para el correcto funcionamiento de las VPNs, ya que se aseguran a emisor y receptor que están intercambiando información con el usuario o dispositivo correcto.

La autenticación en redes virtuales es similar al sistema de inicio de sesión a través de usuario y contraseña, pero tienes unas necesidades mayores de aseguramiento de validación de identidades.

La mayoría de los sistemas de autenticación usados en VPN están basados en sistema de claves compartidas.

La autenticación se realiza normalmente al inicio de una sesión, y luego, aleatoriamente, durante el transcurso de la sesión, para asegurar que no haya algún tercer participante que se haya podido entrometer en la conversación.

Todas las VPNs usan algún tipo de tecnología de encriptación, que empaqueta los datos en un paquete seguro para su envío por la red pública.

La encriptación hay que considerarla tan esencial como la autenticación, ya que permite proteger los datos transportados de poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión.

Existen dos tipos de técnicas de encriptación que se usan en las VPN: Encriptación de clave secreta, o privada, y Encriptación de clave pública.

En la encriptación con clave secreta se utiliza una contraseña secreta conocida por todos los participantes que van a hacer uso de la información encriptada. La contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de sistema tiene el problema que, al ser compartida por todos los

participantes y debe mantenerse secreta, al ser revelada, tiene que ser cambiada y distribuida a los participantes, lo que puede crear problemas de seguridad.

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las redes virtuales, la encriptación debe ser realizada en tiempo real, de esta manera, los flujos de información encriptada a través de una red lo son utilizando encriptación de clave secreta con claves que son válidas únicamente para la sesión usada en ese momento.

Tipos de VPN.

VPN de acceso remoto

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 preparados, 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

Este esquema se utiliza para conectar oficinas remotas con la sede central de la 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. Es más común el punto anterior, también llamada tecnología de túnel o tunneling.

Tunneling

Internet se construyó desde un principio como un medio inseguro. Muchos de los protocolos utilizados hoy en día para transferir datos de una máquina a otra a través de la red carecen de algún tipo de cifrado o medio de seguridad que evite que nuestras comunicaciones puedan ser interceptadas y espiadas. HTTP, FTP, POP3 y otros muchos protocolos ampliamente usados, utilizan comunicaciones que viajan en claro a través de la red. Esto supone un grave problema, en todas aquellas situaciones en las que queremos transferir entre máquinas información sensible, como pueda ser una cuenta de usuario (nombre de usuario y contraseña), y no tengamos un control absoluto sobre la red, a fin de evitar que alguien pueda interceptar nuestra comunicación por medio de la técnica del hombre en el medio (man in the middle), como es el caso de la Red de redes.

El problema de los protocolos que envían sus datos en claro, es decir, sin cifrarlos, es que cualquier persona que tenga acceso físico a la red en la que se sitúan las máquinas puede ver dichos datos. De este modo, alguien que conecte su máquina a una red y utilice un sniffer recibirá y podrá analizar por tanto todos los paquetes que circulen por dicha red. Si alguno de esos paquetes pertenece a un protocolo

que envía sus comunicaciones en claro, y contiene información sensible, dicha información se verá comprometida.

Si por el contrario, se cifran las comunicaciones con un sistema que permita entenderse sólo a las dos máquinas que son partícipes de la comunicación, cualquiera que intercepte desde una tercera máquina los paquetes, no podrá hacer nada con ellos, al no poder descifrar los datos. Una forma de evitar este problema, sin dejar por ello de utilizar todos aquellos protocolos que carezcan de medios de cifrado, es usar una técnica llamada tunneling.

Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (Secure SHell), a través de las cuales realizaremos las transferencias inseguras, que pasarán de este modo a ser seguras. De esta analogía viene el nombre de la técnica, siendo la conexión segura (en este caso de ssh) el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar.

Ventajas

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costes y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.

5.3 Aplicaciones

5.3.1 MPLS.

Sobre todo en redes de alto rendimiento, donde las decisiones de enrutamiento que han de tomar los routers MPLS con base en la LIB (Label Information Base – Tabla de identificador de etiquetas) son mucho más sencillas y rápidas que las que toma un "router" IP ordinario (la LIB es mucho más pequeña que una tabla de rutas normal). La anidación de etiquetas permite agregar flujos con mucha facilidad, por lo que el mecanismo es escalable.

MPLS y ruteo de tráfico salto a salto.

Varios usos de MPLS requieren que los paquetes con una determinada etiqueta de envío sean transmitidos a través del mismo camino de ruteo salto a salto que pudiera ser utilizado para la transmisión de un paquete con una dirección especificada en su campo de dirección de destino de capa de red.

MPLS y LSP explícitamente enrutados.

Hay una serie de razones por las que puede ser conveniente el uso de enrutamiento explícito en lugar del enrutamiento salto a salto. Por ejemplo, esto permite rutas basadas en políticas administrativas, y permite que las rutas que tomen los LSPs sean cuidadosamente diseñadas para permitir la ingeniería de tráfico [MPLS-TRFENG].

Ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados.

A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los “routers” correspondientes haga aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.

- Permite hacer “encaminamiento restringido” (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios.
- Especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.
- La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

5.3.2 Aplicaciones A-bis sobre MPLS.

La denominada Conmutación de Etiquetas de Multiprotocolo (MPLS), opera independientemente de la tecnología de acceso. MPSL es usado generalmente como una red principal de trasporte para diferentes redes de acceso tales como ATM, IP, TDM, SDH, etc.

MPLS crea flujos, los cuales pueden ser mantenidos en una forma similar a una conexión orientada a una red IP, los flujos pueden ser monitoreados y dirigidos, por lo que se tiene la capacidad de reservar o liberar ancho de banda.

Trasporte de 2G TDM.- La forma de trasportar el trafico de TDM es haciendo una emulación de circuitos sobre MLPS.

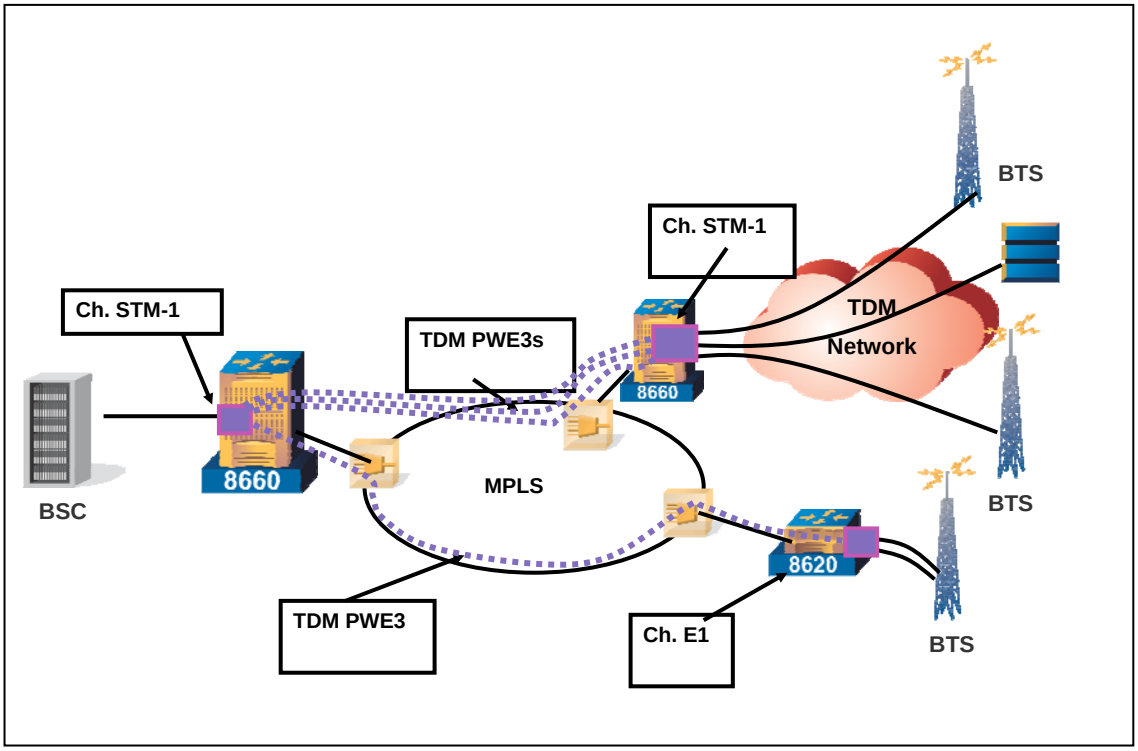
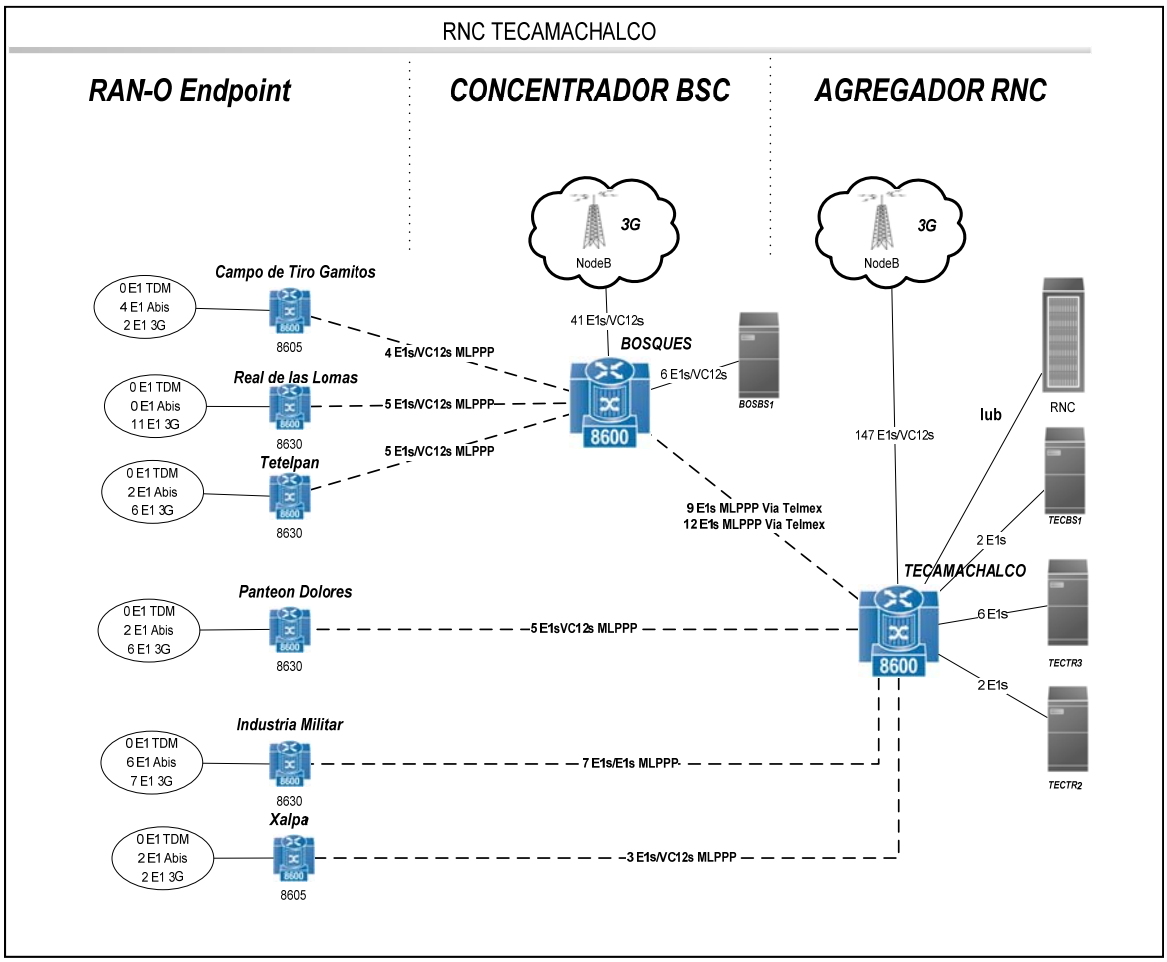


Figura 5.3.2.1

En la siguiente figura se muestra como el tráfico de 2G y 3G son trasportados a través de la red MPLS.



FiFigura. 5.3.2.2 Aplicaciones de MPLS.

- ATM: Asynchronous Transfer Mode. Es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones

- IMA: Inverse Multiplexing for ATM. Es una tecnología usada para transportar tráfico ATM sobre un conjunto de líneas E1 o T1, al que se da el nombre de

grupo IMA (en inglés IMA group). Esta tecnología permite un incremento gradual de la capacidad de transporte de tráfico.

- MLPPP: Multilink PPP (MLPPP) es un método para dividir, recombinar, y mantener la secuencia lógica de datagramas a través de múltiples enlaces de datos agrupados de manera que parezcan de mayor capacidad.

- MPLS: Multiprotocol Label Switching*.* Es un mecanismo de transporte de datos estándar creado por la IETF. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP

- LSP: Label Switched Path*. E*s una ruta sobre una red MPLS, establecida por un protocolo de señalización como LDP, RSVP o CR-LDP. La ruta es establecida basándose en los criterios de ingeniería de tráfico establecida

- Pseudowire: (o Circuito). Conexión lógica en MPLS entre dos “end-points” normalmente del mismo tipo (ATM, Ethernet, CES, VLAN) mediante el cual se trasporta el tráfico en ellos. Estos Pseudowires pueden ser Locales o Remotos

En esta figura se muestra la red de trasporte donde se trasporta el tráfico de 3G y 2G con la interfaz A-bis optimada.

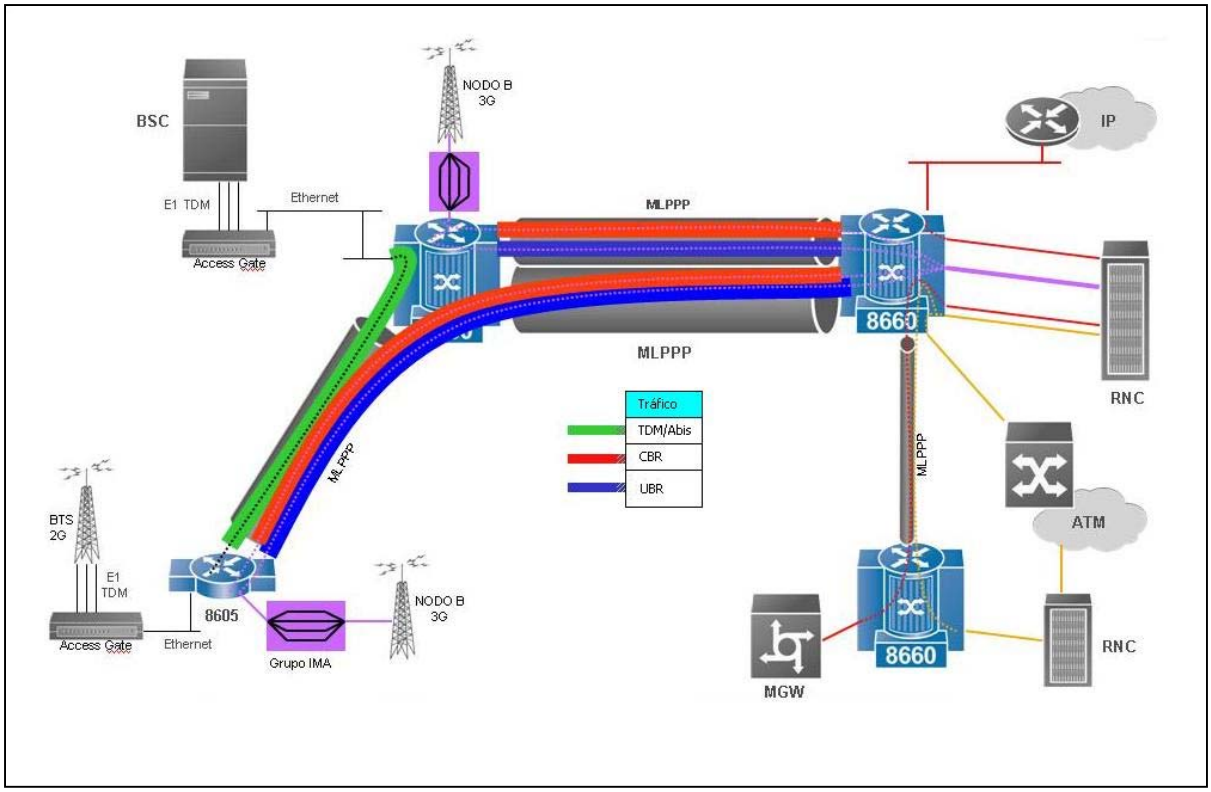


Figura 5.3.2.2 Tráfico 3G