SIMULACIÓN DE ENTORNO VPN EN OPNET

FERNANDO JAVIER SUAREZ LOPEZ

LUIS DAVID TOLOZA MOLINA

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIA ELECTRONICA Y ELECTRICA

CARTAGENA D.T. Y C.

2008

SIMULACIÓN DE ENTORNO VPN EN OPNET

FERNANDO JAVIER SUAREZ LOPEZ

LUIS DAVID TOLOZA MOLINA

Monografía presentada como requisito para optar al titulo de Ingeniero Electrónico

ASESOR

GONZALO LOPEZ VERGARA

INGENIERO ELECTRONICO

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIA ELECTRONICA Y ELECTRICA

CARTAGENA D.T. Y C.

2008

Cartagena, 01 Diciembre de 2008

Señores

Comité curricular de Ingeniería Eléctrica y Electrónica.

Universidad Tecnológica de Bolívar

Ciudad

Respetados Señores:

Por medio de la presente me permito informarles que la monografía titulada "**SIMULACIÓN DE ENTORNO VPN EN OPNET**" ha sido desarrollada de acuerdo a los objetivos establecidos.

Como autores de la monografía consideramos que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

_____ _____

LUIS DAVID TOLOZA MOLINA **FERNANDO JAVIER SUAREZ LOPEZ**

Cartagena, 01 Diciembre de 2008

Señores

Comité curricular de Ingeniería Eléctrica y Electrónica.

Universidad Tecnológica de Bolívar

Respetados Señores:

Cordialmente me permito informarles, que he llevado a cabo la dirección del trabajo de grado de los estudiantes Luís David Toloza Molina y Fernando Javier Suárez López, titulado **SIMULACIÓN DE ENTORNO VPN EN OPNET.**

Atentamente,

_____

GONZALO LOPEZ VERGARA

Ingeniero Electrónico

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Cartagena de Indias D. T. y C. 01 Diciembre de 2008

DEDICATORIA

A Dios y a la Virgen por la fortaleza y

la voluntad para culminar exitosamente

esta etapa de mi vida.

A mis padres David Toloza y Rocio Molina por sus esfuerzos

y sacrificios, por brindarme siempre su apoyo y permitir

Materializar mis sueños e ideales.

A mis profesores por transmisitir sus conocimiento

Y contribuir a mi formación personal.

Luis David Toloza Molina.

DEDICATORIA

A Dios y a los ángeles por darme la gracia y fortaleza

Para vencer todos los obstáculos para

Culminar este proceso.

A mis padre Edicson Suárez y Martha López por

Apoyarme desde un primero momento

Y ayudarme a no desfallecer y acompañarme hasta

Lograr este triunfo que le da gran sentido a mi vida.

A mis amigos por estar conmigo y por

Crearme grandes recuerdos.

Fernando Javier Suárez López.

SIMULACIÓN DE ENTORNO VPN EN OPNET

Cartagena D.T y C., Diciembre 03 de 2008

Señores
UNIVERSIDAD TECNOLOGICA DE BOLIVAR
Cartagena

Como autores del trabajo de grado “SIMULACION DE ENTORNO VPN EN OPNET”, nosotros LUIS DAVID TOLOZA MOLINA Identificado con CC. 1.128.046.098 de Mompòs y FERNANDO JAVIER SUAREZ LOPEZ con CC. 1.128.055.727 de Cartagena, en uso de nuestras facultades legales, autorizamos a la biblioteca de la Universidad Tecnológica de Bolívar para la utilización del mismo.

Dado en Cartagena de indias. Distrito Turístico y Cultural. A los 03 días del mes de Diciembre de 2008.

---------- ----------

LUIS DAVID TOLOZA MOLINA **FERNANDO JAVIER SUAREZ LOPEZ**

CC. 1.128.389.453 De Mompos CC.1.128.055.727 De C/gena

INDICE

INDICE DE FIGURAS

INTRODUCCION

Con el paso del tiempo, la expansión de la mayoría de las empresas existentes es la prioridad para responder a la creciente demanda que puedan llegar a obtener, dentro de este auge se hace necesaria la implementación de nuevos mecanismos para el acceso a información entre sus redes de área local, lo cual es el gran dolor de cabeza para empresas que se encuentren geográficamente distantes.

Las soluciones de cableado mediante los distintos medios de transmisión guiados (cable coaxial, fibra óptica, etc.) usando equipos con rendimiento superior puede hasta cierto punto ser efectiva, pero en la mayoría de los casos excesivamente costosa, este es el punto de partida para empezar a pensar en alternativas de conexión entre redes LAN, que disminuyan costos de operación, montaje y movilidad en una empresa.

Una forma eficaz de efectuar estas conexiones puede ser puesta a punto mediante la utilización de una red privada virtual (VPN), la cual minimizara los costos de infraestructura obteniendo resultados de conexión satisfactorios para a la ejecución de aplicaciones entre las redes a montar,

Las redes virtuales privadas manejan protocolos de seguridad que permiten conseguir acceso a servicios y aplicaciones de carácter privado, únicamente a personal autorizado en determinada empresa, organización, compañía, etc.; el modo de operación es mediante Internet, cuando un usuario se conecta, la configuración de la red privada virtual le permite conectarse a la red privada del destino, de esta manera accede a las aplicaciones de este como si estuviera tranquilamente sentado en su oficina.

La estructura de este proyecto se pasa principalmente en la simulación de esta topología de red se utilizara el software OPNET IT GURU ACADEMIC EDITION 9.1 el cual es un apoyo valido para examinar la red privada virtual, motivo por el cual se analizaran este modelo de red, en distintos escenarios con el fin de mostrar de forma detallada la operación de la aplicación.

En los anexos se incluyen pruebas reales correspondientes a una red VPN las cuales fueron configuradas en base a las simulaciones realizadas en el software analizado.

CAPITULO 1

INTRODUCCION A LAS VPN

1.1 Definición De Una Red Privada Virtual

Una Virtual Private Network (VPN) es un método de conexión utilizado para simular una red privada sobre una red pública, en este caso es Internet. La idea es que la red pública sea "vista" desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

Este tipo de enlace admite la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN, lo cual es conveniente para empresas con personal disperso, o que se encuentren geográficamente distantes.

La forma de comunicación entre los hosts a una red privada es a través de la red pública (Internet), el cual se logra estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autentificación que aseguran la confidencialidad de los paquetes transmitidos utilizando la red pública.

Debido a que se está trabajando con redes públicas, en la mayoría de los casos es necesario tener muy en claro los parámetros de seguridad, que se abordan a través de estos esquemas de encriptación y autentificación y que se describirán a continuación.

La tecnología de túneles "Tunneling" es una forma de transferencia de datos la cual se encapsulan paquetes de datos con el fin de tener el control de la información en el destinatario y de esta manera determinar errores en la transmisión de archivos, que en algunas ocasiones difiere del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

Los modos de identificación son fundamentales en las VPNs, debido a que estas aseguran a los usuarios que están intercambiando información con el destino correcto debido a que se realiza mediante un nombre de usuario y contraseña, esto con el fin de brindar mayores rangos de protección contra violaciones.

Todas las VPN requieren encriptar datos, este proceso es indispensable para llegar a el destino, en este proceso se protegen los datos transportados para poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión.

1.2 Antecedentes De Redes Privadas Virtuales

Inicialmente los viajantes empleados de la empresa accedían a los datos que necesitaban de la central mediante llamadas telefónicas, en ella se encontraban varias operadoras que se encargaban de acceder a los datos y comunicárselos a los empleados.
Ante al gran desarrollo de las tecnologías de telecomunicaciones se pensó en una reestructuración total en el modo de acceder a los datos por parte de los viajantes, creando una red que interconectara a éstos con la central y posibilitando que tuvieran acceso total a todos los equipos conectados a la red con independencia del tiempo o del lugar donde se encontraran.
La empresa deseaba también una garantía de seguridad en las transferencias de información que evitara que sus datos fuesen interceptados por personas ajenas a la empresa.

1.3 Razones Para Implementar Una Red Privada Virtual

Las VPN son una salida al costo que puede significar el pagar una conexión de alto costo, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red.

Los datos son codificados o cifrados y recién enviados a través de la conexión, para de esa manera asegurar la información y el password que se esté enviando.
Esta tecnología proporciona un medio para aprovechar un canal público de Internet como un canal privado o propio para comunicar datos que son privados. Más aún, con un método de codificación y encapsulamiento, una VPN básica, crea un camino privado a través de Internet. Esto reduce el trabajo y riesgo en una gestión de red.

Las VPNs son una gran solución a distintos problemas, pero solo en el campo de la economía de los usuarios porque, por ejemplo en el caso de que se realice una conexión entre dos sedes de empresas, una en Japón y la otra en Perú, sería muy costoso el realizar un cableado entre estos dos países, y un enlace inalámbrico satelital sería muy costoso. Es por ello que una red privada virtual es más económica porque solo se hace uso de Internet que es un conjunto de redes conectadas entre si.

1.4 Requerimientos Y Componentes Básicos De Una VPN.

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione: Identificación de usuario, Administración de direcciones, Codificación de datos, Administración de claves, Soporte a protocolos múltiples.

1.4.1 Identificación de usuario

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.

1.4.2 Administración de direcciones

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

1.4.3 Codificación de datos

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

1.4.4 Administración de claves

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

1.4.5 Soporte a protocolos múltiples

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet (IP), el intercambio de paquete de internet (IPX) entre otros.

CAPITULO 2.

PROTOCOLOS UTILIZADOS EN UNA VPN.

Para que se establezca un túnel tanto el cliente del túnel como el servidor del túnel deberán utilizar el mismo protocolo de túnel. La tecnología del túnel se puede basar ya sea en el protocolo del túnel de nivel 2 ò nivel 3. Los protocolos de nivel 2 corresponden al nivel de enlace de datos, y utilizan tramas como su unidad de intercambio, PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer-2 Tunneling Protocol) y L2F (Layer 2 Forwarding) son los protocolos de túneles de nivel 2, estos encapsulan la carga útil en una trama de protocolo de punto a punto (PPP)

Los protocolos de nivel 3 corresponden al nivel de la red y utilizan paquetes, IP sobre IP y el modo de túnel de seguridad IP (IPSec) son ejemplos de los protocolos de túnel de nivel 3. Estos protocolos encapsulan los paquetes IP en un encabezado adicional IP antes de enviarlos a través de una red.

2.1 PPTP

Este es un protocolo desarrollado por Microsoft y normalizado por la IETF (Internet Engineering Task Force) como RFC 2637 fecha para el acceso a redes privadas virtuales. Este protocolo de red nos permite la realización de transferencias de clientes remotos a servidores localizados en redes privadas. Para ello emplea tanto líneas telefónicas conmutadas como Internet.

PPTP es una extensión de PPP que soporta control de flujos y túnel multiprotocolo sobre IP.

El acceso a una red privada remota empleando PPTP dispone de dos componentes que trabajan en paralelo:

- Control de la conexión a la red privada, empleando el protocolo TCP, entre el equipo (host) remoto y el servidor de túneles.
- Funcionamiento del túnel IP entre el equipo remoto y el servidor de túneles.

En el control de la conexión, se establece una conexión TCP entre el equipo remoto y el puerto 1723 (reservado para este uso en el documento RFC 1700) del servidor de túneles. Esta conexión tiene como objetivo el establecimiento y la gestión de las sesiones que el usuario establece en la red privada y son transportadas por el túnel. El formato de los paquetes en el control de la conexión será como se ilustra en la *figura 2.1:*

Capa de enlace	**IP:Ippublic_rem<->Ippub_serv_tuneles**	**TCP:Puerto_Cliente<->Puerto_Servidor(1723)**	**Datos**

Figura 2.1 - Encabezado de la trama PPTP.

La capa de enlace será la que proporciona el ISP (Internet Service Provider) al equipo remoto. En el caso de Windows 9x, 2000, XP se emplea el protocolo PPP en la fase de establecimiento de la conexión punto a punto entre el ISP y el equipo remoto, seleccionando a continuación como capa de enlace Ethernet aunque en la fase de establecimiento y liberación de la conexión se emplea PPP. La capa de red y de transporte gestiona el establecimiento de una conexión TCP desde el cliente (equipo remoto) al puerto 1723 del servidor (servidor de túneles, router de la red corporativa), empleando el direccionamiento público que proporciona el ISP al equipo remoto y que posee el servidor de túnel para el acceso a Internet.

El funcionamiento del túnel IP permite el envío de paquetes IP con direccionamiento privado, empleando un protocolo de control de túnel (GRE – Generic Routing Encapsulation) y un protocolo de control de enlace entre el

equipo remoto y el servidor de túneles. El efecto de este túnel para el usuario del equipo remoto será proporcionarle un acceso a la red LAN corporativa a nivel de red, con una dirección de la red privada. El servidor de túneles se encarga del traspaso de los paquetes de la red LAN que vayan dirigidos a la dirección IP del equipo remoto o a la de broadcast. El protocolo de nivel de enlace entre el equipo remoto y el servidor de túneles es PPP, pues permite un control establecido de sesiones y autentificación mediante protocolos PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) o MS-CHAP (Microsoft Challenge Handshake Authentication Protocol). El formato de los paquetes que circularan por el túnel será como se muestra en la figura 2.2:

Figura 2.2 - Formato del paquete IP que transita por el túnel.

La parte de la cabecera correspondiente a la cabecera de enlace ISP, cabecera IP publica, cabecera GRE y cabecera PPP se interpretan entre el equipo remoto y el servidor de túneles para el transporte del paquete de la red privada. La parte correspondiente a la cabecera IP privada y datos se interpreta entre el equipo remoto y la LAN corporativa para el acceso a los sistemas de información.

2.2 L2TP (Layer Two Tunneling Protocol)

Anteriormente se describió cada una de las características del protocolo PPTP, pero para ver como funciona L2TP es necesario hablar de L2F (Layer 2 Forwarding) este protocolo propietario de Cisco, tiene como objetivo proporcionar un mecanismo de tunneling para el transporte de tramas a nivel de enlace: PPP, HDLC (High-level Data Link Control), SLIP(Serial Line Internet Protocol), etc. Este proceso de tunneling involucra tres protocolos diferentes: el protocolo pasajero representa el protocolo de nivel superior que debe encapsularse (IP), el protocolo encapsulador indica el protocolo que será

empleado para la creación, mantenimiento y destrucción del túnel de comunicación (L2F); y el protocolo portador será el encargado de realizar el transporte de todo el conjunto (PPP).
L2TP es un protocolo usado para conectar redes privadas a través de Internet de una manera segura por medio de VPN, combinando protocolos PPTP de Microsoft y el L2F de Cisco resolviendo los problemas de interoperabilidad entre ambos protocolos, proporcionando así un mejor acceso y mayor seguridad. Este permite el túnel de nivel de enlace de PPP, de forma que los paquetes IP, IPX y AppleTalk enviados de forma privada, puedan ser transportados por Internet.

L2TP encapsula las tramas del protocolo punto a punto (PPP) que van a enviarse a través de IP, X.25, Frame Relay, o modo de transferencia asíncrona ATM (Asynchronous Transfer Mode).

Cuando esta configurado para utilizar IP como transporte, L2TP se puede utilizar como protocolo de túnel VPN en Internet. L2TP sobre IP utiliza el puerto UDP 1701 e incluye una serie de mensajes de control L2TP para el mantenimiento del túnel. L2TP, también utiliza UDP para enviar tramas PPP encapsuladas en L2TP como datos del túnel. Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparecen como paquetes IP, aprovechan la seguridad IPSec estándar mediante el modo de transporte IPSec para obtener una fuerte protección e integridad, reproducción, autenticidad y privacidad.

L2TP se diseño específicamente para conexiones cliente a servidores de acceso a redes, así como para las conexiones puerta de enlace a puerta de enlace. Mediante su utilización del protocolo PPP, L2TP gana compatibilidad multiprotocolo para protocolos como IPX y AppleTalk.

La implementación de L2TP ofrece:

- Soporte de entornos multiprotocolo L2TP que puede transportar cualquier protocolo enrutado, incluyendo IP, IPX y AppleTalk.
- Independientemente del medio este opera sobre cualquier red con capacidad de distribuir tramas IP. Soporta cualquier tecnología backbone WAN, incluyendo Frame Relay, ATM, X.25 o SONET. Soporta también medios LAN como Ethernet, Fast Ethernet, Token Ring y FDDI.

Para comprender mejor este protocolo es necesario identificar los términos de:

Access Concentrador (LAC). Es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes. También se le conoce como el servidor de acceso a la red en el protocolo Layer 2 Forwarding (L2F).

Network Server (LNS): Opera sobre cualquier plataforma con capacidad de terminación PPP. LNS gestiona el lado del servidor del protocolo L2TP.

Network Access Server (Servidor de Acceso a la red) NAS. Este dispositivo proporciona a los usuarios acceso temporal a la red bajo demanda. Este acceso es punto a punto, de uso típico en líneas de la red telefónica convencional o RDSI. En la implementación Cisco, un NAS sirve como LAC.

En un entorno de conexiones telefónicas, un túnel L2TP puede iniciarse desde un servidor de acceso de red (NAS) (como un túnel iniciado NAS) o desde software cliente (como un túnel iniciado por el cliente) hacia un router que actúa como el punto de terminación del túnel.

2.2.1 Encapsulación en L2TP

Las tramas PPP que contienen un datagrama IP se empaquetan con un encabezado L2TP y un encabezado UDP como se muestran en la figura 2.3.

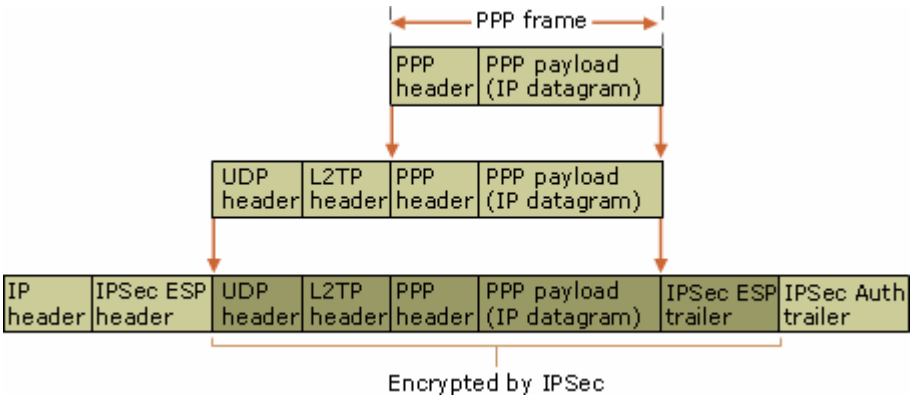

Figura 2.3 - Formato del paquete IP cifrado en L2TP y IPSec.

L2TP es una solución que ofrece una larga lista de ventajas a loas usuarios de empresa: estas ventajas incluyen:

1. Seguridad y prioridad garantizada para la mayoría de las aplicaciones esenciales de trabajo.
2. Una mejor conectividad, costes reducidos y libertad para redistribuir los recursos en núcleos de funciones.
3. Un entorno de acceso de red remota flexible y ampliable sin comprometer la seguridad corporativa o poner en peligro las aplicaciones esenciales.

2.3 IPSec

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos.

Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino.

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.*(Ver figura 2.3)*

AH sigue al header IP y contiene datos encriptados tanto en los datos como en la información de identificación. El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga. . *(Ver figura 2.3)*

Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway:

- El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.
- El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

CAPITULO 3

CONCEPTOS BÁSICOS DE OPNET

3.1 QUE ES OPNET?

OPNET (Optimized Network Engineering Tools) es una herramienta para modelado, simulación y análisis de performance de redes y protocolos de comunicaciones. Opnet fue desarrollado pro MIL3, Inc. Esta herramienta puede ser utilizada por desarrolladores para:

- Desarrollar nuevos protocolos
- Optimizar los protocolos existentes
- Estudiar la performance de diferentes topologías de redes de comunicaciones mediante la utilización de diferentes cargas de tráfico.

OPNET contienes una librería con modelos de los protocolos de comunicaciones más utilizados como son: Ethernet, TCP, UDP, IP, ATM, FDDI, Frame Relay, etc. Estos modelos incluyen todas las características de los protocolos mencionados. También contiene modelos de elementos de networking más utilizados de diferentes marcas, como: 3com. Cisco, Lucent, Hewlett Packard, etc.

OPNET IT Gurú trabaja con un concepto de cuatro pasos para el desarrollo de una simulación: (*Ver figura 3.1*)

Figura 3.1- Pasos para construir un modelo de red y analizar la simulación.

3.2 ENTORNO DE TRABAJO EN OPNET

OPNET IT GURU ofrece un sistema mediante el cual podemos emular el comportamiento de una red por completo, teniendo en cuenta que poseemos un banco de dispositivos donde encontraremos equipos tales como routers, switches, servidores, y aplicaciones en red.

Al iniciar OPNET IT GURU Edición Académica nos encontraremos con la pantalla que nos muestra la ***Figura 3.2***

Figura 3.2 – Pantalla de Inicio para OPNET IT GURÚ ACADEMIC EDITION.

Este editor contiene tres tipos básicos de objetos: subredes, nodos y enlaces. Las paletas (accesibles mediante el icono en la parte superior izquierda del editor) ordenan los objetos disponibles por categorías. *Ver Figura 3.3*

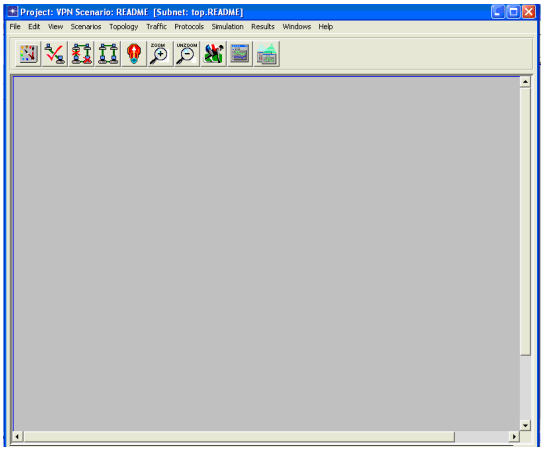

Figura 3.3 – Área de trabajo del editor.

Botones de Herramientas: Las opciones más habituales del menú pueden ser activadas por medio de estos botones. Ver *Figura 3.4*

Figura 3.4– Barra de Herramientas.

- Paleta de objetos
- Consistencia de un enlace.
- Objetos que no han sido seleccionados.
- Recuperar objetos seleccionados.
- Volver a subred anterior.
- Zoom.
- Reestablecer.
- Configurar evento discreto en simulación.
- Ver resultados de simulación.
- Esconder o ver los gráficos.

3.2.1 Proyectos y Escenarios

Cuando deseemos cargar algún proyecto existente en la librería debemos seleccionar el modelo deseado de la lista de proyectos y posteriormente analizar cada uno de los escenarios.

Un proyecto tiene un grupo de escenarios relacionados, los cuales examinan diferentes aspectos de la red, en este orden de ideas, un proyecto puede tener uno o varios escenarios.

Un escenario es un conjunto de objetos que forman parte de la topología de nuestro modelo de red.

Después de elegido el proyecto y el escenario podremos empezar con el proceso de edición de valores de nuestro proyecto.

Teniendo en cuenta el esquema de trabajo propuesto en la ***figura 3.1***, procedemos a enumerar los pasos a seguir para iniciar con nuestro objetivo, la creación de una red privada virtual (VPN).

3.2.2 Herramientas.

3.2.1.1 *Node editor*

Este editor es usado para crear modelos de nodos especificando su estructura interna. Estos modelos son usados para crear nodos en el interior de la red en el Project editor.

Internamente, los modelos de nodos tienen una estructura modular, al ser definido como un nodo como una conexión que permite intercambiar información y paquetes entre ellos. Cada modulo tiene una función especifica dentro de un nodo, tal como: generar paquetes, encolarlos, procesarlos o transmitirlos y recibirlos.

3.2.1.2 *Process Model Editor*

Se utiliza en la creación de modelos de procesos que a su vez controlan los modos de nodo creados por el Node Editor los Process Model son

representados por estados (FSM) y son creados por iconos que presentan estados y líneas que presentan transiciones entre ellos.

3.2.1.3 ***Link Model Editor:*** ofrece la posibilidad de crear nuevos tipos de objetos link. Cada nuevo tipo de link puede tener diferentes atributos y representaciones.

3.2.1.4 ***Path Editor:*** Es usado para crear nuevos objetos path (patrón) que sirven para definir un traffic route.

3.3 ANALIZANDO EL MODELO DE RED

Para examinar un modelo de red que se encuentre dentro de la librería estándar de OPNET IT GURU Edición Académica debemos tener claro antes que todo el tipo de red al cual queremos analizar, ya que el software nos ofrece una amplia gama de topologías para soluciones de comunicaciones distintas.

En nuestro caso, entraremos al análisis de la topología de red VPN, a continuación los pasos para efectuar la práctica:

3.3.1 PASOS PARA EJECUTAR UN MODELO DE RED.

ARRANCAR EL PROYECTO DE VPN EN OPNET IT GURU EDICIÓN ACADÉMICA:

1. Selecciona Inicio, luego Programas, a continuación OPNET IT GURU ACADEMIC EDITION 9.1.

Figura 3.5 – Modo de acceso a la topología VPN en OPNET.

2. Posteriormente aparecerá la ventana de inicio del software, seleccionas ***File*** en el menú, seguidamente pinchas en ***Open***, y por ultimo te ubicas en el proyecto ***VPN*** y lo escoges, tal como se muestra en la ***figura 3.5***

3. Al escoger el proyecto, *(Ver figura 3.6)* nos ubicamos en el escenario inicial del proyecto, el cual nos muestra información básica de la topología de red a analizar dividida en varios segmentos que analizaremos detalladamente, este primer escenario es básicamente una introducción teórica a las practicas que se realizaran más adelante.

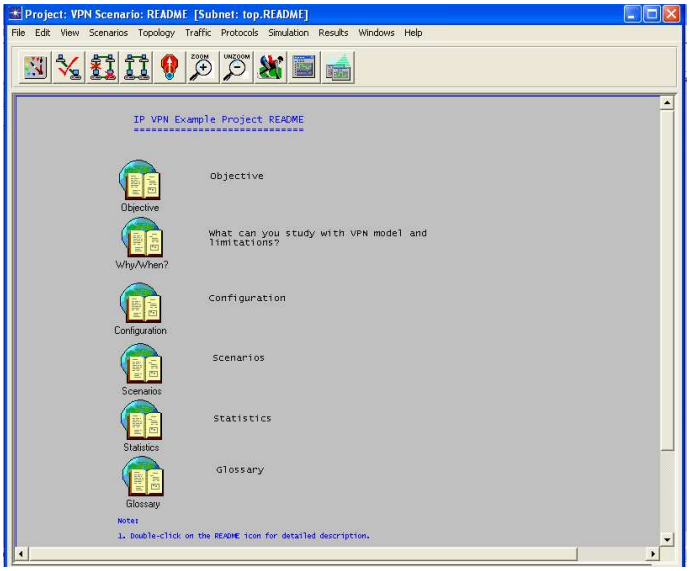

Figura 3.6- Pantalla inicial de el escenario 1 de el proyecto VPN

En pantalla se muestran una serie de opciones a escoger, donde se muestra información detallada de cada una de las funciones que se pueden implementar con este proyecto.

CAPITULO 4

ESCENARIOS VPN.

CAPITULO 4

ESCENARIOS VPN.

Este capitulo prioriza en utilizar el simulador de red previamente mencionado (Opnet IT GURU Academic Edition) para que con sus diversas herramientas se puedan diseñar modelos, simular datos y analizar las redes y asi comprender de manera eficiente los diversos conceptos de las tecnologías de redes privadas virtuales en distintos escenarios: Sin túnel vpn, túnel voluntario y túnel obligatorio.

Sin túnel VPN: Sin túnel vpn, este es un escenario de referencia, sin túnel vpn está configurado y sirve como guía básica para los escenarios 3 y 6.

Túnel voluntario: Este escenario nos muestra el modo de operación voluntaria del túnel.

Túnel obligatorio: Este escenario nos muestra el modo obligatorio del tunelamiento.

4.1 ESCENARIO: SIN TUNEL VPN

En este escenario se muestra un esquema de conexión sin túnel VPN entre un cliente y un servidor remoto. *(Ver Figura 4.1.1)*

El conducto regular por el cual se realiza la conexión es a través del servidor de acceso (L2TP Access Server , señalado en la *figura 4.1.1)* de allí sale mediante un enlace PPP (Ver *Figura 4.1.2),* este servidor es una puerta de enlace hacia Internet, en este punto se revisa la solicitud para posteriormente ser ruteada.

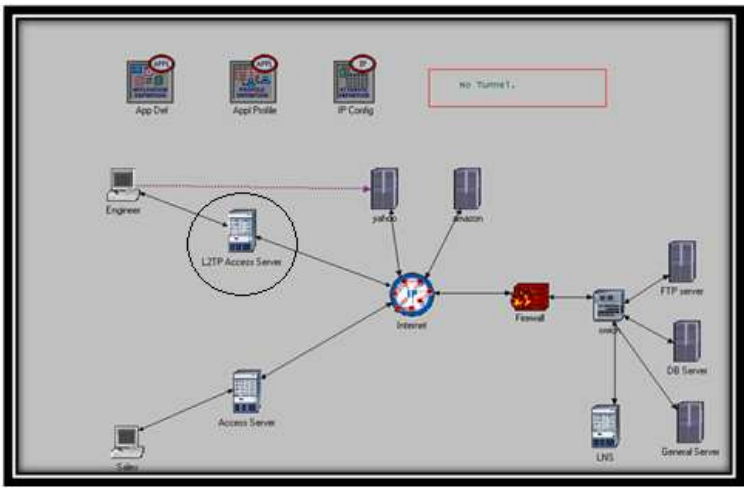

Figura 4.1.1 – Esquema de conexión utilizado para la topología sin túnel vpn.

4.1.1 CONFIGURACIÓN DE PARÁMETROS

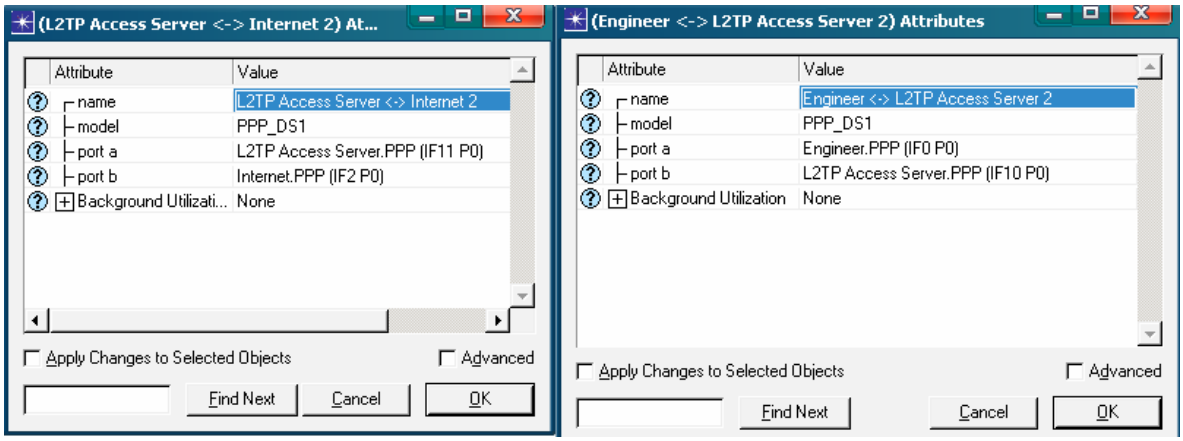

Figura 4.1.2 **–** Configuración de enlaces desde el usuario final hasta la nube de internet.

Del Gateway sale un enlace PPP hacia la nube de Internet, que a su vez ubica la dirección del destinatario, en este caso el Server (Yahoo), reubicando el paquete para que sea recibido por el dispositivo. El servidor se encuentra configurado para que la mayoría de las aplicaciones se encuentren bajo el protocolo TCP como se puede observar en la ***Figura 4.1.3***

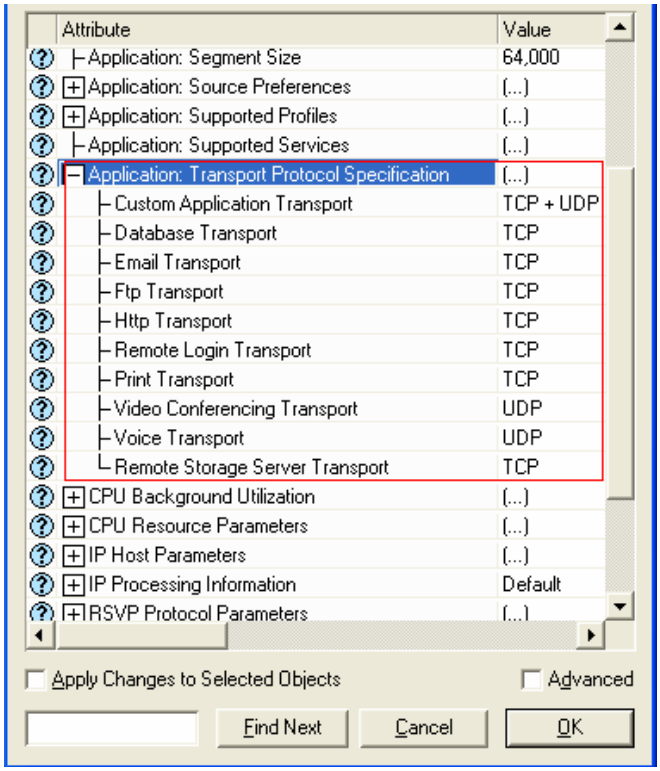

Figura 4.1.3 – Protocolos sobre los cuales corren las aplicaciones a montar en red.

A hora definiremos las aplicaciones que deberán correr sobre la topología de red implementada, para ello nos dirigimos al objeto Aplication definition, posteriormente hacemos clic derecho y escogemos la opción Edit Preferences.

Para este escenario se crearon 16 aplicaciones las cuales se definirán a continuación. (*Ver Figura 4.1.4)*

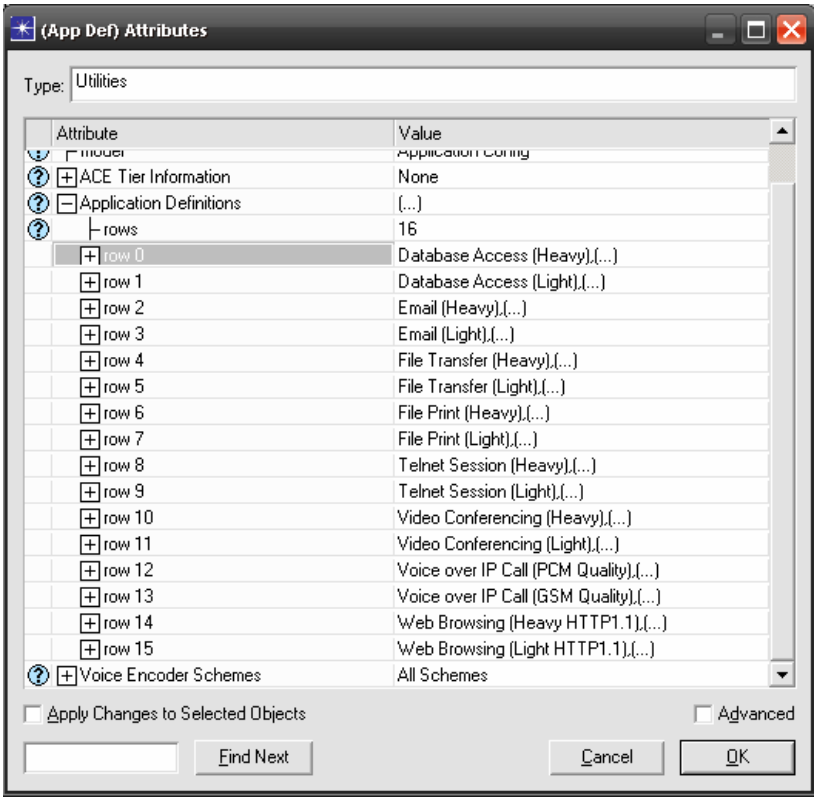

Figura 4.1.4- Aplicaciones a definir para la topología de red sin túnel vpn.

4.1.2 CONFIGURACIÓN DE APLICACIONES

Cada perfil tiene configuraciones comunes para todos los escenarios por lo tanto no se hace necesario repetir la información ya que las aplicaciones se encuentran definidas de la misma forma para todas las topologias de vpn.

Las aplicaciones comunes se encuentran deshabilitadas para los ítems Database Access(Heavy) y Database Access(Light) por lo tanto no se hará detalle en estas.

La fila 2 (row 2) correspondiente a la aplicación de email con trafico pesado (Email- Heavy) se configura de acuerdo a la ***figura 4.1.5.***

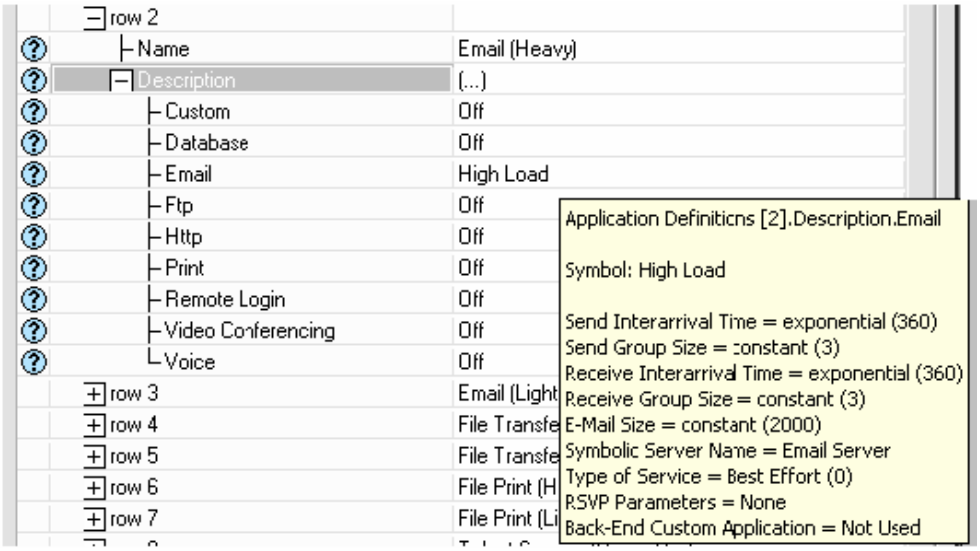

Figura 4.1.5 - Configuración de la aplicación de email con trafico pesado.

La aplicación de email se configura con la preferencia de carga alta (High Load) lo que agrega una condición de mayor trafico a la red.

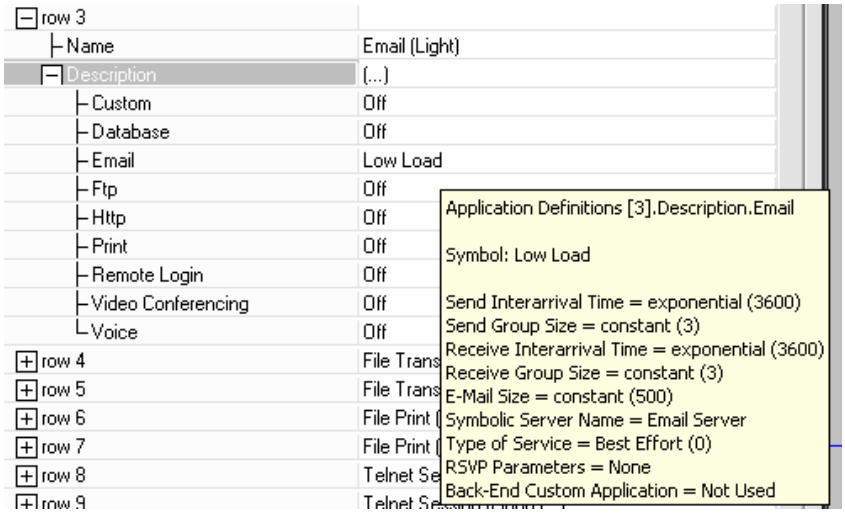

Figura 4.1.6 - Configuración de la aplicación de email con trafico ligero.

Para las aplicaciones de FTP se configuran las opciones de acuerdo como se plantean en las Figuras 4.1.7 y 4.1.8.

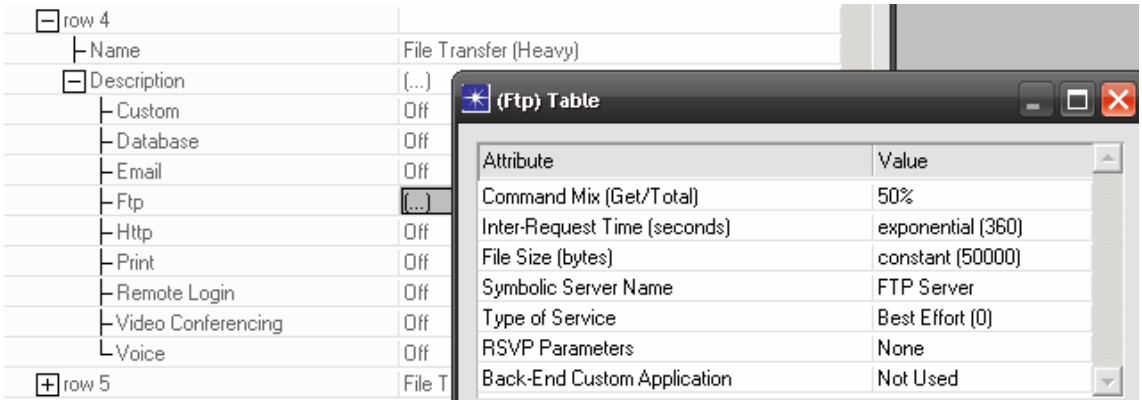

Figura 4.1.7- Configuración de la aplicación de File Transfer (Heavy)

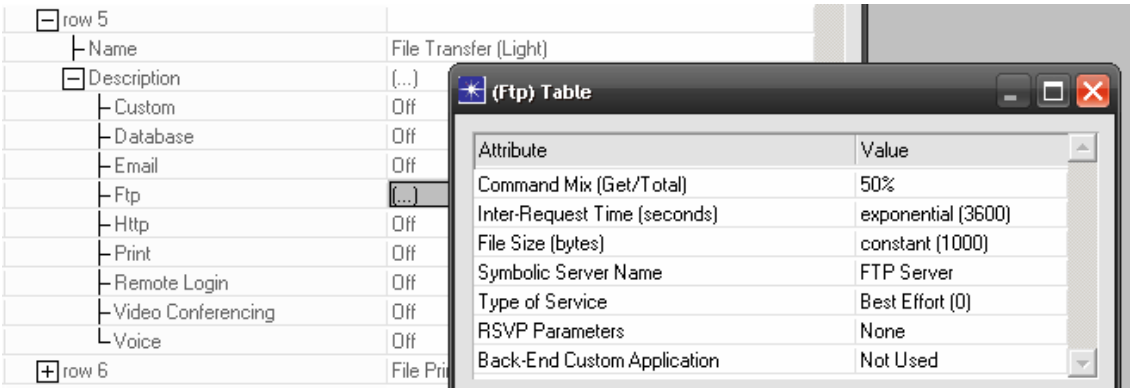

Figura 4.1.8 - Configuración de la aplicación de File Transfer (Light)

Ahora configuraremos la aplicación de impresión, la cual permitirá iniciar trabajos de impresión en red. Los parámetros se ilustran en las figura 4.1.9 para configuraciones de tráfico diferentes.

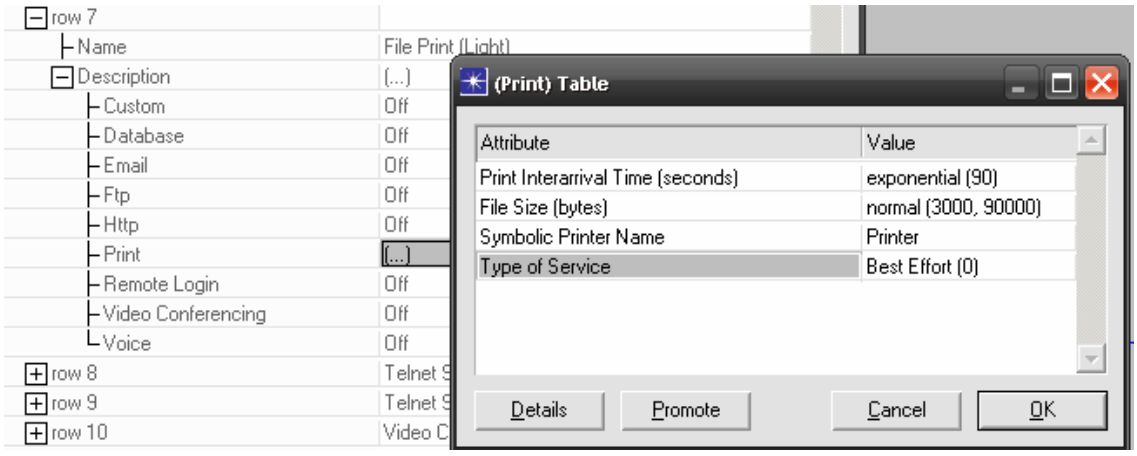

Figura 4.1.9- Configuración de la aplicación de File Transfer (Light)

A continuación se asignaran parámetros para la aplicación de Telnet en tráfico pesado y ligero. Los parámetros configurados se ilustran en las figuras 4.1.10 y 4.1.11. Posteriormente se definen los parámetros de video conferencia.(*Ver figuras 4.1.12 y 4.1.13)*

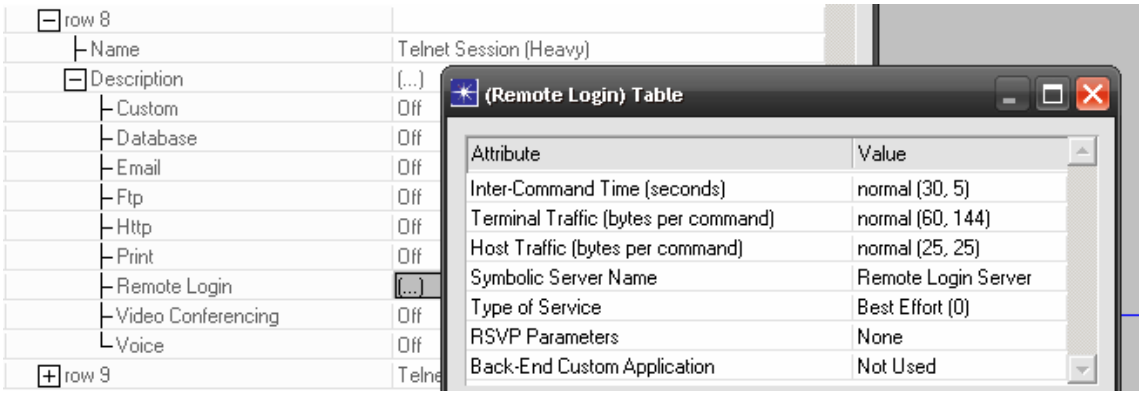

Figura 4.1.10- Configuración de la aplicación de Telnet Session (Heavy)

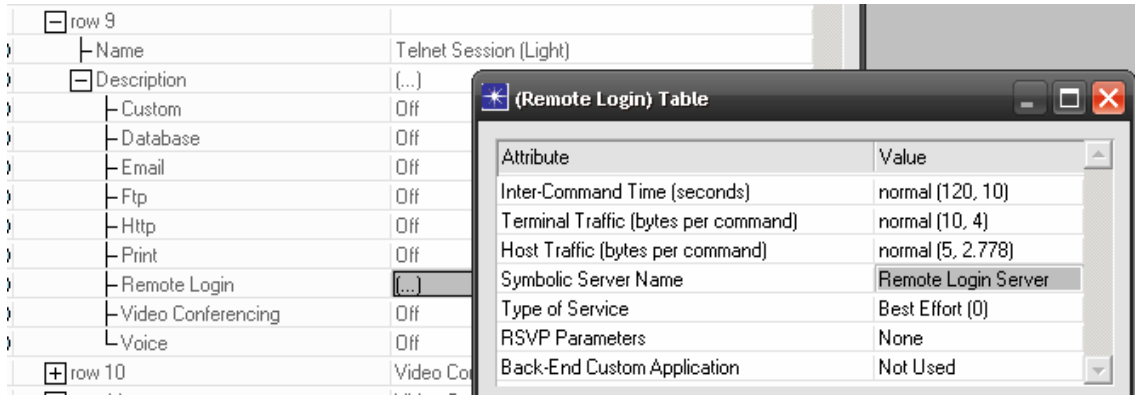

Figura 4.1.11 - Configuración de la aplicación de Telnet Session (Light)

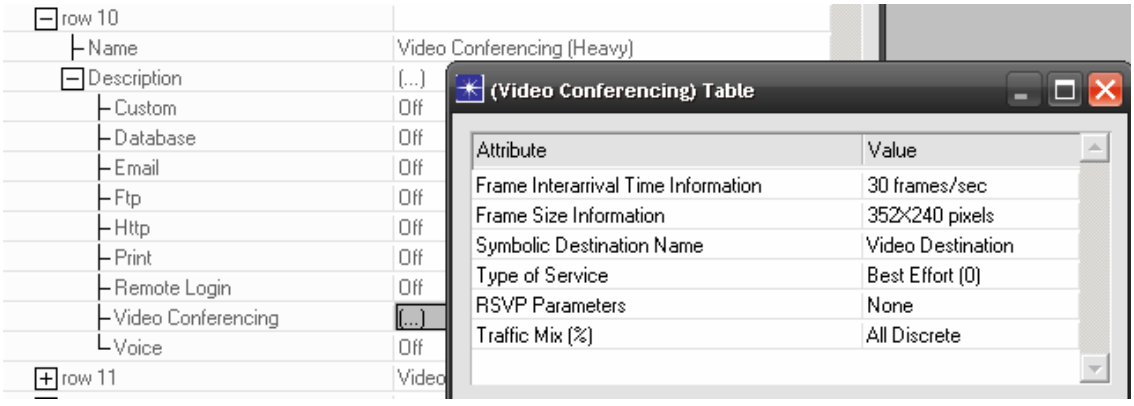

Figura 4.1.12- Configuración de la aplicación de Video Conferencia (Heavy)

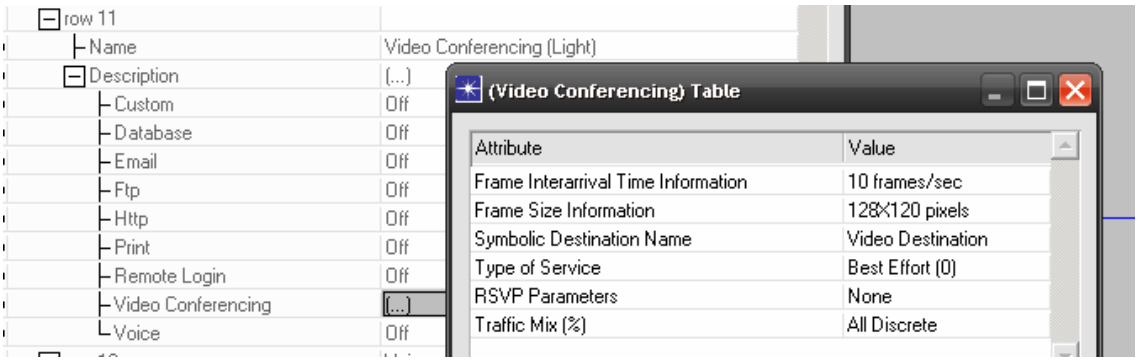

Figura 4.1.13- Configuración de la aplicación de Video Conferencia (Light)

Seguidamente se definirán los parámetros para la aplicación de Voz sobre IP para distintos tipos de calidad de esta (*Ver figuras 4.1.14 y 4.1.15*).

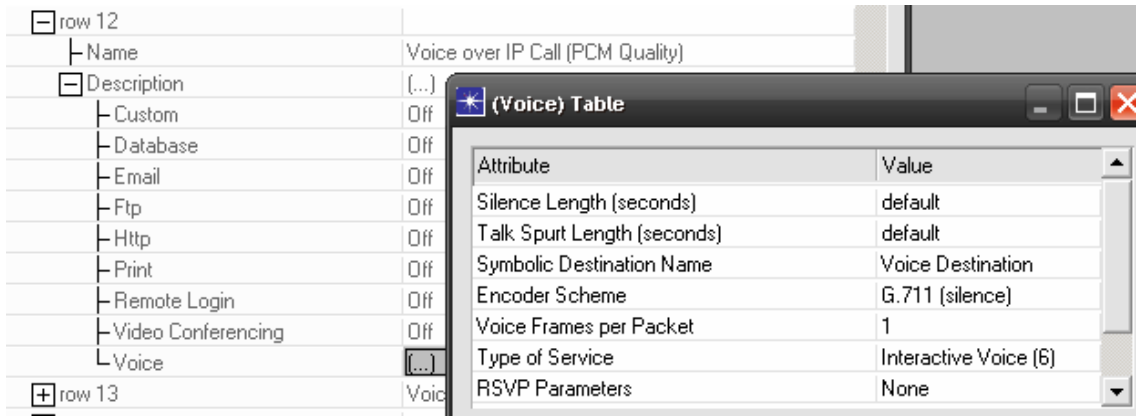

Figura 4.1.14- Configuración de la aplicación de Voice over IP(PCM Quality)

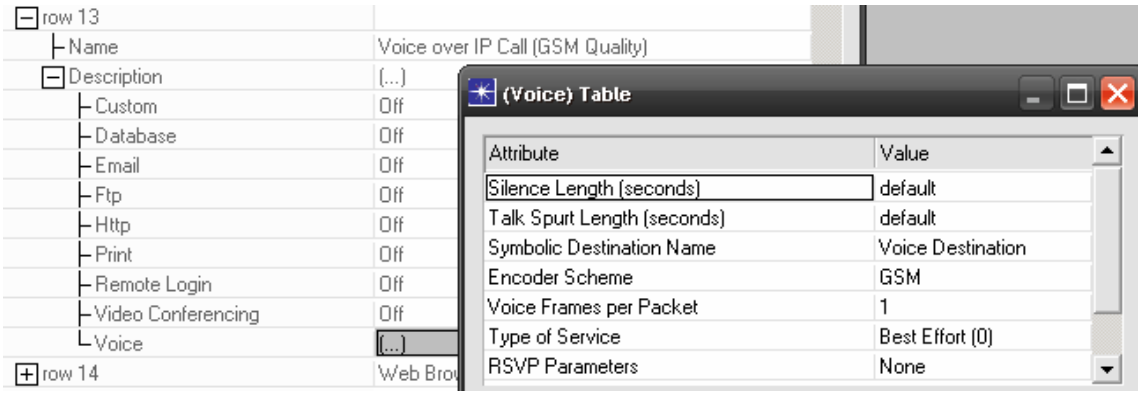

Figura 4.1.15 - Configuración de la aplicación de Voice over IP(GSM Quality)

Seguidamente configuraremos la aplicación de navegación en la web para distintas instancias de tráfico, los parámetros establecidos se ilustran en las figuras 4.1.16 y 4.1.17.

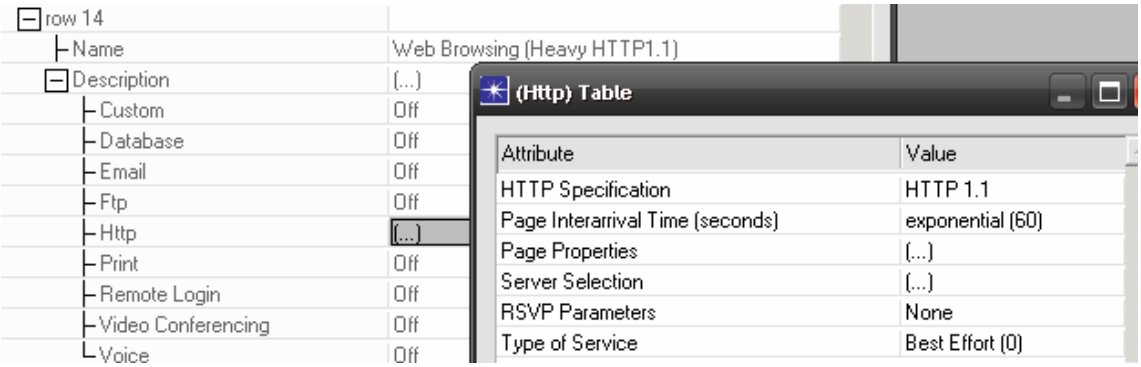

Figura 4.1.16 - Configuración de la aplicación de Web Browsing (Heavy)

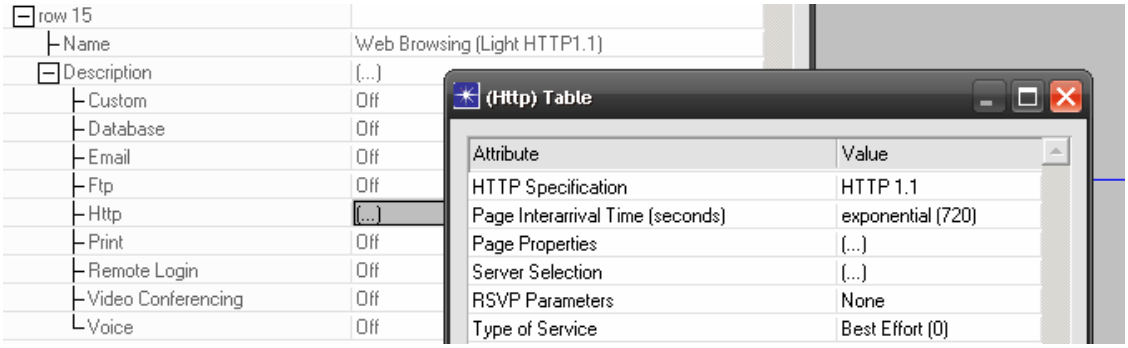

Figura 4.1.17 - Configuración de la aplicación de Web Browsing (light).

4.1.2.1 CONFIGURACION DE PERFILES

Después de definir las aplicaciones a utilizar con los distintas condiciones de trafico de red, procedemos a definir los perfiles de los usuarios, para esto hacemos clic derecho en el objeto Appl Profile, posteriormente escogemos la opción Edit Preferences del menú desplegable. *Ver Figura 4.1.18.*

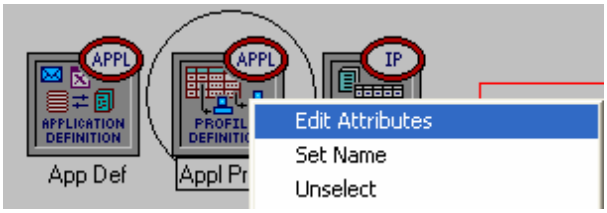

Figura 4.1.18- Configurando las aplicaciones para cada uno de los perfiles en modo sin túnel.

Teniendo en cuenta que los usuarios que manejamos en esta topología de red (Engineer y Sales Person) configuraremos los perfiles para cada uno de ellos.

Para el usuario Engineer se configuran los parámetros de acuerdo con la figura 4.1.19.

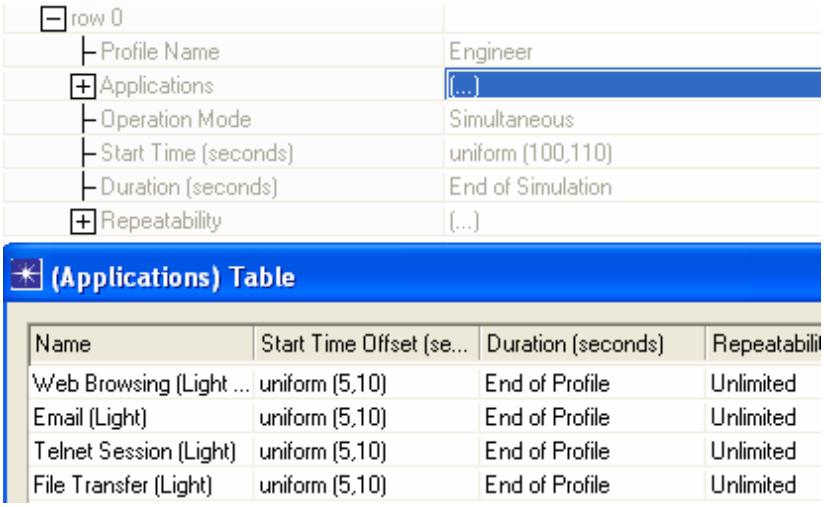

Figura 4.1.19- Configurando las aplicaciones para el perfil Engineer

Ahora configuraremos el perfil Sales Person, los parámetros se encuentran definidos en la *figura 4.1.20.*

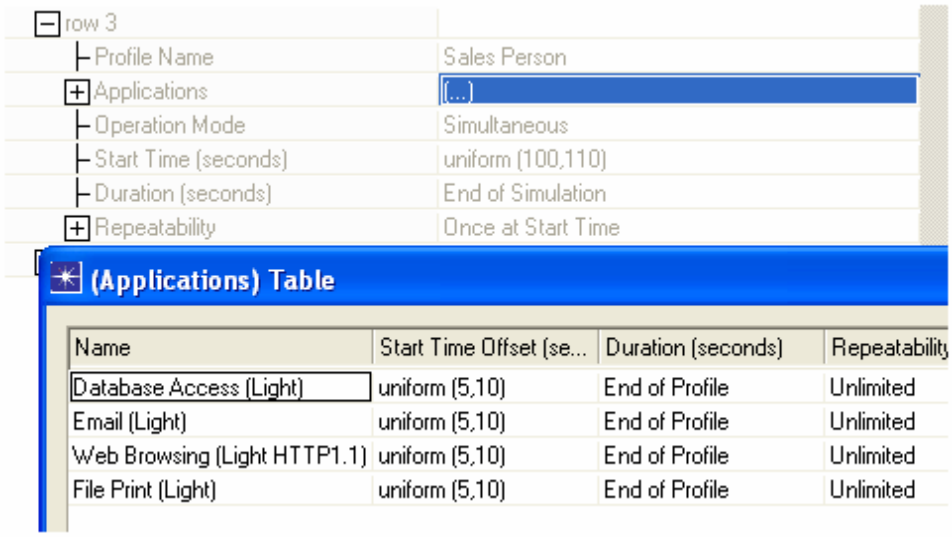

Figura 4.1.20 - Configurando las aplicaciones para el perfil Sales.

Para definir los parámetros de solicitudes de ping a otros host nos vamos al objeto IP config, le damos clic derecho y escogemos la opción Edit Attributes en el menu desplegable.

En la opción IP Ping Parameters configuramos los ítems de acuerdo con los rangos mostrados en la Figura 4.1.21.

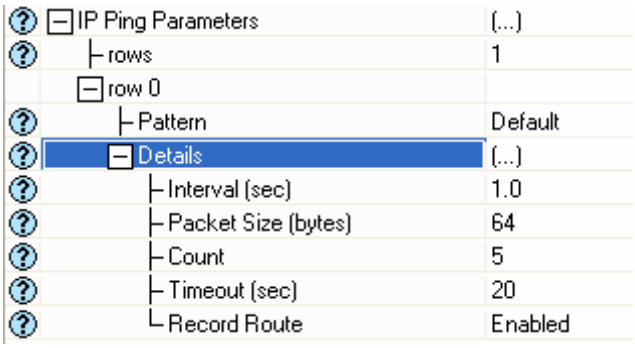

Figura 4.1.21- Parámetros modificados para la solicitud de ping.

Este parámetro es común para todos los perfiles por lo tanto no es necesario especificar para cuales usuarios se aplicaran los cambios.

4.1.2.2- DEFINICION DE APLICACIONES SOPORTADAS POR LOS SERVIDORES.

Para la optimización de recursos de la red se ha decidido implementar las aplicaciones en diferentes servidores y de esta manera segmentar el trafico que pasa por la red y evitar la saturación de estos equipos como consecuencia de las múltiples aplicaciones que tendrán que ejecutar.

Las aplicaciones para este escenario fueron dividas en tres partes: las aplicaciones FTP (transferencia de archivos) se ubican en el servidor FTP, las de bases de datos en el servidor DB, y las aplicaciones de email, impresión de archivos y sesiones Telnet son ubicadas en el servidor general. Las figuras 4.1.22, 4.1.23 y 4.1.24 muestran las aplicaciones que corren cada uno de los servidores mencionados.

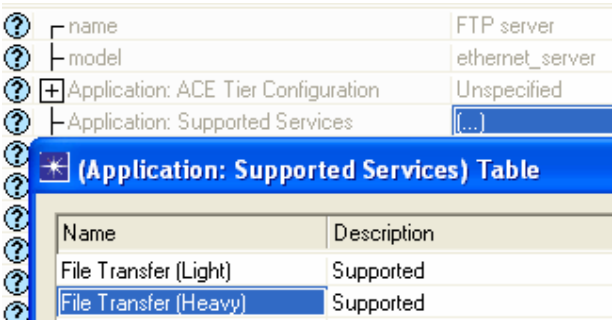

Figura 4.1.22: Aplicaciones soportadas por el FTP server.

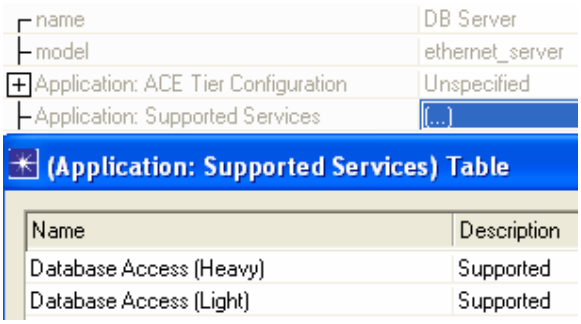

Figura 4.1.23: Aplicaciones soportadas por el DB server.

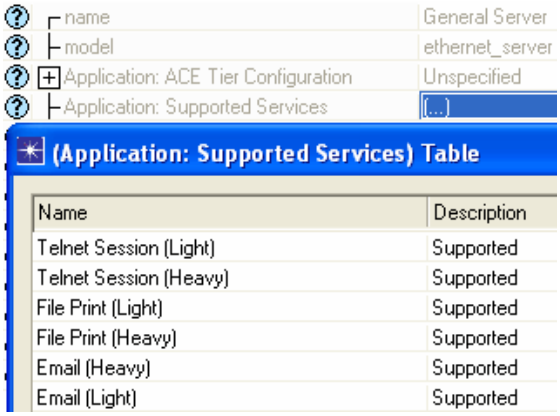

Figura 4.1.24: Aplicaciones soportadas por el General server.

Para los servidores Yahoo y Amazon se definirán parámetros de aplicaciones que pueden correr, teniendo en cuenta que no necesariamente todas las aplicaciones definidas son utilizadas en este escenario. Estas aplicaciones son descritas en las figuras 4.1.25 y 4.1.26

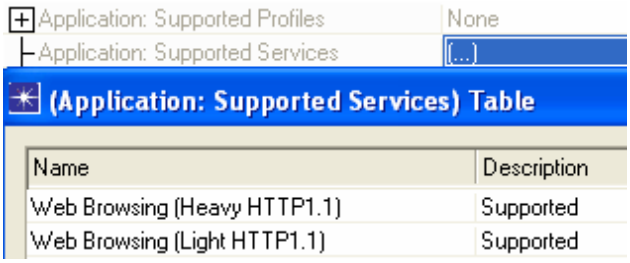

Figura 4.1.25- Aplicaciones que utiliza el server Yahoo.

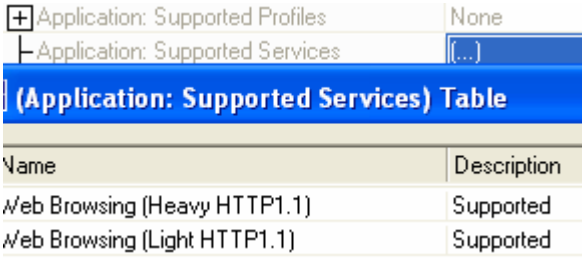

Figura 4.1.26: Aplicaciones que utiliza el server Amazon.

4.2.1.3 - Configuración de Firewall

Teniendo en cuenta que se quiere filtrar el uso de aplicaciones y obtener mayor seguridad en la red se implemento un firewall, que regulara el uso de todas las aplicaciones definidas con anterioridad, la configuración de este objeto se muestra a continuación. Ver Figura 4.1.27.

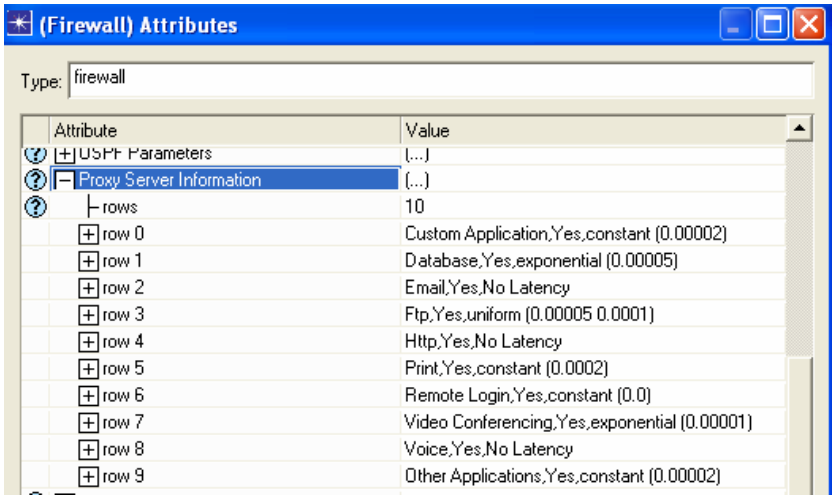

Figura 4.1.27: Aplicaciones que acepta el firewall.

Los filtros realizados por el firewall pueden ser modificados para cada una de las aplicaciones definidas, para admitir o denegar una aplicación en el firewall modificamos el parámetro Proxy Server Deployed en cada una de las aplicaciones. *Ver figura 4.1.28*

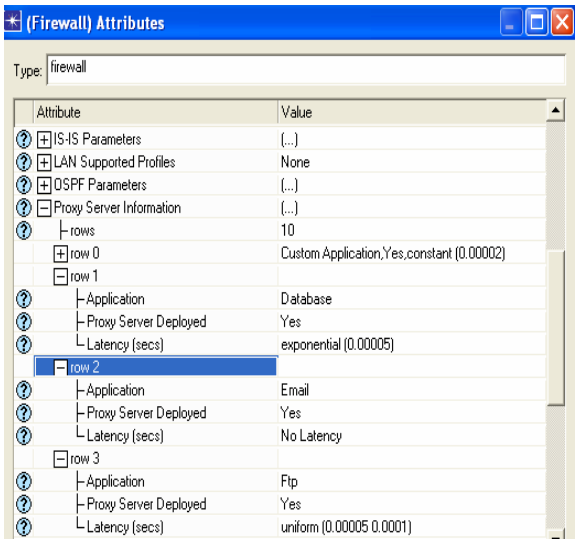

Figura 4.1.28: Configuración del Firewall.

4.1.3 VISUALIZACION DE RESULTADOS

Con base al plan de trabajo propuesto en la ***figura 3.1***, nos ubicamos en la barra de menú y seleccionamos la opción ***Simulation***, luego en el desplegable hacemos click en ***Choose Individual Statistics***, expandimos el árbol ***Node Statistics*** y realizamos el mismo procedimiento con el árbol de ***IP***, de allí escogemos las opciones a analizar posteriormente. *Ver Figura 4.1.29*

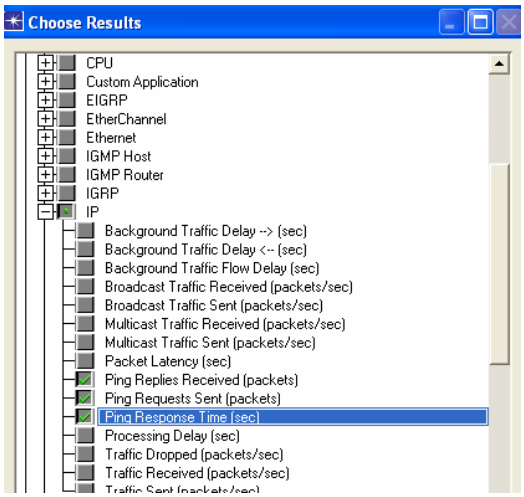

Figura 4.1.29 – Parámetros seleccionados a partir del modelo de trabajo propuesto en la figura 3.1.

Para configurar la simulación se establecerá un criterio de duración de la prueba estándar (1 hora) en el cual se analizara detalladamente el modelo de red. Ver *Figura 4.1.30.*

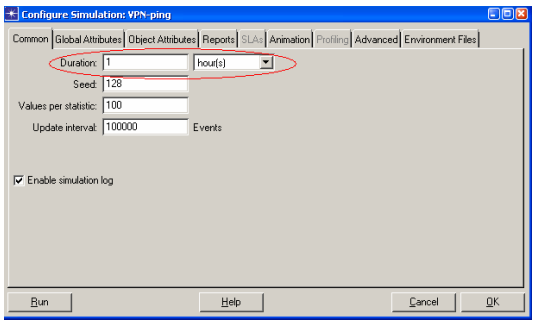

Figura 4.1.30 – Configuración establecida para la simulación del escenario sin tunel.

El objetivo del ping en esta topología es verificar el correcto envío de paquetes, es decir que todos los paquetes lleguen a su destino.

A continuación podemos observar la respuesta a la solicitud de ping hecha desde los clientes con los que se está trabajando. Ver figuras *4.1.31 y 4.1.32.*

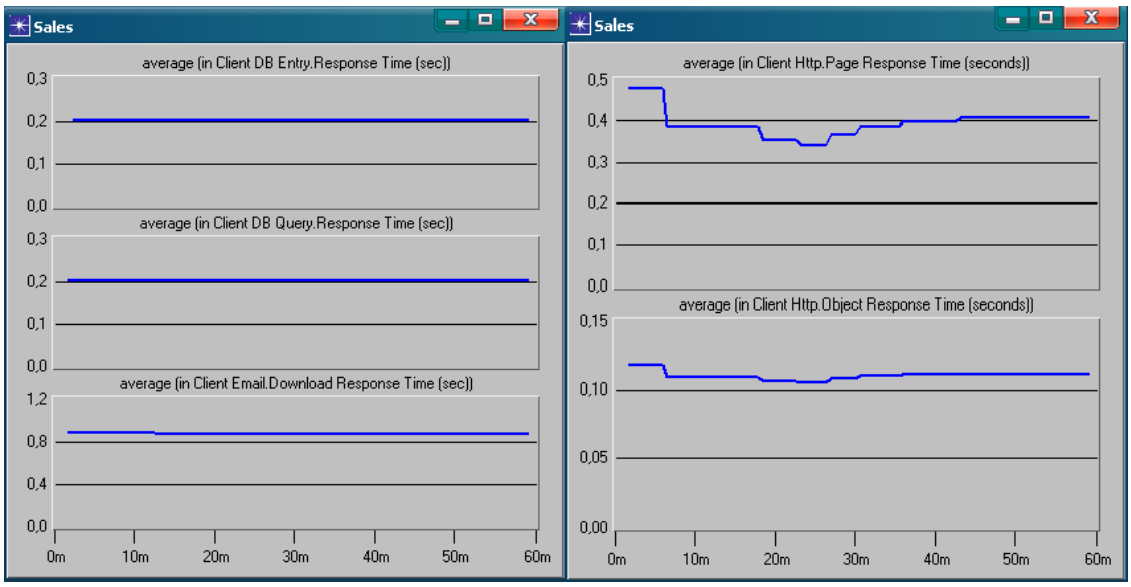

Figura 4.1.31– Solicitud de ping realizada desde el usuario Sales Person a las distintas aplicaciones que corren en los servidores con un tráfico ligero.

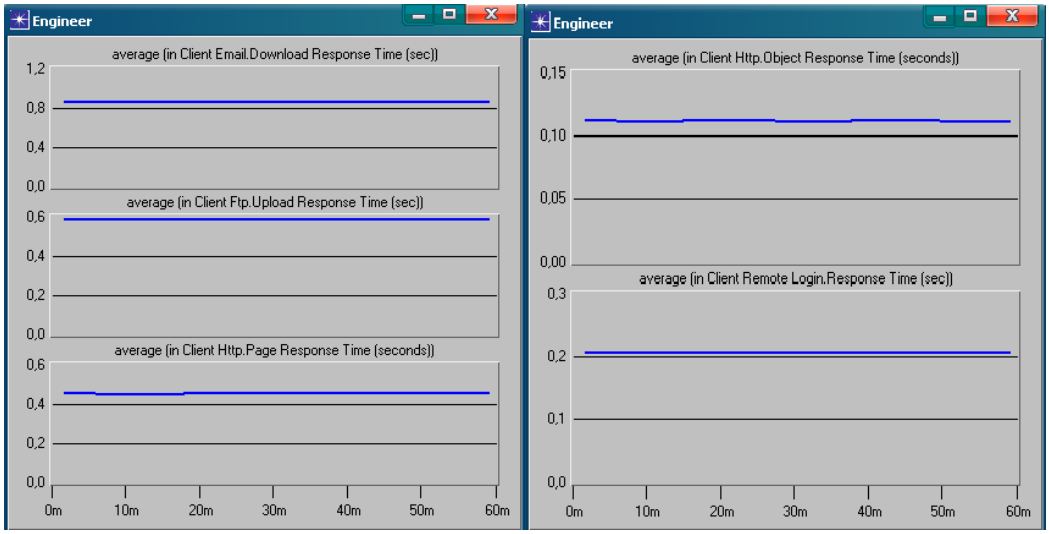

Figura 4.1.32– Solicitud de ping realizada desde el usuario Engineer a las distintas aplicaciones que corren en los servidores con un tráfico ligero.

Como podemos observar los tiempos de respuesta son relativamente bajos para todas las aplicaciones que se están corriendo, esto debido a que el número de equipos con los cuales se está trabajando es reducido (routers switches, etc) lo cual es una ventaja a la hora de reducir tiempos de espera a solicitudes de ping.

A continuación se mostraran los resultados obtenidos para los distintos niveles de tráfico en la red.

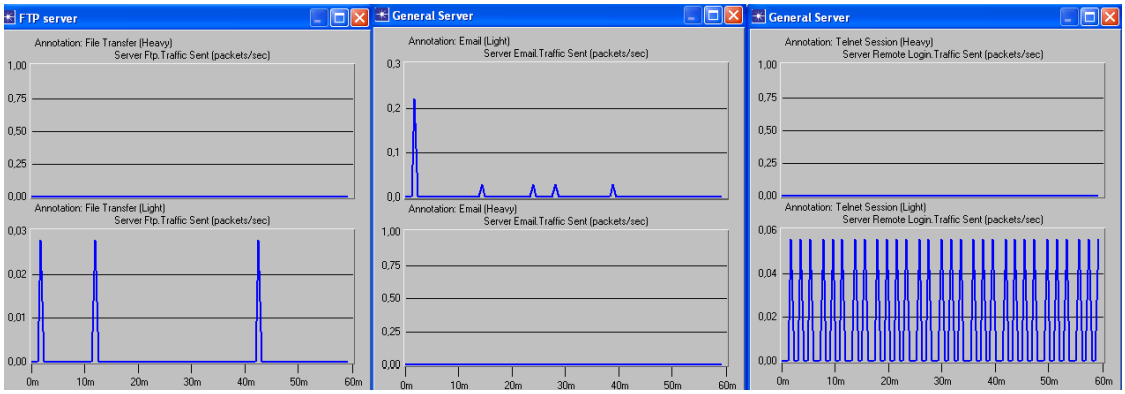

Figura 4.1.33 **–** Trafico enviado para las distintas aplicaciones que están en la red.

En la *figura 4.1.33* se puede evaluar cómo afecta la utilización del ancho de banda a las aplicaciones que se corren en una red ya que en la medida en que el tráfico aumenta los paquetes tardaran mucho más en realizar el recorrido habitual para llegar a su destino.

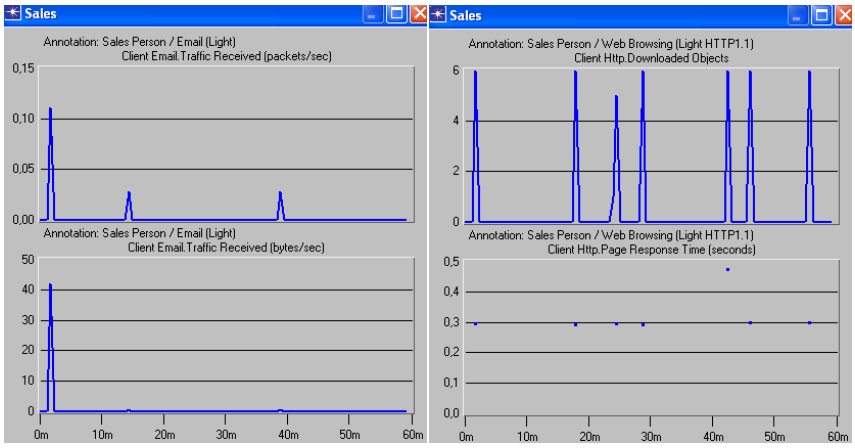

Figura 4.1.34 **–** Trafico recibido para en el usuario Sales para aplicaciones de email y Web Browsing.

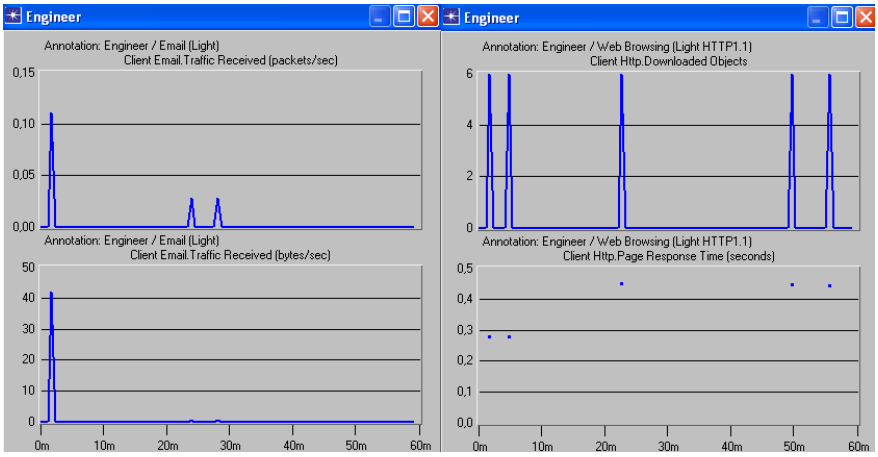

Figura 4.1.35 **–** Trafico recibido para en el usuario Engineer para aplicaciones de email y Web Browsing.

Como se puede apreciar en la *figuras 4.1.34* y 4.1.35 el trafico es muy bajo lo que indica que la aplicación de email está corriendo de manera optima, por otra parte al observar los tiempos de respuesta a la aplicación de navegación web se aprecia que están alrededor de 400mSeg lo cual es un tiempo considerablemente aceptable para acceder a una página web.

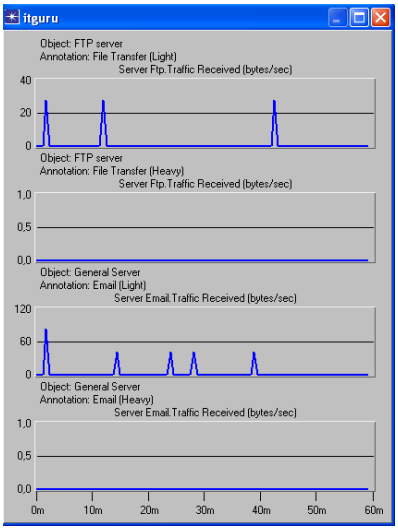

Figura 4.1.36 **–** Trafico recibido para los servidores FTP y General.

De la *Figura 4.1.36* podemos tasar que el tráfico proveniente de las aplicaciones de correo electrónico predomina sobre las de transferencia de archivos ya que el tráfico promedio de la aplicación de correo es mayor que la de ftp.

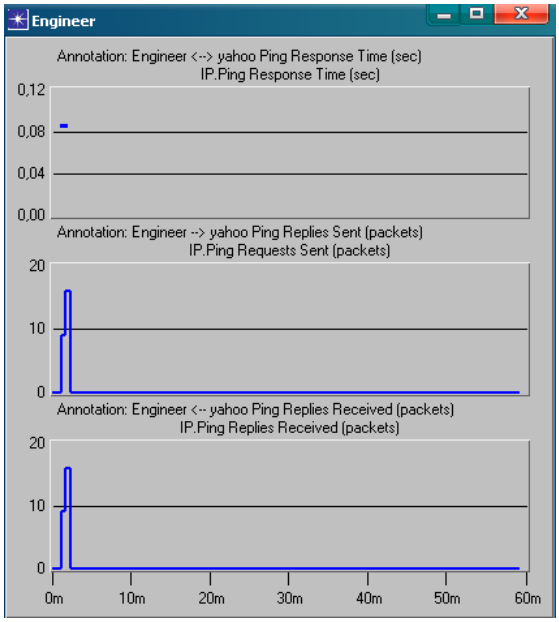

Figura 4.1.37 **–** Tiempos de respuesta a solicitud de ping desde cliente Engineer para configuración sin túnel VPN.

La figura 4.1.37 nos muestra tiempos de respuesta a solicitud de ping hecha desde el cliente Engineer para un modo de operación sin túnel VPN, los tiempos de respuesta son inferiores a 10ms, óptimos para una solicitud de ping realizada a un servidor en otra red. Esta solicitud será utilizada para posteriores comparaciones en los escenarios de tunelamiento voluntario y obligatorio

En este escenario se realizó una configuración de red sin túnel VPN, lo anterior nos ubica en una topología de una red con conexiones físicas, por lo tanto los tiempos de respuesta observados en la figuras 4.1.31 y 4.1.32 variarán con respecto a los distintos modos de entunelamiento. En su gran mayoría se observan tiempos de respuesta aceptables para una navegación optima (tiempos de respuesta inferior a un segundo) esto debido a que no se están manejando protocolos de encapsulación y cifrado de datos, que en la mayoría de los casos provocan retardos como producto de los procesos de encriptación y compresión a los que son sometidos durante el establecimiento del túnel.

Las aplicaciones que se corren con tráfico pesado consumen mayor ancho de banda por lo tanto afecta directamente al resto de las aplicaciones que se estén corriendo en la red implementada, lo cual genera retardo en los tiempos de envío y recepción de paquetes en los usuarios.

4.2 ESCENARIO: TUNEL VOLUNTARIO

A continuación se muestra un escenario de túnel voluntario, topología es mostrada en la ***Figura 4.2.1.***

Un túnel voluntario ocurre cuando, una estación de trabajo o un servidor de entunelamiento utiliza el software del cliente del túnel, a fin de crear una conexión virtual al servidor del túnel objetivo; para lograr esto se debe instalar el protocolo apropiado de túnel en la computadora cliente.

Para una PC conectada a una LAN, el cliente ya tiene una conexión a la red que le puede proporcionar un entubamiento a las cargas útiles encapsuladas al servidor del túnel LAN elegido. Este sería el caso para un cliente en una LAN corporativa, que inicia, un túnel para alcanzar una subred privada u oculta en la misma LAN.

Cada petición de tunelamiento será analizada y creada de una forma independiente, de esta forma existirá un túnel por cada petición que se haga por parte de cada cliente y es este quien comienza y termina la sesión del mismo. En este tipo de túneles las políticas de seguridad son implementadas directamente en los hosts debido a que son los puntos finales de la conexión virtual.

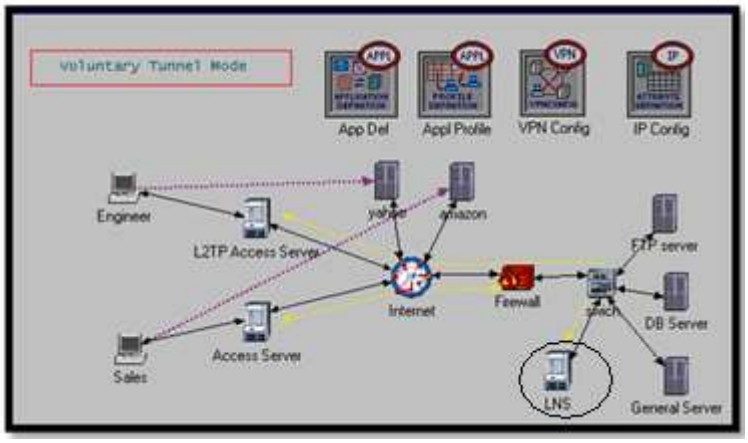

Figura 4.2.1– Túnel VPN en modo Voluntario.

En la figura se muestra un modo de tunelamiento voluntario, en donde la sucursal remota establece un túnel directamente con el servidor de red L2TP (LNS) de la red de empresa. La funcionalidad del concentrador de acceso L2TP (LAC) reside en el cliente. El túnel es transparente para el suministrador de servicios de Internet (ISP) del cliente, o sea que ya no se necesita el ISP para soportar L2TP.

En esta topología de red, el túnel es creado por el usuario, normalmente por el uso de un cliente habilitado para L2TP que se llama cliente LAC. El usuario podrá enviar paquetes L2TP para el proveedor de servicios de Internet (ISP) que se remitirá a la LNS.

En este tipo de túneles el ISP no necesita el apoyo L2TP, que sólo remite los paquetes L2TP entre LAC y LNS. El cliente actúa como un túnel L2TP iniciador que de hecho reside en el mismo sistema que el cliente remoto. El túnel se extiende por todo el período de sesiones PPP desde el cliente L2TP al LNS.

4.2.1 CONFIGURACION DE PARAMETROS.

La definición de aplicaciones y de perfiles son comunes al escenario Sin Túnel VPN por lo tanto, estos parámetros no se configuran nuevamente.

Por otra parte, teniendo en cuenta que se trabajará con un túnel vpn en *modo voluntario* se deben adicionar nuevas características a los parámetros ya establecidos con el fin de indicar la ruta a seguir en la conexión virtual.

Para configurar un túnel VPN en modo voluntario nos dirigimos hacia el objeto VPN Config, seleccionamos clic derecho y escogemos la opción *Edit Preferences* en el menú desplegable.

Expandiendo el árbol de configuración tenemos la siguiente figura, (Ver ***Figura 4.2.2),*** en donde podemos apreciar los dos tipos de túneles utilizados, en este caso los dos son voluntarios, el ítem (desde el Access Server hasta el Firewall), y el segundo paso (comenzando en L2TP Acces Server y termina en el LNS)

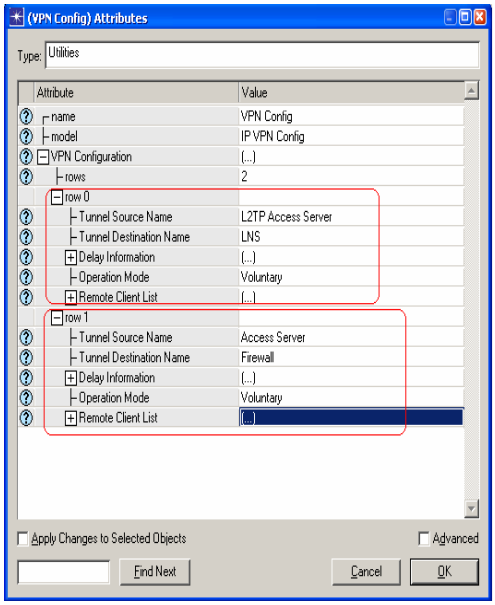

Figura 4.2.2– Configuración de túneles en modo voluntario.

Para escoger el tipo de túnel a utilizar expandimos la opción ***Operation mode*** en cada uno de los túneles a implementar, de esta manera cambiamos el modo de operación a ***voluntary.***

4.2.2 CONFIGURACION DE APLICACIONES

Las aplicaciones para este escenario son comunes con las del escenario sin túnel VPN y fueron descritas en el escenario sin túnel vpn.

4.2.3 VISUALIZACION DE RESULTADOS

Acorde con las premisas aclaradas en la ***figura 3.1***, procedemos a escoger las estadísticas que pretendemos mostrar.

Elegimos en el menú de inicio ***Simulation***, luego en la opción ***Choose Individual Statistics***, en el desplegable ***Global Results*** seleccionamos la opción ***VPN*** y habilitamos todas las opciones que se muestran(*IP y VPN*), a continuación le damos ***OK***.

Para visualizar los resultados obtenidos de la simulación seleccionamos ***Results*** en la barra de menú, luego la opción ***View Results*** del menú desplegable.

Para el análisis de resultados en el modo de túnel voluntario se hace una comparación de este con una conexión sin vpn esto con el fin de escatimar las el potencial de esta topología de red.

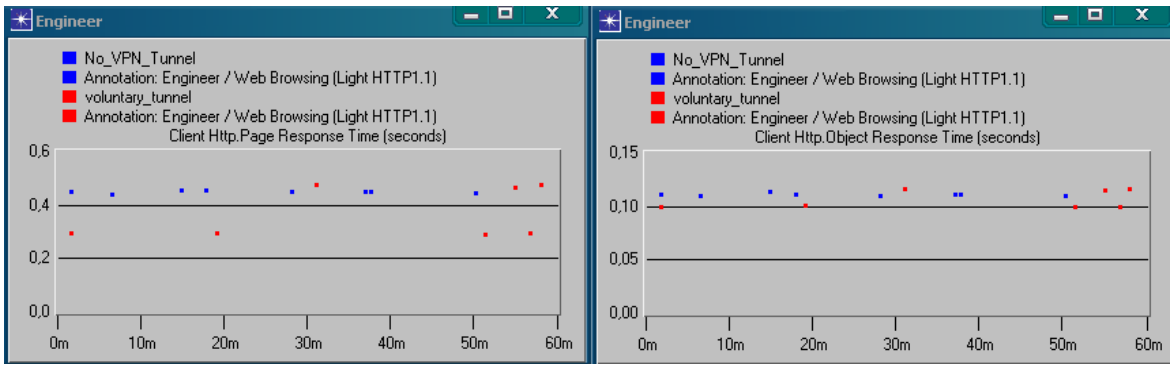

Figura 4.2.3– Comparación de aplicaciones para el cliente Engineer.

La figura 4.2.3 muestra una comparación entre tiempos de respuesta para el cliente Engineer, testeados en los modos de operación sin túnel y voluntario, donde se puede apreciar una mayor latencia en los tiempos ofrecidos en el modo de tunelamiento voluntario.

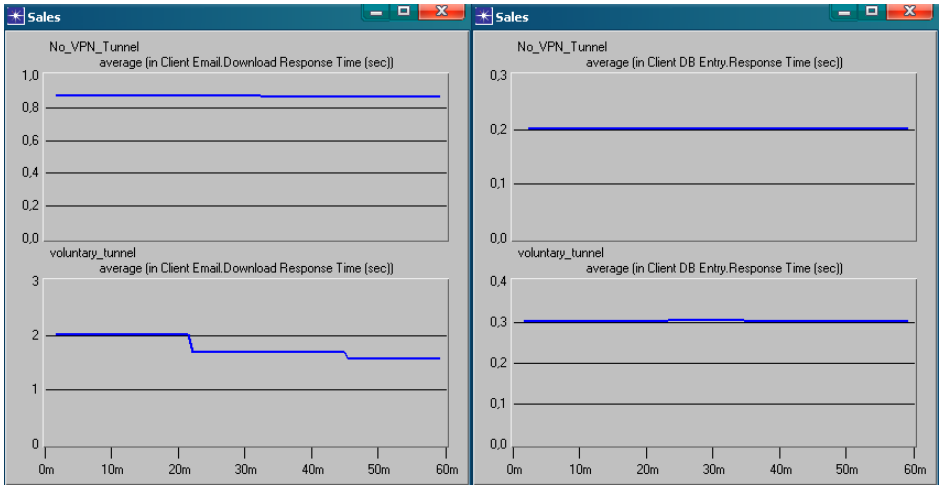

Figura 4.2.4– Comparación de aplicaciones para el cliente Sales.

Realizando la misma comparación para el cliente Sales (Ver Figura 4.2.4) se evidencia el mismo comportamiento, lo cual nos indica que la creación de túneles genera un mayor consumo de recursos de la red adicionando así retardos a las conexiones producto de los distintas formas de encapsulación y encriptación de paquetes.

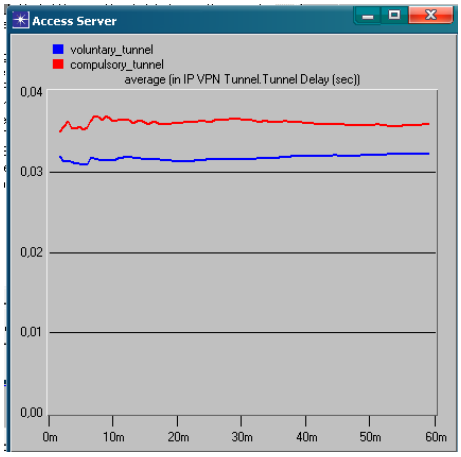

Figura 4.2.5– Retardo de túnel VPN para la operación en modo voluntario y obligatorio.

En la figura 4.2.5 se muestra el retardo provocado por el túnel para una conexión en modo voluntario, este retardo es un aspecto importante a tener en cuenta al momento de la implementación de un túnel ya esta vinculado directamente con el tiempo de recepción de paquetes al destinatario del túnel, para aplicaciones de voz puede llegar a generar inconvenientes.

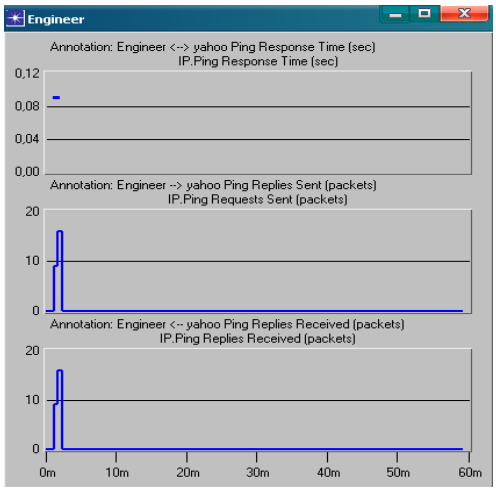

Figura 4.2.6– Tiempos de respuesta para túnel operando en modo voluntario desde cliente Engineer.

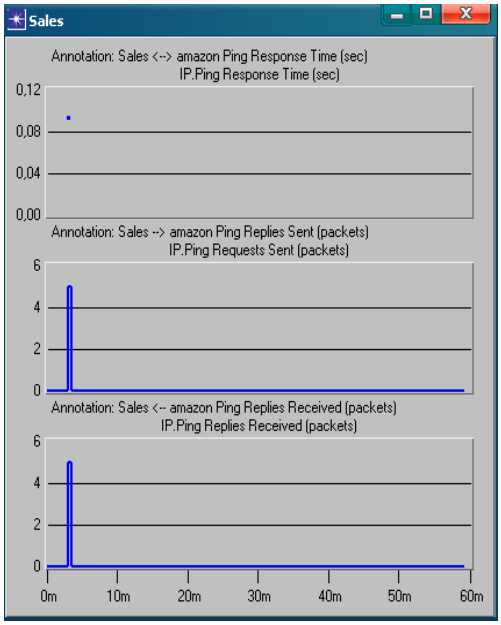

Figura 4.2.7– Tiempos de respuesta para túnel operando en modo voluntario desde cliente Sales.

Durante el envio de paquetes en el túnel existen otros factores que afectan los tiempos de respuesta de recepción de los mismos tales como el retardo de procesamiento IP y la latencia de paquetes de la red publica. Ver figuras 4.2.8, 4.2.9 y 4.2.10.

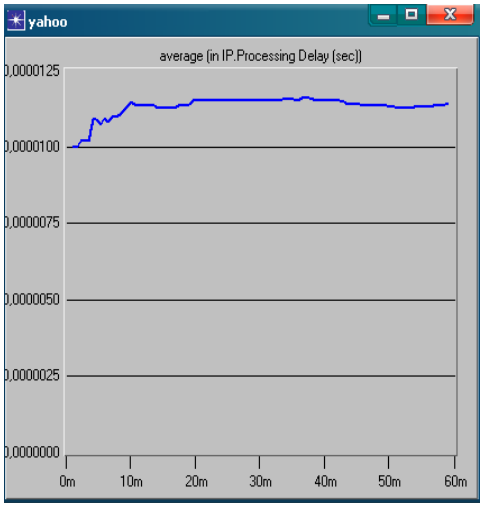

Figura 4.2.8– Retardo de procesamiento IP en el server Yahoo.

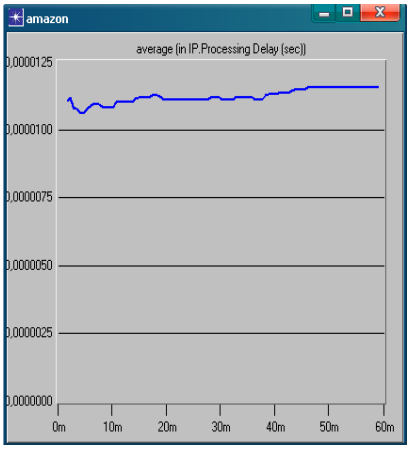

Figura 4.2.9– Retardo de procesamiento IP en el server Amazon.

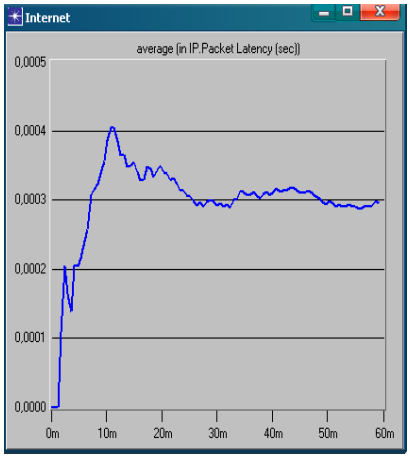

Figura 4.2.10– Latencia de Paquetes en Internet.

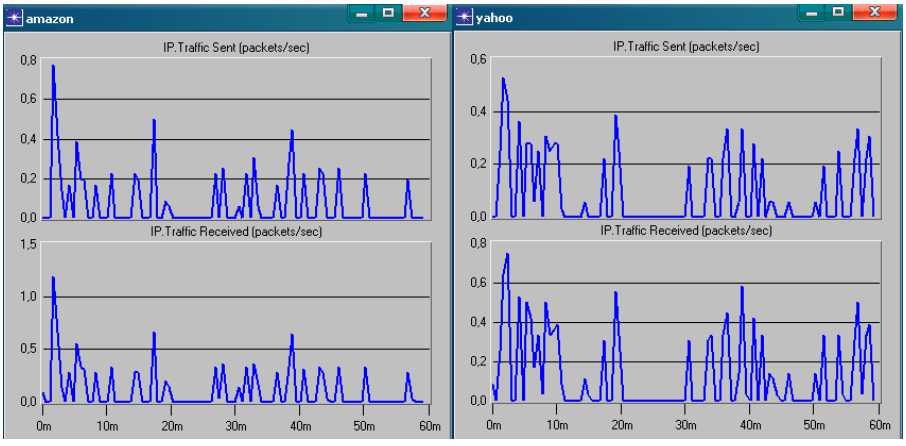

Figura 4.2.11–Trafico enviado y recibido para los dos servidores.

El trafico IP correspondiente a las aplicaciones montadas en los servidores Amazon y Yahoo (Ver figura 4.2.11) nos muestra que la navegación en el

servidor Yahoo es levemente mayor que para el de Amazon, teniendo en cuenta el trafico recibido y enviado desde y hacia la red.

Comparando las graficas *4.1.37 y 4.2.6* podemos observar como los tiempos de respuesta para las solicitudes de ping realizadas desde los clientes están dentro del rango deseado, aún después de implementado el túnel vpn siguen dentro de rango (inferiores a 10ms) y no hay pérdidas de paquetes durante las trayectorias de las topologías enunciadas.
En la *figura 4.2.3* podemos observar las variaciones de tiempo de respuesta la aplicación de Web Browsing (Navegación Web), que se manejan en el enlace para el cliente Engineer, la cual nos muestra que el modo de operación de un túnel voluntario reduce tiempos de respuesta para navegación en paginas web con respecto a la operación sin túnel (0.3 segundos), pero los objetos contenidos en las pagina cargan en el mismo periodo de tiempo para las dos configuraciones.

La aplicación de correo electrónico (*Ver figura 4.2.4*) posee menor tiempo de respuesta a la petición de descarga de correo electrónico (0,9 Seg) con respecto a la operación en modo voluntario (1.6 Seg.) aproximadamente. Por otra parte para la aplicación de acceso a la base de datos, la topología sin túnel VPN presenta menores tiempos de respuesta que implementando túnel voluntario reduciendo el tiempo de respuesta en 0.1 segundos.

Los tiempos de respuesta ante las diferentes aplicaciones pueden variar de acuerdo a factores tales como saturación de la red, latencia en paquetes IP a través de la nube de internet (Ver figura 4.2.10), retardo de procesamiento IP en los clientes (*Ver Figura 4.2.8 y 4.2.9*), retardo en el túnel implementado, en este caso, voluntario, que aunque sea un valor mínimo(0.035 seg *Ver figura 4.2.5)*, puede llegar a ser molesto en la medida en que se corran varias aplicaciones que adicionen tiempo de espera a solicitudes, por tanto es de vital importancia tener en cuenta cuales de estas aplicaciones son mas necesarias al implementar la red y de esta manera darle prioridad.

4.3 ESCENARIO: TUNEL OBLIGATORIO

El siguiente escenario nos muestra un túnel obligatorio, cuya topología es mostrada en la ***4.3.1.***

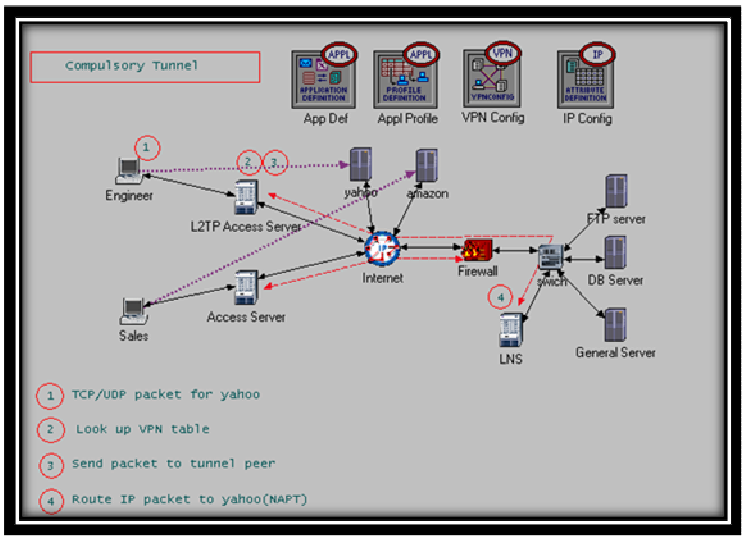

Figura 4.3.1 – Diseño de red para el modo de túnel obligatorio.

De la topología anterior nos ponemos dar cuenta que contamos con la misma infraestructura de equipos en comparación con el modo voluntario, los cambios serán a nivel de configuración interna de equipos para hallar el equivalente a cada una de las redes a implementar.

En el modelo de túnel obligatorio, ambos hosts usan dispositivos VPNs situados en la frontera de la red corporativa para negociar y conceder servicios de seguridad. De esta manera, las funciones de seguridad no necesitan ser implementadas en los hosts finales donde los datos son generados y recibidos. La implementación de los servicios de seguridad es completamente transparente para los hosts. Esta implementación reduce drásticamente la complejidad en el manejo de las políticas de seguridad.

A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel obligatorio puede estar compartido entre varios clientes. Cuando un segundo cliente marca al servidor de acceso a fin de alcanzar un destino no

hay necesidad de crear una nueva instancia del túnel entre el servidor de acceso y el servidor del túnel.

4.3.1 CONFIGURACION DE PARAMETROS

OPNET IT GURU ACADEMIC EDITION nos brinda la opción de trabajar simulando esta topología, para acceder a ella seleccionamos la opción escenarios en la barra de menú, posteriormente escogemos la opción ***Switch to escenario,*** seguidamente elegimos ***Compulsory_Tunnel.***

Posteriormente se analizará la configuración de la vpn teniendo en cuenta cual es el parámetro a utilizar para cada una de los dos túneles. Para configurar las conexiones existentes en cada uno de los túneles le damos clic derecho al icono ***VPN Config***, seguidamente seleccionamos ***Edit Attributes***.

Expandiendo el árbol de configuración *(Ver Figura 4.3.2)***,** podemos apreciar los dos tipos de túneles utilizados, en esta etapa se trabajará con ambos túneles obligatorios, la primera ruta (desde el Access Server hasta el Firewall), y la segunda (comenzando en L2TP Acces Server y termina en el LNS)

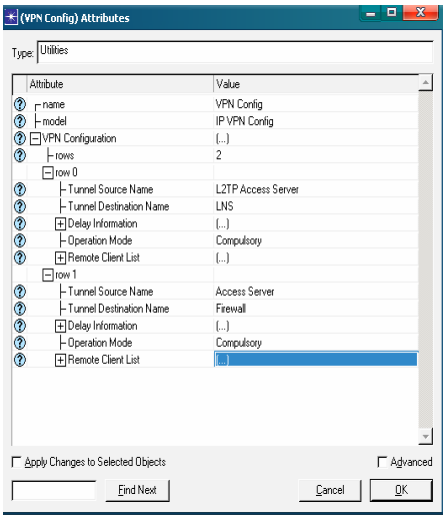

Figura 4.3.2 – Configuración de túnel VPN en modo Obligatorio.

4.3.2 CONFIGURACION DE APLICACIONES

Las aplicaciones para este escenario son comunes con las del escenario sin túnel VPN y fueron descritas en el escenario sin túnel vpn.

4.4.3 VISUALIZACION DE RESULTADOS

Acorde con las premisas aclaradas en la ***figura 3.1***, procedemos a escoger las estadísticas que pretendemos mostrar.

Elegimos en el menú de inicio ***Simulation***, luego en la opción ***Choose Individual Statistics***, en el desplegable ***Global Results*** seleccionamos la opción ***VPN*** y habilitamos todas las opciones que se muestran(VPN delay, VPN load y VPN throughput), a continuación le damos ***OK***.

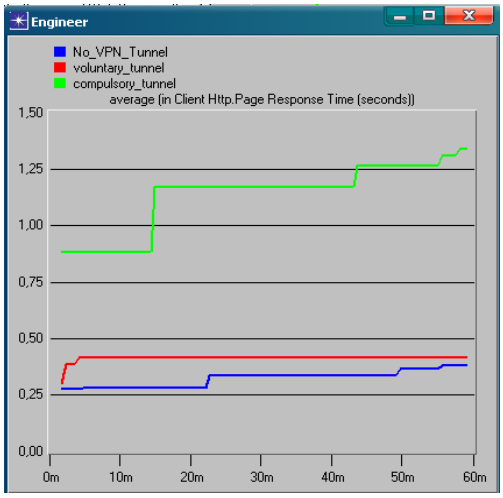

Figura 4.3.3 – Comparación de tiempo de respuesta de pagina entre tres escenarios para cliente Engineer.

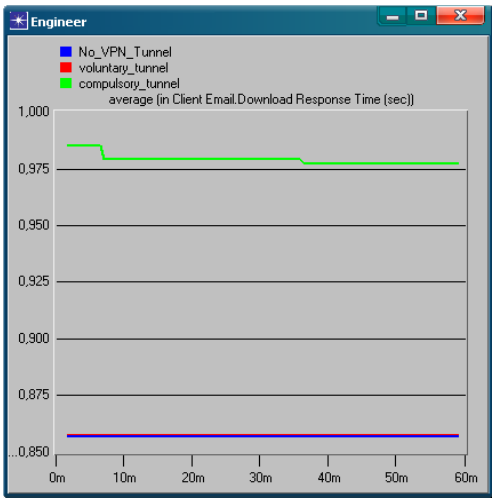

Figura 4.3.4– Comparación de tiempo de respuesta de descarga de Email entre tres escenarios para cliente Engineer.

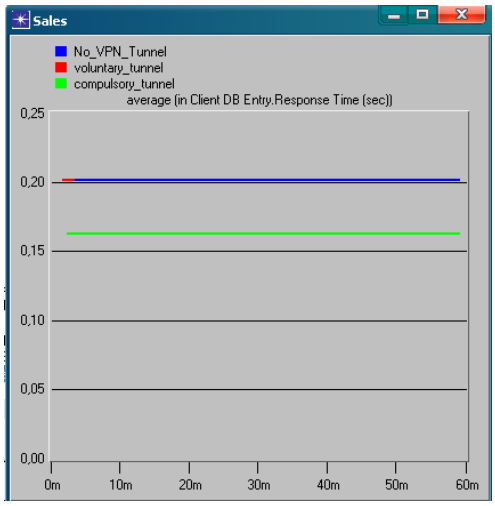

Figura 4.3.5– Comparación de tiempo de respuesta de entrada a base de datos entre tres escenarios para cliente Sales.

Las comparaciones observadas en las figuras 4.3.3, 4.3.4 y 4.3.5 nos indican que para el modo de tunelamiento obligatorio se presentan mas retardos en los tiempos de descarga de archivos ya que los usuarios que están accediendo al túnel consumen una mayor cantidad de recurso en cuanto a ancho de banda lo cual contribuye al incremento del trafico y como consecuencia directa el retardo de paquetes.

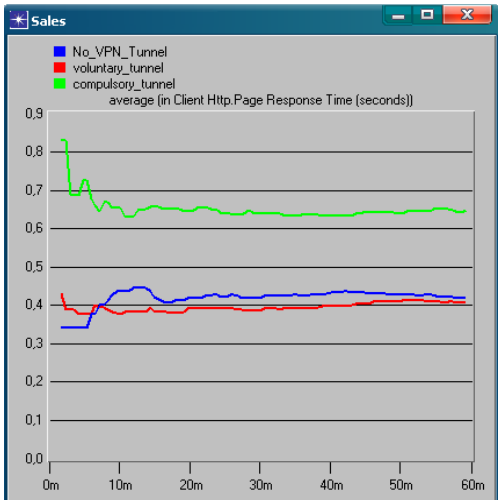

Figura 4.3.6– Comparación de tiempo de respuesta de pagina entre tres escenarios para cliente Sales.

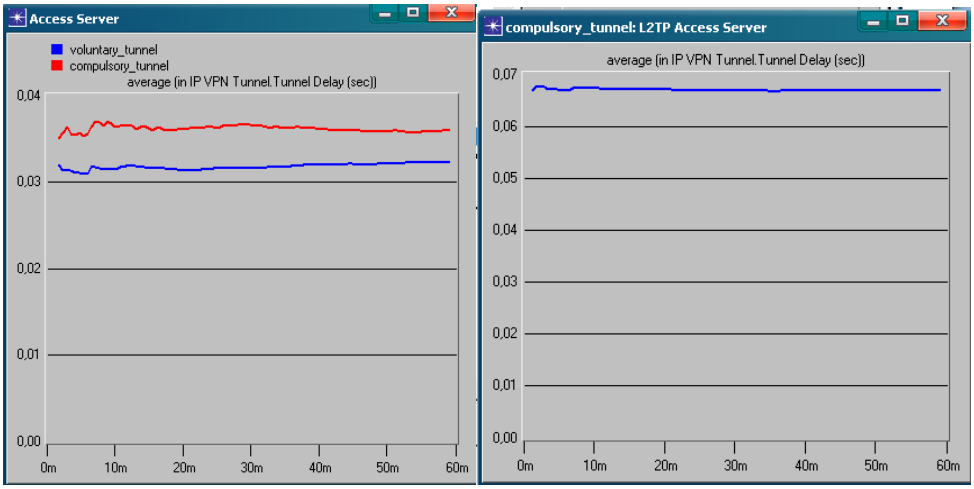

Figura 4.3.7– Retardo de túnel VPN desde Access Server para la operación en modo obligatorio y voluntario.

La figura 4.3.7 nos muestra el retardo en túneles para los puntos terminales de las conexiones, como podemos apreciar en el modo de operación voluntaria no se toma como punto de referencia el servidor de acceso L2TP ya que el cliente es quien es quien empieza y culmina la sesión, por tanto no se establece una comparación en este punto de la red para los dos modos de tunelamiento.

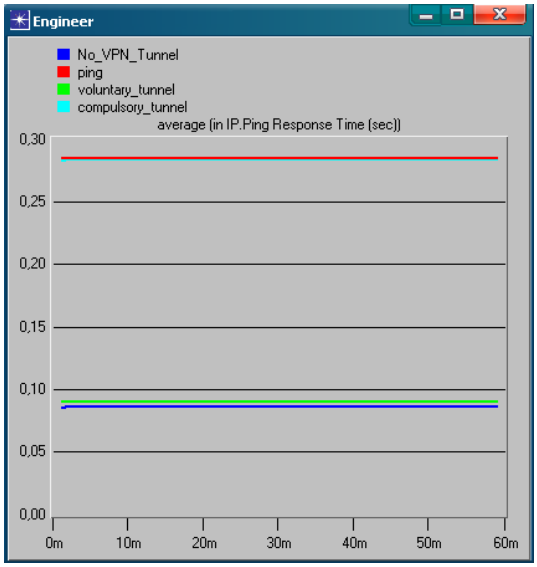

Figura 4.3.8– Tiempos de respuesta para túnel operando en modo obligatorio desde cliente Engineer.

Los tiempos de respuesta observados en la figura 4.3.8 nos muestran que la operación en modo voluntario responde en menor tiempo a las solicitud de ping

realizada desde el cliente de manera similar a la operación sin túnel vpn (0.1Seg)

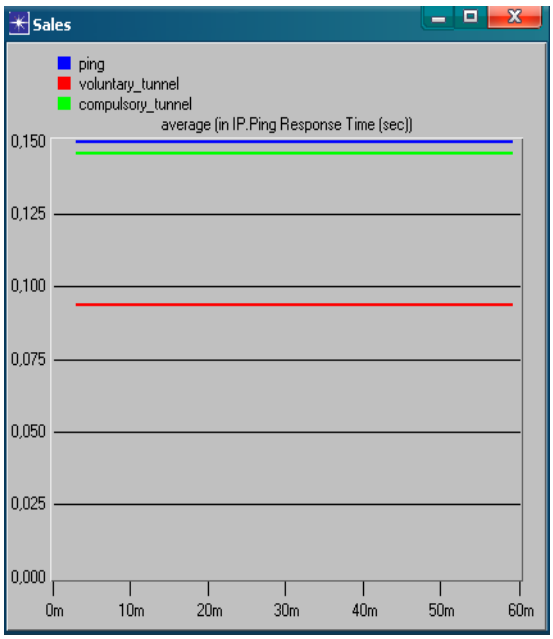

Figura 4.3.9– Tiempos de respuesta para túnel operando en modo obligatorio desde cliente Sales.

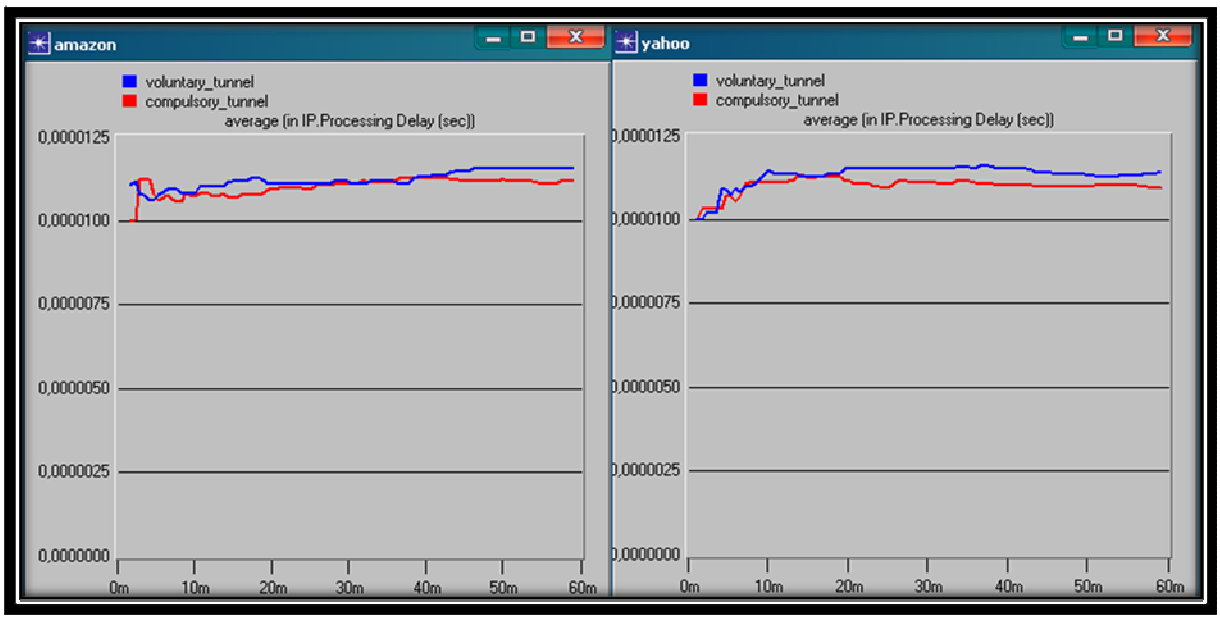

Figura 4.3.10– Retardo de procesamiento IP en el servidores Yahoo y Amazon.

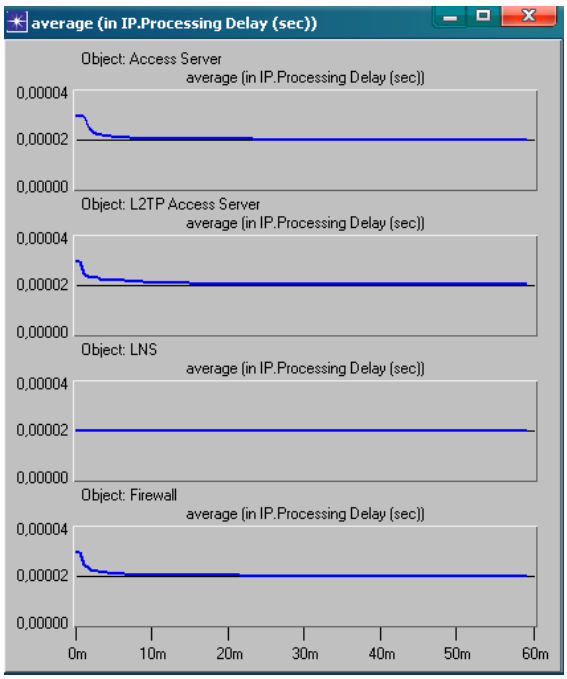

Figura 4.3.11– Retardo de procesamiento IP en los puntos terminales de los túneles VPN establecidos.

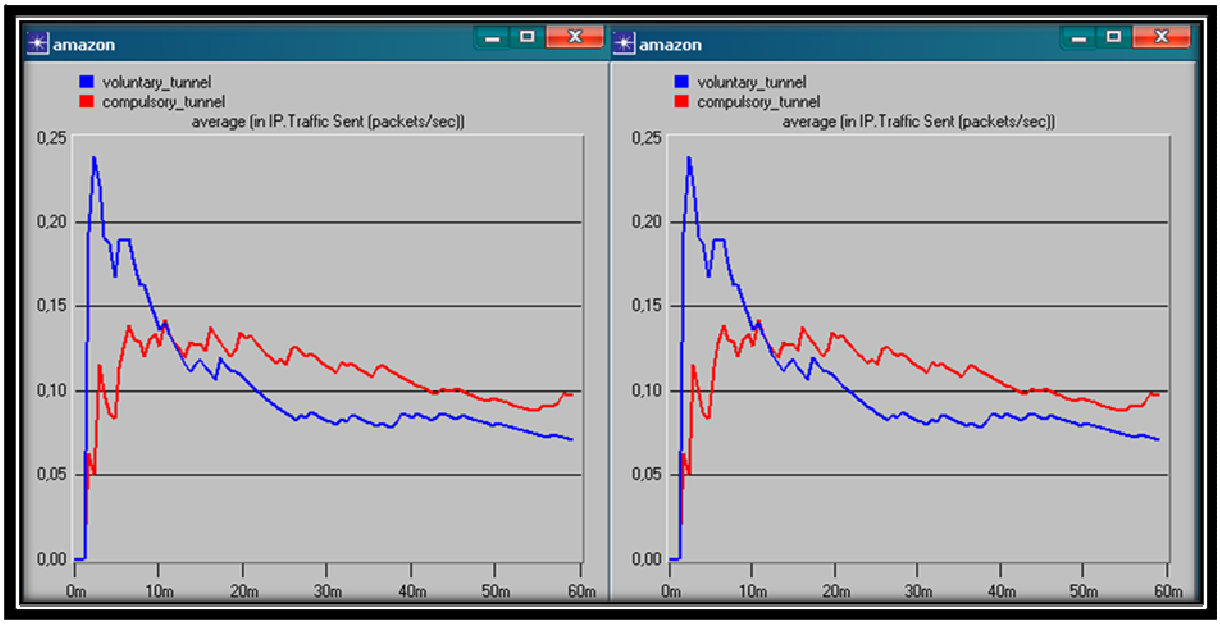

Figura 4.3.12–Trafico enviado y recibido para Amazon.

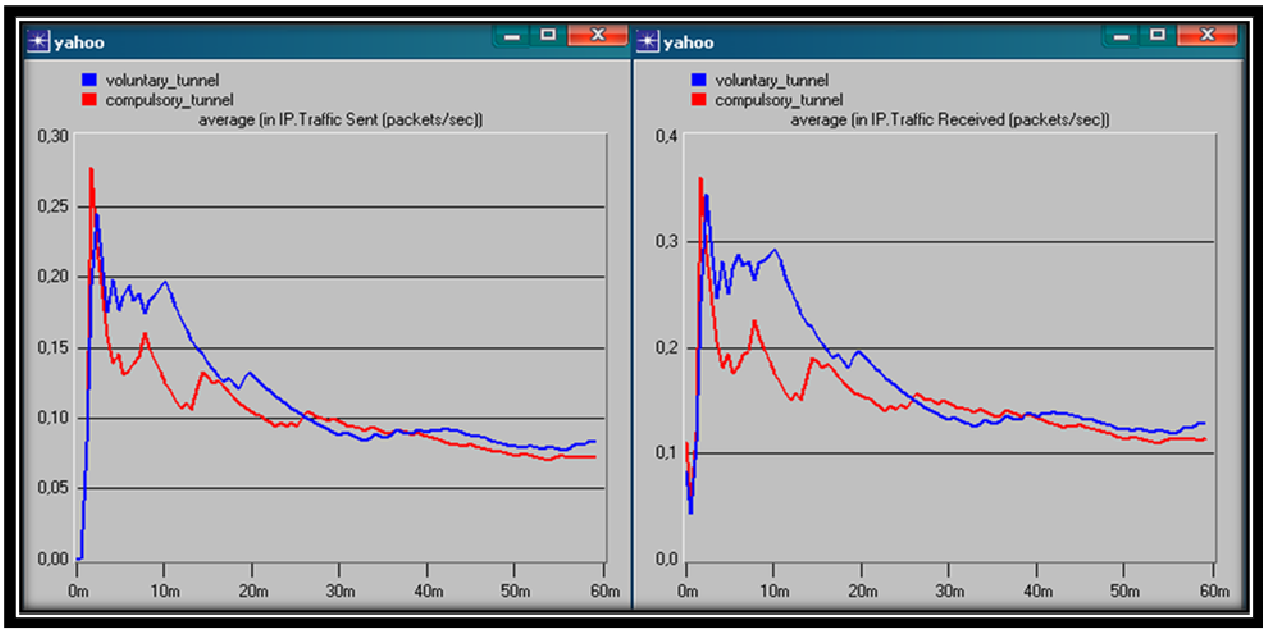

Figura 4.3.13–Trafico enviado y recibido para Yahoo.

El trafico IP correspondiente a las aplicaciones montadas en los servidores Amazon y Yahoo (Ver figura 4.3.12 y 4.3.13) nos muestra que para el túnel obligatorio la navegación en el servidor Amazon es levemente menor que para el de Yahoo, teniendo en cuenta el trafico recibido y enviado desde y hacia la red. Esto se debe a que en un túnel obligatorio se maneja la mayor parte del trafico en los dispositivos de frontera (LNS, Firewall, L2TP Access Server y Access Server) mientras que para un túnel voluntario la conexión se realiza directamente en los host, tal y como se evidencia en las graficas, existe un trafico mayor para la operación en modo voluntario ya que se están analizando el comportamiento de un host, en este caso el de destino del túnel. Por otra parte podemos observar que existe un mayor tráfico en las aplicaciones para la topología de túnel voluntario.

Los tiempos de respuesta a las solicitudes de ping realizadas desde el cliente Engineer para la operación obligatorio (280 ms, *Ver figura 4.3.8*) son mayores que en modo voluntario (10ms, *Ver Figura 4.2.6*). Este mismo rango aplica para el cliente Sales, ya que la latencia sigue siendo mayor (15ms, *Ver figura 4.3.9*) con respecto al modo de operación voluntaria (10ms, *Ver Figura 4.3.7*).

Los retardos observados en la topología de túnel obligatorio obedecen a retardos individuales producidas en distintas fases durante la creación y mantenimiento del túnel, la figura 4.3.7 muestra el retardo producido en la creación de los túneles, en los servidores de acceso, además del retardo producido por el procesamiento IP en los terminales de cada uno de los túneles (Ver Figura 4.3.11). Cada uno de estos factores influye en el rendimiento de un túnel VPN.

Para la aplicación de navegación web (Ver Figura 4.3.3), el modo obligatorio incrementa radicalmente los tiempos de respuesta (3 seg) en comparación con el escenario sin túnel VPN (450mS), este comportamiento se repite para la aplicación de Email (*Ver Figura 4.3.4*), en donde el tiempo de respuesta en modo obligatorio (3 seg) es mayor comparado con la operación sin túnel (900ms).Para el cliente Sales, los tiempos de acceso a las bases de datos (*Ver Figura 4.3.5*) y de respuesta a páginas (*Ver Figura 4.3.6*) son mayores para la topología de túnel obligatorio, lo que nos lleva a analizar las aplicaciones que queremos correr en el túnel debido a que para las mencionadas anteriormente el modo voluntario trabaja mejor, en cuanto a reducción de tiempos de espera ante aplicaciones.

Teniendo en cuenta los escenarios propuestos, se analizaron los dos tipos de tunelamiento vpn, voluntario y obligatorio, los resultados obtenidos a partir de las simulaciones nos muestran que el modo de operación voluntaria se ajusta mas a las características deseadas a la hora de implementar una vpn, en cuanto a un menor tiempo de respuesta a peticiones realizadas desde los dispositivos finales, trafico en la red y retardo de túneles, cabe resaltar que estas afirmaciones se hacen con base a las implementaciones hechas en los modelos de red propuestos, algunos aspectos pueden variar levemente las condiciones de la red ya que para los host no se han implementado políticas de seguridad que restrinjan el acceso (operación voluntaria) lo cual agrega retardos adicionales en cuanto al envío y recepción de paquetes en estos dispositivos.

CONCLUSIONES.

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, son sencillas de usar, se pueden instalar en cualquier Pc Windows, ofrece herramientas de diagnostico remoto así como también un control de acceso basado en las políticas de la organización.

El montaje de una red con VPN es útil en la medida en que se puedan reducir costos en una empresa pero hay que tener en cuenta que son muchos los riesgos que se tienen que asumir en cuanto a seguridad, vulnerabilidad de la información y dependencia de los ISP mediante los cuales este implementada la red virtual, por lo que es primordial establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

En la transmisión de datos se usan medidas estándares y protocolos de los elementos que intervienen. Protocolos como el L2TP, el cual es la base de las VPNs proporcionando túneles seguros, rentables y eficientes para el uso y la solución de nuestras necesidades de inter conectividad para el flujo de la información.

La latencia de los paquetes enviados a través de una VPN es mayor a las de una LAN, esto como consecuencia de los múltiples procesos de encriptación y compresión por los cuales tiene que pasar un paquete al llegar a su destino debido a que los protocolos se hacen más robustos en la medida en que se aumente la seguridad del enlace.

Las topologías de vpn implementadas (túnel voluntario y obligatorio) nos muestran grandes posibilidades y un sinnúmero de variables a tener en cuenta a la hora de implementar una vpn, las cuales debemos adaptar a nuestras

necesidades como clientes. Como podemos apreciar en el estudio realizado a estas topologías la operación en modo voluntario reduce los tiempos de retardo de paquetes, retardo de túneles y trafico en la red, lo cual es una gran ventaja si lo que buscamos es agilidad y confiabilidad, estos tiempos pueden ser optimizados con la asignación de mas ancho de banda a la conexión, ya que con estos recursos mejoramos la operación del túnel, por otra parte esta la operación en modo obligatorio, la cual ofrece mejorías de seguridad debido a que se pueden implementar políticas que restrinjan la operación de la vpn, estas condiciones aumentan los tiempos de retardo del túnel ya que inducen trafico a la red como consecuencia de la utilización permanente del túnel.

El desarrollo de las practicas y la simulaciones para diferentes escenarios, donde se consideran diversas situaciones para comprobar la performance de protocolos y herramientas de redes de forma interactiva, nos permite considerar este programa como una herramienta de juicio para el ingeniero de redes a la hora de implementar determinada configuración, con antelación a la implementación física y sentando bases para futuras expansiones de la disposición original.

BIBLIOGRAFIA

LIBROS:

PAGINAS WEB:

http://www.dei.uc.edu.py/tai2003/vpn/protocol.htm

http://www.cisco.com/warp/public/44/solutions.htm

http://www.infor.uva.es/~jvegas/docencia/ar/seminarios/VPN.pdf

http://www.helmig.com/j_helmig/vpn.htm

GLOSARIO

Aplicación: es el programa de cómputo diseñado para apoyar al personal de una organización a realizar cierto tipo de trabajo. Dependiendo del tipo de trabajo para la cual fue diseñada, la aplicación puede servir para el procesamiento de textos, números, gráficos o la combinación de estos elementos. (Application)

Atributo: es cada una de las características que definen un elemento. Es el término utilizado en las bases de datos relacionales para referirse a los campos de un registro de un archivo. Cada atributo esta asociado a un dominio del cual toma sus posibles valores.

BROADCAST: es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Cabecera: Porción frontal de un paquete que contiene información de protocolo, como direcciones, para dirigir el paquete a través de la red.

Dirección IP: es la identificación numérica de un nodo o servidor en Internet. Consta de cuatro números del 0 al 255 separados por puntos.

Encriptación: tratamiento de la información mediante la aplicación de una clave, de tal forma que si se desconoce el código, no se puede acceder a los datos transmitidos.

Firewall: son los programas que protegen a una red de otras. Conjunto de programas de protección y dispositivos especiales que ponen barreras al acceso exterior a una determinada red privada. Es utilizado para proteger los recursos de una organización de consultas externas no autorizadas.

FTP: Es el protocolo para la transferencia de archivos. Norma específica que regula el intercambio de archivos entre diferentes máquinas y sistemas. (File transfer protocol)

HOST: Computadora que, mediante la utilización de los protocolos TCP/IP, permite a los usuarios comunicarse con otros sistemas anfitriones de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, WWW y FTP. Los hosts son comúnmente llamados servidores.

HTTP (Hyper Text Transfer Protocol): Protocolo de comunicación de datos que permite la transmisión de documentos de hipertexto a través de redes. Es el protocolo en el que está basado el web.

ISP: Siglas de Internet Service Provider (Proveedor del servicio de Internet). Empresa que proporciona el servicio de acceso a la red Internet.

IPSec: Protocolo de seguridad para Internet. IPSec proporciona confidencialidad y/o integridad de los paquetes IP.

LAC: Dispositivo físico que se añade a los elementos de interconexión de la red conmutada; Como lo es la red telefónica convencional RDSI, o se coloca con un sistema de terminación PPP capaz de gestionar el protocolo L2TP.

LAN: (Local Área Network) Red de Área Local. Como su nombre indica, es una red de ordenadores de tamaño pequeño/medio localizada en un edificio (como máximo). Se conectan los ordenadores a través de tarjetas de red, y las arquitecturas más conocidas son Ethernet y Token-Ring.

LNS: L2TP NETWORK SERVER, Opera sobre cualquier plataforma con capacidad de terminación PPP. LNS gestiona el lado del servidor del protocolo L2TP.

L2TP: Layer-2 Tunneling Protocol, facilita el tunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.

MTU: Maximum Transmission Unit. Unidad Maxima de Transmision. Tamaño máximo de paquete en protocolos IP como el SLIP.

NAPT: Network Address Port Translation (NAPT). Método por el cual muchos de red y sus direcciones TCP / UDP se traduzcan en una sola dirección de red y su TCP / UDP.

PING: Es la herramienta que permite averiguar si existe un camino (comunicación) de TCP/IP entre dos computadoras de cualquier parte de Internet.

PPP: Point to Point Protocol. Protocolo Punto a Punto. Protocolo Internet para establecer elnlace entre dos puntos.

PPTP: Point-to-Point Tunneling Protocol, mecanismo de encapsulamiento, para permitir el transporte de protocolos diferentes del TCP/IP.

PUERTO: Es la conexión lógica y/o física de una computadora, que permite comunicarse con otros dispositivos externos o con otras computadoras. Los servicios de Internet (como el e-mail o la Web) utilizan puertos lógicos para establecer comunicaciones entre una computadora cliente y un servidor.

ROUTER: Dispositivo físico o lógico que permite encaminar la conexión entre redes TCP/IP, es el encargado de que los paquetes de información lleguen a su destino.

RUTAS ESTÁTICAS: rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso del enrutamiento según los parámetros del administrador. Las rutas estáticas por default especifican un gateway (puerta de enlace) de último recurso, a la que el router debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento, es decir que desconoce.

SMTP: [Simple Mail Transfer Protocol o Protocolo Sencillo de transferencia de correo.] El protocolo con el que se transmite un mensaje de correo electrónico de una máquina a otra.

Switch: Es un dispositivo electrónico de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo

OSI. Un switch interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

TCP: Protocolo de control de transmisión; norma orientada a conexión, que en general se parece al protocolo de transporte del modelo OSI, pero es completamente diferente a éste en cuanto a sus formatos y detalles. Conjunto de protocolos de comunicación que se encargan de la seguridad y la integridad de los paquetes de datos que viajan por Internet. Complemento del IP en el TCP/IP. (Transmission control protocol)

THROUGHPUT: Rendimiento final de una conexión. Volumen de datos que una conexión brinda como resultante de la suma de su capacidad y la resta de los overheads que reducen su rendimiento.

TOPOLOGÍA: es el mapa o idea de la red. La topología física describe el trazado de los hilos y los cables y la topología lógica o eléctrica describe el flujo de los mensajes.

TRAMA: es una secuencia de bits delimitada por un indicador de apertura y otro de cierre que se envían en serie a través de un canal de comunicaciones.

TUNNELING: técnica que usa una infraestructura entre redes para transferir datos de una red a otra. Los datos o la carga pueden ser transferidas como tramas de otro protocolo.