Clasificación de las Redes Privadas Virtuales

Por MsC. Javier Rafael Gómez Valdivia
Subgerente Filial de CUBADATA, Sancti Spíritus, ETECSA
javier@ssp.tel.etecsa.cu

Las primeras redes de computadoras fueron implementadas con dos tecnologías fundamentales: líneas dedicadas —*leased lines*— para una conectividad permanente, y conexiones conmutadas —*dial-up lines*— para requerimientos de conectividad ocasional[1]. Estas redes iniciales brindaban a los usuarios gran seguridad —para tener acceso a datos transportados sobre líneas dedicadas hay que tener equipamiento y acceso físico a dichas líneas—; pero no una buena relación costo-beneficio por dos razones esenciales: la primera, el promedio de tráfico entre dos sitios cualesquiera de una red varía debido a muchos factores, entre ellos, el momento del día, de la semana, del mes, etc.; la segunda, los usuarios finales siempre necesitan respuestas más rápidas, lo que requiere de mayores anchos de banda entre los sitios de red, no obstante, el ancho de banda de una línea dedicada sólo es usado una parte del tiempo cuando el usuario está activo.

Estas dos razones llevaron a la industria del transporte de datos y a los proveedores de servicios a desarrollar e implementar esquemas de multiplexores estadísticos que brindan a los clientes servicios equivalentes a líneas dedicadas. En Cuba la primera red privada virtual basada en estas tecnologías fue la X.25, luego *Frame Relay* y más tarde ATM. La figura 1 muestra una VPN típica construida con estas tecnologías —*Frame Relay*—.

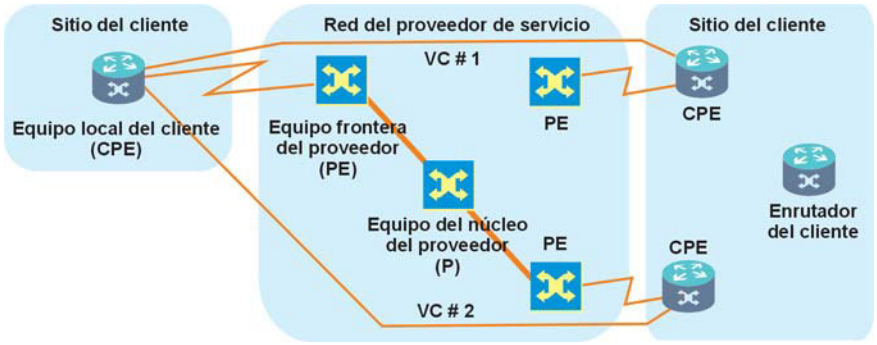

Figura 1 Ejemplo de VPN sobre Frame Relay

Las soluciones VPN tienen, en sentido general, un número de componentes (Figura 1) entre los que pueden mencionarse: el Proveedor de Servicio —*Service Provider* (SP)— que es la organización propietaria de la infraestructura —el equipamiento y el medio de transmisión— con la que brinda emulación de líneas dedicadas a los clientes; la conexión del cliente a la red del SP a través del equipo local del cliente —*Customer Premises Equipment* (CPE)—. Usualmente el CPE es un PAD —*Packet Assembly and Disassembly*— que brinda conectividad terminal, un *bridge* o un enrutador. También es llamado frontera del cliente —*Customer Edge* (CE)—; el CPE es conectado a través de un medio de transmisión —líneas dedicadas, pero también puede ser de forma conmutada— al equipo del SP que puede ser X.25, *Frame Relay*, ATM o un enrutador IP. El dispositivo de frontera del SP es llamado PE —*Provider Edge*—; el *Service Provider* generalmente tiene equipos de núcleo en la red llamados P —*Provider*—.

Con la introducción de nuevas tecnologías en las redes de los SP y los nuevos requerimientos de los clientes, las implementaciones de VPN son mayores y más

complejas, los servicios de VPN modernos recorren gran variedad de tecnologías y topologías.

Existe una clasificación según tipos de IP VPN dados en la RFC 2764, una división en categorías según el alcance de las VPN para las organizaciones, y según los modelos implementados superpuestos, y par a par.

En la RFC 2764 los IP VPN están definidos en cuatro tipos [2,3]:

- Las Líneas Dedicadas Virtuales —*Virtual Leased Lines* (VLLs)— brindan enlaces punto a punto entre los sitios de los clientes orientados a conexión. El cliente percibe cada VLL como un enlace (físico) privado dedicado, aunque en realidad está realizado por un túnel IP a través del *backbone* de la red, el protocolo de túnel IP utilizado debe ser capaz de transportar cualquier protocolo entre los sitios conectados por las VLLs.
- Los Segmentos LAN Privados Virtuales —*Virtual Private LAN Segments* (VPLS)— brindan una imitación de LAN entre sitios VPLS, como con las VLLs, un VPLS requiere del uso de túneles IP que sean transparentes a los protocolos transportados por las LAN simuladas. Las LAN pueden ser simuladas con el uso de un engranaje de túneles entre los sitios de los clientes o por el mapeado de cada VPLS a una dirección IP multicast separada.
- Las Redes de Enrutadores Privados Virtuales —*Virtual Private Routed Networks* (VPRNs)— simulan redes dedicadas de enrutadores IP entre los sitios de los clientes, aunque una VPRN transporte tráfico IP, debe ser tratada como un dominio de enrutamiento separado desde la subyacente red del SP. Como la VPRN es probablemente usada por varios clientes asignando direcciones IP, cada cliente se ve como el operador de la red y, por lo tanto, puede asignarse las direcciones IP como desee.
- Las Redes Conmutadas Privadas Virtuales —*Virtual Private Dial Networks* (VPDNs)— permiten a los clientes que el SP le aprovisione y gestione los accesos conmutados a su red. En lugar de que cada cliente configure sus servidores de acceso y use secciones PPP —*Point to Point Protocol*— entre un local central y los usuarios remotos, el SP brinda uno o muchos servidores de accesos compartidos. Secciones PPP para cada VPDN son transportadas con el empleo de túneles desde el servidor de acceso del SP hasta un punto de acceso dentro de la red del cliente, conocido como concentrador de acceso.

Según la utilización que le dan las organizaciones a las VPN, pueden ser divididas en tres categorías: VPN intranet, entre departamentos de una misma organización; VPN extranet, entre una organización, sus socios, clientes y suministradores (Figura 3); y VPN con accesos remotos, entre la organización y empleados móviles o remotos.

Las VPN intranet que se utilizan para interconectar departamentos o dependencias de una misma organización son generalmente redes con alto nivel de aislamiento y seguridad, además, requieren de garantías de calidad de servicio para aplicaciones críticas. Principalmente por estas dos razones es que muchas organizaciones no utilizan Internet para este tipo de VPN. Las VPN intranet usualmente son implementadas con tecnologías tradicionales como X.25, *Frame Relay* o ATM (Figura 2).

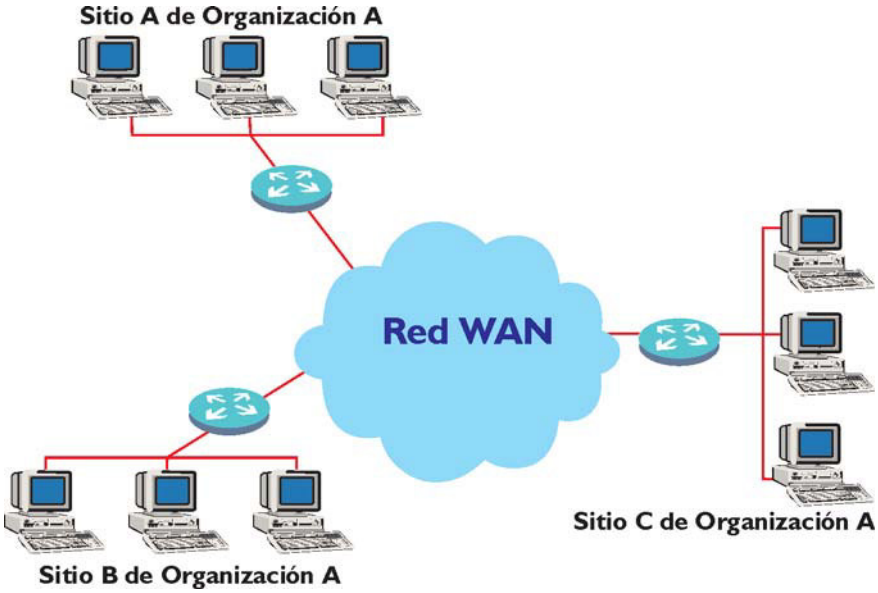

Figura 2 VPN como intranet

Figura 3 Configuración típica de una VPN extranet utilizando Internet

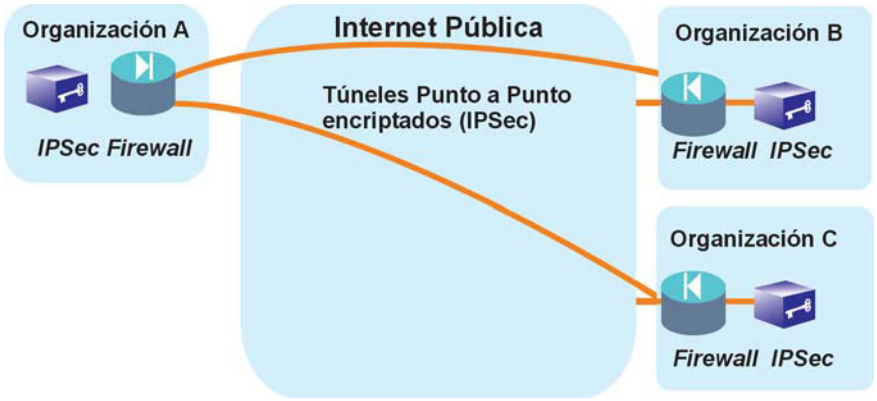

Figura 4 VPN como extranet

Las VPN extranet frecuentemente tienen lugar interconectando sitios principales de diferentes organizaciones, dedican dispositivos de seguridad como *firewall* o de encriptación, similar a la configuración mostrada en la figura 3.

Esta configuración presenta menos requerimientos de calidad de servicio, lo que hace a Internet más adaptable a este tipo de VPN para la comunicación entre organizaciones; no es una sorpresa que cada vez más tráfico entre organizaciones se realice a través de Internet. La figura 4 muestra una VPN extranet.

Por último, las VPN con accesos remotos presentan características similares a las VPDN de la RFC 2764 y utilizan protocolos como L2F —*Layer 2 Forwarding*— ó L2TP —*Layer 2 Tunneling Protocol*— (Figura 5).

Estas categorías no son excluyentes, es decir, una red puede estar conformada por una combinación de ellas, incluso, por la unión de las tres.

De los posibles modelos de VPN existen dos que han ganado en uso: el modelo superpuesto (*overlay*), donde el SP simula líneas dedicadas para el cliente; y el modelo par a par —*peer to peer*— en el cual el SP y el usuario intercambian información de enrutamiento de nivel 3, con la que el proveedor transporta los datos entre los sitios del usuario por un trayecto óptimo sin intervención del usuario.

El modelo superpuesto puede comprenderse mejor porque en él existe una separación entre las responsabilidades del cliente y del SP. El SP brinda al cliente una configuración que simula líneas dedicadas llamadas circuitos virtuales —*Virtual Circuit* (VC)—, los cuales pueden estar disponibles constantemente —*Permanent Virtual Circuit* (PVC)— o establecidos bajo demanda —*Switched Virtual Circuit* (SVC)—.

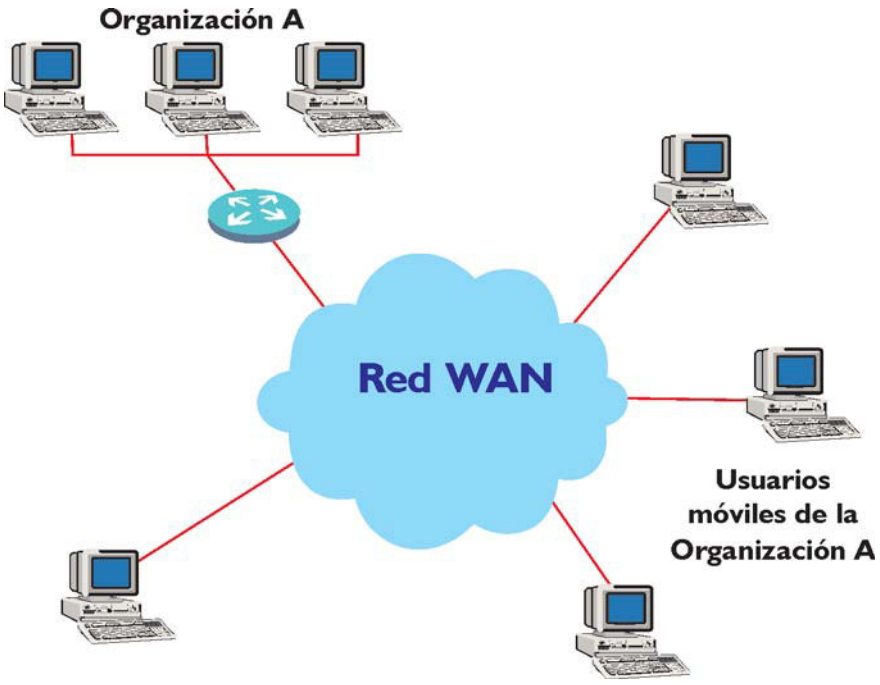

Figura 5 VPN con accesos remotos

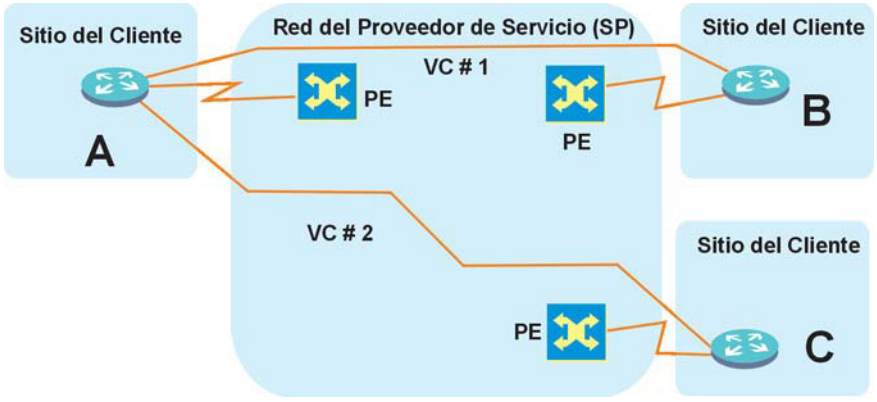

Figura 6 Ejemplo de topología de red VPN superpuesta

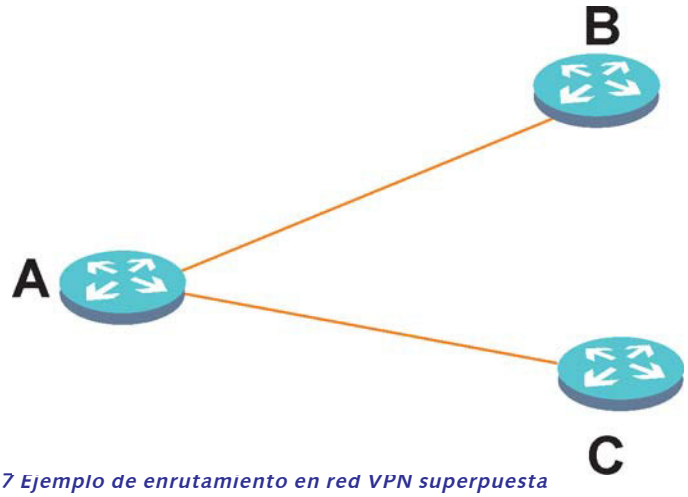

Figura 7 Ejemplo de enrutamiento en red VPN superpuesta

La figura 6 muestra un ejemplo de topología de VPN superpuesta donde el cliente establece comunicación entre sus enrutadores sobre los VCs suministrados por el SP. La información de los protocolos de enrutamiento siempre es intercambiada entre los dispositivos del cliente, por lo que el SP desconoce la topología interna de la red del cliente. La figura 7 ejemplifica la topología del enrutamiento en la red de la figura 6.

En el modelo par a par, el PE es un enrutador que intercambia directamente información de nivel 3 con el CPE (Figura 8).

Las redes VPN pueden ser clasificadas por varias vías. La clasificación más utilizada se basa en el intercambio o no de la información de enrutamiento entre los clientes y los SP. En el modelo VPN par a par se intercambia información de enrutamiento entre los enrutadores de los clientes y de los SP. En el de VPN superpuesta, el SP sólo brinda VC —similar a líneas dedicadas— y la información de enrutamiento es intercambiada directamente entre los enrutadores de los clientes. En grandes redes de SP los dos modelos pueden ser combinados, el VPN par a par puede utilizar VPN superpuesta en la parte de acceso, por ejemplo, los clientes conectados a los enrutadores PE a través de *Frame Relay* o ATM o en el núcleo, enlazando los enrutadores P del SP a través de ATM.

El modelo VPN superpuesta puede implementarse con tecnologías de conmutadores de redes WAN de nivel 2 —*Frame Relay*, SMDS, ATM— o con tecnologías de túneles de nivel 3 —IP sobre IP, IPSec—. Tradicionalmente, el modelo VPN par a par ha sido implementado con complejos artificios de enrutamiento o con listas de acceso IP, lo cual ha presentado inconvenientes. Las

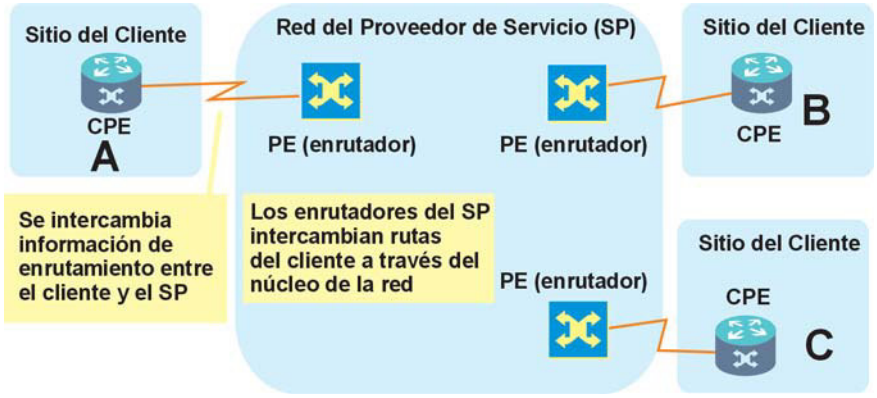

Figura 8 Ejemplo de VPN par a par

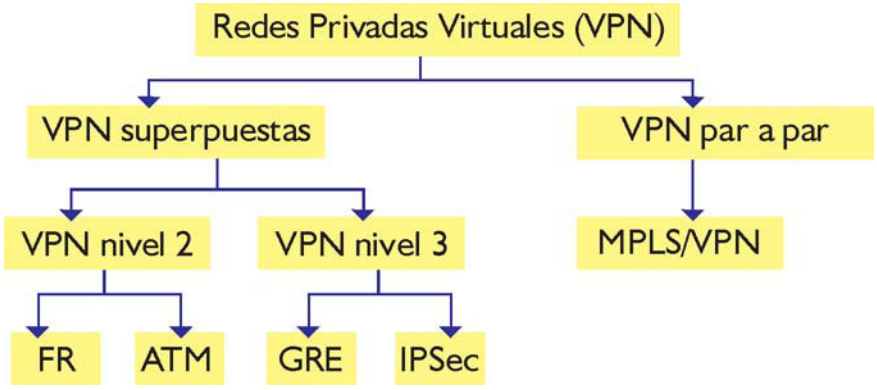

Figura 9 Clasificación de las VPN según tecnología subyacente

VPN basadas en MPLS superan la mayor parte de los inconvenientes y permiten a los SP la combinación de los beneficios de los modelos par a par —simplificar el enrutamiento, simplificar la implementación de los requerimientos de los clientes—, con la seguridad y el aislamiento del modelo de VPN superpuesta [4]. La figura 9 muestra la clasificación de las diferentes VPN.

De manera general, en este artículo se han descrito las diferentes clasificaciones de las Redes Privadas Virtuales, tanto las VPN que utilizan el modelo superpuesto como las que utilizan el modelo par a par. Actualmente, es una realidad la oferta del servicio de VPN por los proveedores de servicios de datos con el uso de diferentes tecnologías. Debido al crecimiento de Internet y a que la gran mayoría de las aplicaciones son para redes de tráfico IP, es vital para estos proveedores la migración hacia tecnologías que permitan brindar servicios de VPN más eficientes y con mayores prestaciones en el transporte de tráfico IP. En ETECSA, la Unidad de Negocio CUBADATA ya está dando los primeros pasos para brindar servicios sobre un *backbone* IP/MPLS, específicamente, VPN de capa 3 sobre MPLS.

Notas

[1] Zeus Kerravala . "The Evolution of Virtual Private Networks" (Octubre 2002). Disponible en: http://www.webtorials.com/main/resource/papers/nortel/paper6/yankee-vpn.pdf (Consultado: abril, 2004).

[2] Paul Brittain. "MPLS Virtual Private Network", Data Connection (2000) Disponible en: http://www.dataconnection.com/ (Consultado: mayo, 2004).

[3] IETF. "RFC 2764. IP based VPN" (Febrero 2000). Disponible en: http://www.ietf.org/rfc/rfc2764.txt (Consultado: mayo, 2004).

[4] Jim Guichard e Ivan Pepelnjak. "MPLS and VPN Architectures". Londres: Cisco Press, 2000.

Bibliografía

Cisco White Paper. "MPLS for VPNs" (2002). Disponible en: http://www.hp.com/communications/patners/cisco/joint/hpcisco-mpls-brochure.pdf (Consultado: abril, 2004).

Data Connection. "VPN Technologies-a Comparison"(2002). Disponible en: http://www.dataconnection.com/iprouting/wpdl.htm (Consultado: mayo, 2004).

Frame Relay FORUM. "Frame Relay VPNs"(2003). Disponible en: http://www.webtorials.com/main/resource/papers/frforum/paper3/vpn.pdf (Consultado: mayo, 2004).

Gómez, A.F. "RedIRIS. Redes Privadas Virtuales Dinámicas"(Nov. 2002). Disponible en: http://www.rediris.es/rediris/boletin/54-55/ponencia2.html (Consultado: marzo, 2004).

Hernández, Erich. "Manual de Redes Privadas Virtuales"(2002). Disponible en: http://www.geocities.com/erichernandezp/indice.htm (Consultado: abril, 2004).

Internet Week. "VPN Frequently Ask Questions"(2004). Disponible en: http://www.internetweek.com/VPN/faq.htm (Consultado: abril, 2004).

Luyuan, Fang . "Design and Deploy Scalable MPLS VPN in Large IP Networks"(2003) Disponible en: http://www.webtorials.com/main/MPLScon2003/20030521/FANG.pdf (Consultado: mayo, 2004).