ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS E IMPLEMENTACIÓN DE LA MEJOR ALTERNATIVA PARA UNA VPN DE LA EMPRESA OPTIMSOFT PARA INTERCONECTAR LA BASE DE DATOS DE IMPORTACIONES ENTRE QUITO Y GUAYAQUIL

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

VIVIANA MARIBELL PAZMIÑO PULLAS

vivypapu@gmail.com

Director: Ing. Pablo Willian Hidalgo Lascano

Pablo.hidalgo@epn.edu.ec

Quito, Junio 2013

DECLARACIÓN

Yo, Viviana Maribell Pazmiño Pullas, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Viviana Maribell Pazmiño Pullas

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Viviana Maribell Pazmiño Pullas, bajo mi supervisión.

Ing. Pablo Hidalgo
DIRECTOR

AGRADECIMIENTOS

Agradezco a Dios por darme la oportunidad de culminar con éxito esta etapa de mi vida.

Un agradecimiento muy especial al Ingeniero Pablo Hidalgo, quien a más de ser uno de los mejores profesores de la Escuela Politécnica Nacional, es un amigo que con su ayuda y paciencia supo dirigirme de la mejor manera para poder llegar a terminareste proyecto.

Al Ing. Marco Guayasamín y a todo el personal de Optimsoft Cia. Ltda., por brindarme todas las facilidades para poder desarrollar el presente proyecto.

A mis padres por su constante esfuerzo y apoyo durante toda mi vida.

A mi esposo por apoyarme, motivarmey demostrarme que todas las metas que me he propuesto las puedo alcanzar con constancia y dedicación.

A mi hermano David por ser un ejemplo, y un amigo con el que siempre puedo contar.

A todos los amigos y familiares que en este largo caminar siempre supieron apoyarme e incentivarme allegar a la meta.

Al Ingeniero Carlos Herrera por su apoyo y amistad incondicional durante mi carrera universitaria.

Mil gracias a todos

Viviana Pazmiño

DEDICATORIA

Este Proyecto de Titulación quiero dedicarle a mi hija que es el tesoro más grande de mi vida, a mi esposo por ser la ayuda idónea que Dios me ha dado.

Es justo dedicarla a miMamia que con su comprensión y amor me supo siempre motivar para poder terminar este sueño de ser Ingeniera. A mi Papio que con su constante insistencia de “termina la tesis” fue una motivación muy grande.

Viviana Pazmiño

ÍNDICE DE CONTENIDOS

DECLARACIÓN i
CERTIFICACIÓN ii
AGRADECIMIENTO iii
DEDICATORIA iv
ÍNDICE DE CONTENIDOS v
ÍNDICE DE FIGURAS xii
ÍNDICE DE TABLAS xv
RESUMEN xvi
PRESENTACIÓN xvii

CAPÍTULO 1

1. INTRODUCCIÓN A LAS VPNs 1

1.1 DEFINICIÓN DE LAS VPN 3
1.1.1 HISTORIA DE LAS VPN'S 3
1.1.2¿QUÉ ES UNA VPN?.....6
1.2 FUNCIONAMIENTO DE UNA VPN 8
1.2.1SOLUCIONES VPN'S EN EL MODELO OSI 11
1.2.1.1 Capa 2 - Capa enlace de datos 11
1.2.1.1.1Protocolo Punto a Punto (PPP) 12
1.2.1.1.2Protocolo de túnel Punto a Punto (PPPTP) 15
1.2.1.1.3 Reenvío de capa 2 (L2F) (Layer 2 Forwarding) 17
1.2.1.1.4Protocolo de Túnel de Capa 2 (L2TP) Layer 2 Tunneling Protocol 18
1.2.1.2 Capa 3- Capa Red 20
1.2.1.3 Capa 7 – CapaAplicación 22
1.2.1.3.1 Protocolo Secure Sockets Layer (SSL) 22
1.2.1.3.2 Protocolo Transport Layer Security TLS 24

1.3 CATEGORÍAS DE LAS VPNs 26
1.3.1 VPN'S SEGÚN EL PUNTO DE TERMINACIÓN 26
1.3.1.1 VPN Overlay 27
1.3.1.2 VPN Peer to Peer 29
1.3.2 VPN Según el tráfico de cliente transportado 30
1.3.2.1 VPN de nivel2 30
1.3.2.2 VPN de nivel 3 31
1.3.3VPN SEGÚN EL NÚMERO DE SEDES CONECTADAS 31
1.3.4 VPN SEGÚN LA TECNOLOGÍA DE TÚNELES 31
1.3.4.1 Túnel IPsec 31
1.3.4.1.1 Redes Ruteadas Privadas Virtuales (VPRNs, Virtual Private Routed Networks) 31
1.3.4.1.2Redes Conmutadas Privadas Virtuales (VPDNs, Virtual Private Dial Networks)..... 32
1.3.4.2 Túnel L2TP 32
1.3.5 VPN SEGÚN EL ALCANCE 32
1.3.5.1 VPN de Acceso Remoto 32
1.3.5.2 VPN de Intranet 33
1.3.5.3 VPN de Extranet 34
1.4 TIPOS DE SEGURIDAD QUE SE PUEDEN UTILIZAR EN LA TRANSMISIÓN DE DATOS 35
1.4.1ENCRIPTACIÓN 35
1.4.1.1 Algoritmo de Encriptación DES (Data EncriptionStandard)35
1.4.1.2 Algoritmo de Encriptación 3DES (Triple DES) 36
1.4.1.3 Algoritmo de Encriptación AES(Advanced Encryption Standard) 36
1.4.1.4 Algoritmo de EncriptaciónRSA 37
1.4.1.5 Algoritmo de Encriptación IDEA (International Data Encryption Algorithm) 37
1.4.2ENCAPSULAMIENTO 37
1.4.3AUTENTICACIÓN 38
1.4.3.1 Algoritmos de Hashing 38

1.4.3.2 SHA (Secure Hash Algorithm) ……..…….. 38
1.4.3.3 MD4 (Message-Digest Algorithm 4) ……..…… 39
1.4.3.4 MD5 (Message-Digest Algorithm 5) …….. 39
1.4.3.5 HMAC (Hash-base del Código de autenticación de mensajes) …….. 39
1.4.3.6 EAP (Extensible Authentication Protocol) ……... 40
1.4.3.7 CHAP (Challenge Handshake Authentication Protocol) ….. 40
1.4.3.7.1 MS CHAP …….. 41
1.4.3.7.2 MS CHAP versión 2 …….. 42
1.4.3.8 SPAP (Shiva Password Authentication Protocol) …….. 42
1.4.3.9 PAP (Password Authentication Protocol) …….. 42
1.4.3.10 Grupo Hellman …….. 43
1.4.4 AUTORIZACIÓN …….. 44
1.4.5 CONFIDENCIALIDAD …….. 44
1.5 REQUERIMIENTOS BÁSICOS DE UNA VPN …….. 44
1.5.1 IDENTIFICACIÓN DE USUARIO …….. 44
1.5.2 ADMINISTRACIÓN DE DIRECCIONES …….. 45
1.5.3 CODIFICACIÓN DE DATOS …….. 45
1.5.4 ADMINISTRACIÓN DE CLAVES …….. 45
1.5.5 SOPORTE A PROTOCOLOS MÚLTIPLES …….. 45

CAPÍTULO 2

2. ESTUDIO DE LAS ALTERNATIVAS DE IMPLEMENTACIÓN DE UNAVPN ……..... 46
2.1 IMPLEMENTACIÓN MEDIANTE SOFTWARE …….. 46
2.1.1 USOS DE LA VPN MEDIANTE SOFTWARE …….. 46
2.1.2 VPNs WINDOWS SERVER 2003 ……..…..…... 46
2.1.2.1 Consideraciones básicas para instalación de una VPN …… 47
2.1.2.2 Requerimientos para crear una VPN mediante Windows Server 2003 …….. 49

2.1.2.3 Parámetros de diseño de la VPN de acceso remoto ……. 49
2.1.2.4 Configuraciones para crear una VPN con Windows Server 2003 ……... 52
2.1.2.4.1 Configuración del Servidor de la VPN …… 52
2.1.2.4.2 Configuración del Cliente VPN …… 57
2.1.2.4.3 Configuración de la clave compartida de IPSec …… 58
2.1.2.5 VPNs de nivel 2 con Microsoft…… 61
2.1.2.6 Problemática de las VPNs …… 61
2.1.3 LogmeIn HAMACHI …… 62
2.1.3.1 Funcionamiento de LogmeIn Hamachi …… 62
2.1.3.2 Ventajasde LogmeIn Hamachi …… 62
2.1.3.3 Seguridades de LogMeIn Hamachi …… 63
2.1.3.3.1 Arquitectura …… 63
2.1.3.3.2 Autenticación …… 63
2.1.3.3.3 Cifrado …… 64
2.1.3.3.4 Administración …… 64
2.1.3.3.5 Administración Centralizada …… 65
2.1.3.4 Instalación centralizada de software …… 65
2.1.3.5 Tipos de redes en LogmeIn Hamachi …… 66
2.1.3.5.1 Redes virtuales de puerta de enlace …… 66
2.1.3.5.2 Redes virtuales de concentrador y radio …… 66
2.1.3.5.3 Redes Virtuales de malla …… 67
2.1.3.6 Requerimientos para crear VPN con LogmeIn Hamachi ….. 67
2.1.3.7 Configuración para crear la VPN con LogmeIn Hamachi …. 67
2.2 IMPLEMENTACIÓN MEDIANTE HARDWARE …… 69
2.2.1 INSTALACIÓNDE LA VPN MEDIANTE HARDWARE …….. 69
2.2.2 CLASES DE VPN MEDIANTE HARDWARE …… 69
2.2.2.1 Sitio a sitio ……69
2.2.2.1.1 Requisitos para crear una VPN sitio a sitio utilizando Hardware …… 69
2.2.2.2 Acceso Remoto …… 70
2.2.2.2.1 Requisitos para crear una VPN de acceso remoto

mediante Hardware 70
2.2.3 VENTAJAS DE UTILIZAR VPN CON HARDWARE 70
2.2.4 CONFIGURACIÓN DE VPN MEDIANTE HARDWARE 71
2.2.5 PROTOCOLOS QUE SE UTILIZAN 74
2.2.5.1 Protocolos de Encriptación disponibles en el Router Linksys WRV 200 75
2.2.5.2 Protocolos de Autenticación disponibles en el Router Linksys WRV 200 75
2.3 IMPLEMENTACIÓN MEDIANTE FIREWALL 75
2.3.1 INTRODUCCIÓN A ISA SERVER 2004 75
2.3.2 CLASES DE VPN CON ISA SERVER 76
2.3.2.1 VPN de Acceso Remoto 76
2.3.2.1.1 Protocolos para VPN de acceso remoto 76
2.3.2.1.2 Funcionamiento de la VPN de Acceso Remoto 77
2.3.2.2 VPN Sitio a Sitio 77
2.3.2.2.1 Protocolos para VPN de Sitio a Sitio 78
2.3.2.2.2 Configuración básica para crear una VPN sitio a sitio mediante ISA Server con IPSec 78
2.3.3 VERIFICACIÓN DE CLIENTES DE LAVPN 79
2.3.3.1 Verificación por conexión 80
2.3.3.2 Verificación por usuario 80
2.4 ANÁLISIS COMPARATIVO DE LAS ALTERNATIVAS DE IMPLEMENTACIÓN 81
2.5 ANÁLISIS DE COSTOS DE LA IMPLEMENTACIÓN DE LA VPN 82
2.5.1 VPN DE SOFTWARE 85
2.5.2 VPN DE HARDWARE 85
2.5.3 VPN DE FIREWALL 86
2.6 PROTOCOLOS DE SEGURIDAD 87
2.6.1 PROTOCOLOS PARA VPNsMEDIANTE SOFTWARE 87
2.6.1.1 LogmeIn Hamachi 87
2.6.1.2 Windows Server 2003 88
2.6.2 PROTOCOLOS PARA VPNs MEDIANTE HARDWARE 88

2.6.3 PROTOCOLOS PARA VPNs MEDIANTE FIREWALL …… 89
2.6.4 PROTOCOLOS DE TÚNEL …….. 89
2.6.4.1 Comparaciónentre PPTP y L2TP …….. 89
2.6.5 PROTOCOLO DE CONFIGURACIÓN DINÁMICA DHCP …….. 90

CAPÍTULO 3

3. DISEÑO E IMPLEMENTACIÓN DE LA VPN …… **91**
3.1 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LAS APLICACIONES Y SERVICIOS EN LA RED DE LA EMPRESA OPTIMSOFT …….. 91
3.1.1 MONITOREO DE LA RED QUITO ……..... 91
3.1.2 DESCRIPCIÓN DE LA EMPRESA ……..... 93
3.1.2.1 Antecedentes de la empresa Optimsoft Cia. Ltda. …… 93
3.1.2.1.1 Trámites de Aduana o Nacionalización …….. 93
3.1.2.1.2 Trámites de Aduana o Nacionalización - In House …..… 95
3.1.2.1.3 Consultoría y Capacitación en Comercio Exterior ……. 95
3.1.2.1.4 Sistemas Integrados de Comercio Exterior - SICE …..... 96
3.1.2.2 Objetivo de la empresa Optimsoft Cia. Ltda. …….. 96
3.1.2.3 Misión de la Empresa …… 97
3.1.2.4 Visión de la Empresa …….. 97
3.1.2.5 Valores de la Empresa ……... 97
3.1.2.6 Sistemas de Información …… 98
3.1.2.6.1 Sistema SICE Profesional …… 98
3.1.2.6.2 Análisis de la Base de Datos de importaciones (db_impo) ……..…… 102
3.1.2.6.3 SICE Pro Scan …….. 104
3.1.2.6.4 Easy Marketing ……..…….. 105
3.1.2.7 Esquema actual de la red Optimsoft Matriz Quito ……... 105
3.1.2.8 Esquema actual de la red Optimsoft Sucursal Guayaquil …… 106
3.1.2.9 Descripción de las Aplicaciones actuales que generan tráficoen la red Optimsoft Quito …… 109

3.2 CÁLCULO DE LACAPACIDAD NECESARIA DEL CANAL PARA INTERCONECTAR LA BASES DE DATOS DE IMPORTACIÓN DE LA EMPRESA OPTIMSOFT ……..…… 113
3.3 DISEÑO DE LA VPN ……..... 122
3.3.1 ANTECEDENTESPARA REALIZAR LA VPN …….... 122
3.3.2 SELECCIÓN DE LA MEJOR ALTERNATIVA DE IMPLEMENTACIÓN …… 123
3.3.3 CARACTERÍSTICAS DEL ROUTER LINKSYS WRV-G200 ……. 124
3.4 IMPLANTACIÓN Y PRUEBAS DE LA VPN…….... 125
3.4.1 CONFIGURACIÓN DE LA VPN DELROUTER DE GUAYAQUIL …….. 126
3.4.2 CONFIGURACIÓN DEL ROUTER DE QUITO …… 131
3.4.3 PRUEBAS DE LA VPN …… 137

CAPÍTULO 4

4. CONCLUSIONES Y RECOMENDACIONES …….. 144

4.1 CONCLUSIONES …… 144
4.2 RECOMENDACIONES …… 146

REFERENCIASBIBLIOGRÁFICAS……148

ANEXOS

ANEXO A Tabla comparativa de las versiones LogmeIn Hamachi
ANEXO B Monitoreo con el programa PRTG *Traffic Grapher*

ÍNDICE DE FIGURAS

Capítulo 1

Figura 1.1 Red LAN …… 2
Figura 1.2 Redes de Área Extendida …… 2
Figura 1.3 VPN de Primera Generación ……..3
Figura 1.4 VPN de Segunda Generación …… 4
Figura 1.5 VPN de Tercera Generación ……..5
Figura 1.6 VPN basada en MPLS ……5
Figura 1.7 Usuarios VPN …… 7
Figura 1.8 Conexión mediante Dial Up …… 9
Figura 1.9 Encapsulamiento de Datos …… 10
Figura 1.10a Túnel con Protocolo GRE …….. 10
Figura 1.10b Túnel con Protocolo GRE …….. 11
Figura 1.11 Soluciones VPNs en el Modelo OSI …… 12
Figura 1.12 Trama PPP …….. 13
Figura 1.13 Trama PPTP …… 15
Figura 1.14 Trama L2F …… 18
Figura 1.15 Formato del paquete L2TF (Mensaje de datos) …… 20
Figura 1.16 Formato del paquete L2TF (Mensaje de control) …….. 20
Figura 1.17 Trama IPsec- Modo Túnel …… 21
Figura 1.18 Trama IPsec- Modo Transporte ……... 21
Figura 1.19 Clasificación de las VPNs. ……26
Figura 1.20a VPN OVERLAY ……... 27
Figura 1.20b VPN OVERLAY …….. 28
Figura 1.21 VPN Peer to Peer …… 30
Figura 1.22 VPN de acceso remoto …….. 33
Figura 1.23 VPN deIntranet …….. 34
Figura 1.24 VPN de Extranet …….. 34
Figura 1.25 Clave de 64 bits del algoritmo DES …….. 36

Capítulo 2

Figura 2.1 Enrutamiento y acceso remoto Windows Server 2003 53
Figura 2.2 Enrutamiento y acceso remoto al servidor 54
Figura 2.3 Asistente para instalación del servidor de enrutamiento y acceso remoto 54
Figura 2.4 Configuración en modo de acceso remoto 55
Figura 2.5 Configuración VPN en el acceso remoto 56
Figura 2.6 Requisitos de retransmisión DHCP 57
Figura 2.7 Establecer una clave compartida previamente en el enrutador de respuesta 60
Figura 2.8 Clave compartida previamente en el enrutador de llamada 61
Figura 2.9 Administración de redes Hamachi desde la web 65
Figura 2.10 Red Virtual de puerta de enlace 66
Figura 2.11 Red Virtual de concentrador y radio 66
Figura 2.12 Red Virtual de malla 67
Figura 2.13 VPN sitio a sitio de Hardware 70
Figura 2.14 VPN de acceso remoto con hardware 71
Figura 2.15 VPN mediante Firewall ISA Server 2004 77
Figura 2.16 VPNcon verificación por conexión 80
Figura2.17 VPN con verificación por usuario 81

Capítulo 3

Figura3.1 Monitoreo de la tarjeta de red del servidor UIO.....92
Figura3.2a Propiedades del servidor SQL de la empresa Optimsoft 100
Figura 3.2b Propiedades del servidor SQL de la empresa Optimsoft 101
Figura 3.3 Características de la Base de Datos db_impo 101
Figura 3.4 Diagrama red Optimsoft Quito 107
Figura 3.5 Diagrama red Optimsoft Guayaquil 108

Figura 3.6 Porcentajes de ancho de banda utilizado por las aplicaciones de la empresa Optimsoft …….. 120
Figura 3.7 Tráfico generado en la base de datos db_impo …….. 122
Figura 3.8 Velocidad de carga y descarga de Internet de la conexión en Quito …… 122
Figura 3.9 Envío de la información UIO- GYE (correo electrónico) ……. 123
Figura 3.10 Configuración de la IP del Router de Guayaquil …….. 126
Figura 3.11 Configuración actual del router de Guayaquil …….. 127
Figura 3.12 Resumen de los datos de configuración actual del router de Guayaquil …….. 127
Figura 3.13 Habilitación de la VPN …….. 130
Figura 3.14 Configuración de protocolos de encriptación y autentificación …. 130
Figura 3.15 Habilitación Protocolos de Túnel …… 131
Figura3.16 Configuración de la IP del Router para acceder al servidor de base de datos …… 132
Figura 3.17 Resumen de la configuración del Router de Optimsoft en la ciudad de Quito …… 132
Figura 3.18 Configuración de la VPN para el Router de Quito …….. 135
Figura 3.19 Estado del Túnel de la VPN creada visto desde UIO ……. 135
Figura 3.20 Túnel Conectado de la VPN (UIO-GYE) (Tunel Opt) …….. 136
Figura 3.21 Túnel Conectado dela VPN (GYE- UIO) (Tunel Opt) ……. 136
Figura 3.22 Información Avanzada de la conexión del Túnel Quito Guayaquil …….. 137
Figura 3.23 Ping a un usuario del Grupo remoto Seguro de la VPN ……. 138
Figura 3.24a Prueba de Acceso a recursos compartidos a través del IP del computador de la red remota …….. 138
Figura 3.24b Prueba de Acceso a recursos compartidos a través del IP del computador de la red remota …….. 139
Figura 3.25 Verificación Acceso remoto desde la aplicación GYE a db_impo UIO …….. 140
Figura 3.26 Acceso al sistema SICE Profesional …….. 140

Figura 3.27 Acceso al SICE Profesional desde un usuario remoto seguro en Guayaquil …….. 141
Figura3.28 Prueba de Conexión de la VPN con programa VPN Link Test 142
Figura 3.29 Prueba de Conexión de la VPN con opción VPN Summary …..... 143

ÍNDICE DE TABLAS

Capítulo 1

Tabla 1.1 Comparación de Modo IP Transporte con IP Túnel …….. 22
Tabla 1.2 Ventajas y Desventajas de las VPNs Overlay …….... 28
Tabla 1.3 Ventajas y desventajas de la implementación de VPNs peer to peer ……. 29

Capítulo 2

Tabla 2.1 Comparación de protocolos para VPN …….... 78
Tabla 2.2 Cuadro comparativo de alternativas de implementación de VPN ... 83

Capítulo 3

Tabla 3.1 Comparación Google Apps con Google Apps for Business ..…... 110
Tabla 3.2 Estadísticas de visitasa las redes sociales ……. 112
Tabla 3.3 Cálculo del ancho de banda utilizado por cada aplicación ……... 119

RESUMEN

El presente proyecto de titulación busca determinar las principales alternativasde VPN que pueden ser implementadas para establecer una conexión con protocolos de seguridad hacia la base de datos de importaciones de la empresa Optimsoft ubicada en Quito desde la sucursal de Guayaquil. El capítulo 1, Introducción alasVPNs, introduce al lector en el funcionamiento una VPN, sus diferentes categorías y los tipos de seguridad que se pueden utilizar en la trasmisión de datos.

El capítulo 2, Estudio de las alternativas de implementación de una VPN, trata sobre laimplementación mediante software, *hardware* y *firewall* de una VPN. Además se haceun análisis comparativo de las alternativas de implementación y finalmente se estudian losprotocolos de seguridades en cada alternativa.

El capítulo 3, Diseño e implementación de la VPN,presenta unanálisis de la situación actual del tráfico en la red de la empresa Optimsoft; posteriormente se hace el cálculo de la capacidad del canal necesario para interconectar la bases de datos de importación de la empresa Optimsoft para luego diseñar la VPN y finalmente implementar y realizar pruebas.

En el capítulo 4, Conclusiones y recomendaciones, se detallan las principales conclusiones y recomendaciones que se obtuvieron en el proyecto de titulación.
Cada capítulo sigue la secuencia de actividades por la metodología que se plantea para hacer realidad la Implementación de la VPN en la empresa Optimsoft.

PRESENTACIÓN

El presente trabajofue elaborado para optimizar recursos, tiempo y evitar ataques en la información, analizando las VPN como alternativa económica y segura.

Se interconecta una base de datos entre dos ciudades que se encuentran en diferentes ubicaciones geográficas.

Es un trabajo práctico para la empresa Optimsoft; proporcionándoles una solución al principal problema al que se enfrentaban día a día, el no poder acceder directamente a la información almacenada en la base de datos de Quito.

Este trabajo es muy útil ya que da solución a la interconexión de forma inmediata a un bajo costo, sin realizar cambios en la red existente, sin dejar de lado la seguridad en la transmisión de la información.

Muchas empresas pueden aplicar la VPN para solucionar el problema de compartición de datos y ver el presente proyecto de titulación como una guía para poder realizarlo.

CAPÍTULO 1.INTRODUCCIÓN A LAS VPNs

Las empresas han ido evolucionando y junto con ellas las redes de comunicación que las conectan, dando lugar a las diferentes redes que ahora se conocen.

Mediante las primeras LAN (Redes de Área Local) las empresas iniciaron sus interconexiones y sus accesos a recursos compartidos, en unárea relativamente pequeña, tal como se puede observar en la figura 1.1, tomando en cuenta que para ese entonces eran suficientes para cumplir con las necesidades de las empresas.

A medida que el Internet era más utilizado por motivos laborales, las empresas se extendían formando nuevas sucursales, que se hallaban dispersas en las ciudades, provincias, países. Para solucionar la conectividad se crearon las WAN (Redes de Área Extendida),en las que se realizaba una inversión costosa en hardware, software y servicios de telecomunicaciones. (verfigura 1.2)

Una de esas soluciones fue implementar líneas Punto a Punto también llamadas enlaces dedicados, mediante las cuales se contrataban a empresas que provean el medio de comunicación, realizando un pago por instalación y una mensualidad por el uso de la línea. Esta solución tenía como desventaja que cada punto a interconectar requería una nueva línea dedicada yal ser éstas muy costosas, las empresas pequeñas no las podíanimplementar.

Con el uso conjunto del Internet y las Redes Privadas Virtuales (VPNs) se logró solucionar el problema de costos,permitiendo que empresas pequeñas que cuentan con bajo presupuesto se mantengan conectadas y puedan compartir información con seguridad.

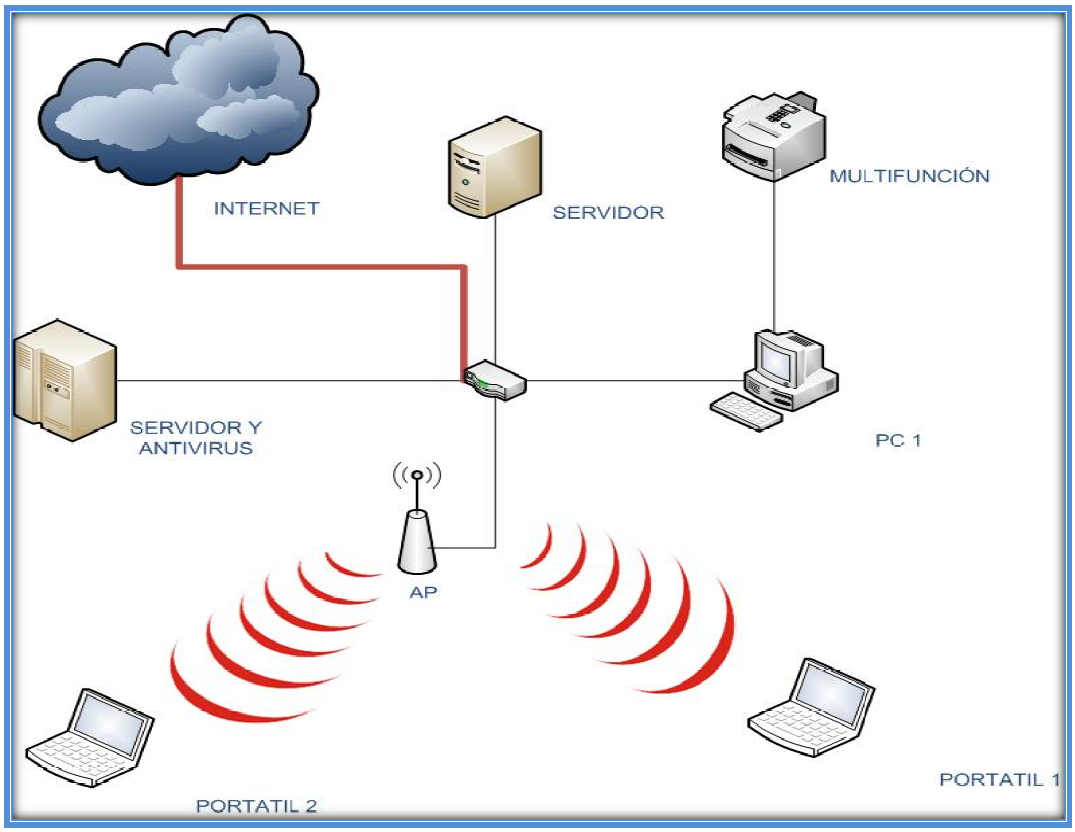


Figura 1.1 Red LAN

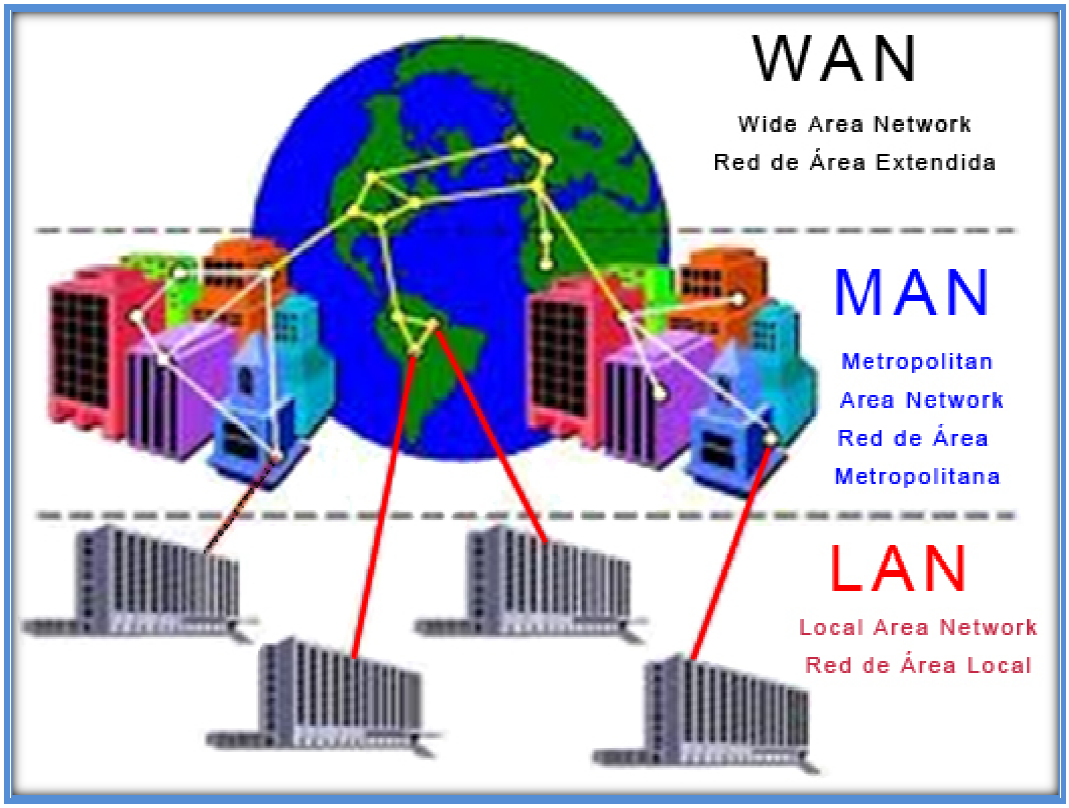


Figura 1.2 Redes de Área Extendida[1]

1.1DEFINICIÓNDE LAS VPN

1.1.1 HISTORIA DE LAS VPNS

El rápido desarrollo y uso del Internet como medio de comunicación para datos críticos en negocios trajo consigo la aparición de las VPNs, que como toda red de comunicación tiene su propia evolución, la misma que se analizará a continuación.[2]

- **1ª Generación**: Terminadas en el CE[1]y basadas en líneas dedicadas que se alquilaban al proveedor, creadas sobre sistemas que "corren" software para VPN. (Ver figura 1. 3).

  Líneas Dedicadas.- Posibilitan la transmisión de datos a velocidades medias y altas (de 64Kbps a 140 Mbps).

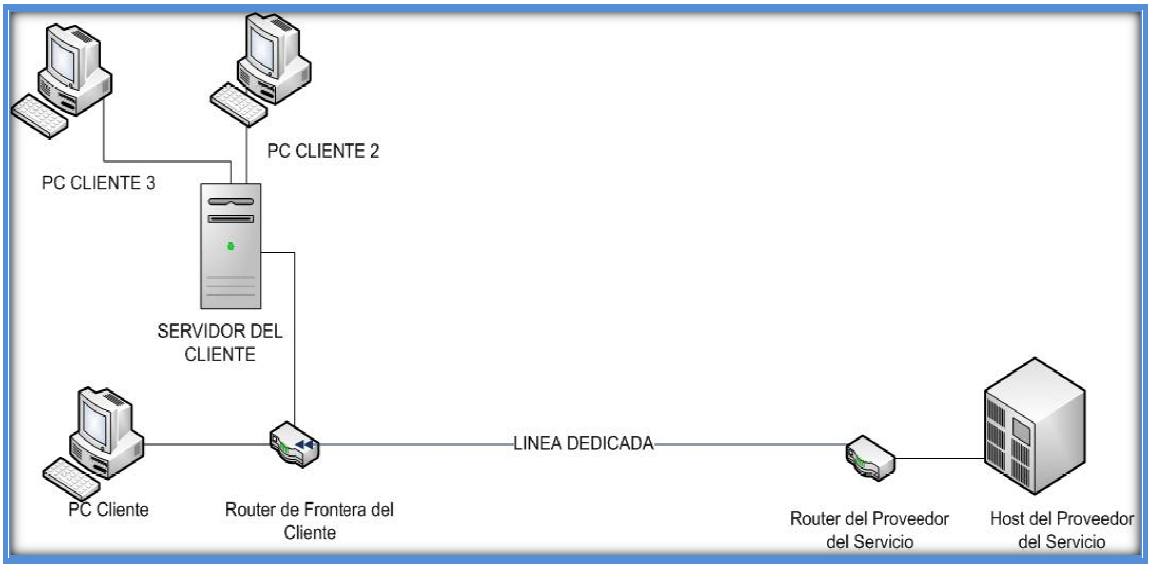


Figura 1.3VPN de Primera Generación

- **2ª Generación**: Terminadas en el CE a base de circuitos virtuales ATM[2] o Frame Relay[3](ver figura 1.4) sobre una red del proveedor. A pesar de

[1] CE (*Customer Equipment*) .- Equipo Del cliente

poseer funcionalidad por parte del proveedor no se cuenta con un buen rendimiento de la VPN.

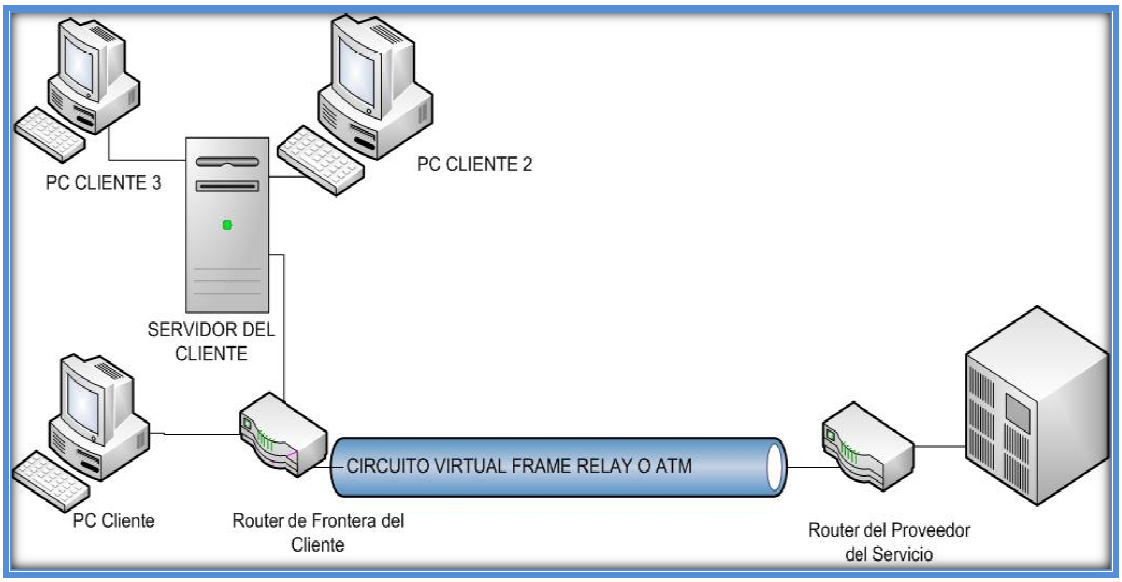


Figura 1.4VPN de Segunda Generación

- **3ª Generación**: Los proveedores gestionan los *routers* del cliente utilizados en sus terminaciones. Está basada sobre hardware dedicado a menudo referido como "aparatos VPN[4]", tal como se observa en la figura 1.5. Estos dispositivos emplean hardware dedicado, para acelerar la encriptación. Muy a menudo, éstos también incluyen un *firewall* más o menos fuerte y otras funcionalidades tales como QoS, VoIP, etc.

  Calidad de Servicio (QoS).- Tecnología que garantiza la transmisión de determinada cantidad de información en un tiempo dado (*throughput)*y con atención a sus requerimientos.Sirve para calificar si se está brindando un buen servicio;es importante para ciertas aplicaciones (ej. vídeo o voz).

---

[2]ATM.- Modo de Transferencia Asíncrona, desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

[3]Frame Relay.- Tecnología de transmisión de datos basada en la retransmisión de tramas.

[4] "Aparatos VPN".- *hardware* que posee características de VPN.

- **4ª Generación**: VPNs de nivel 3 terminadas en el PE[5]y basadas en IP/MPLS. (figura 1.6).

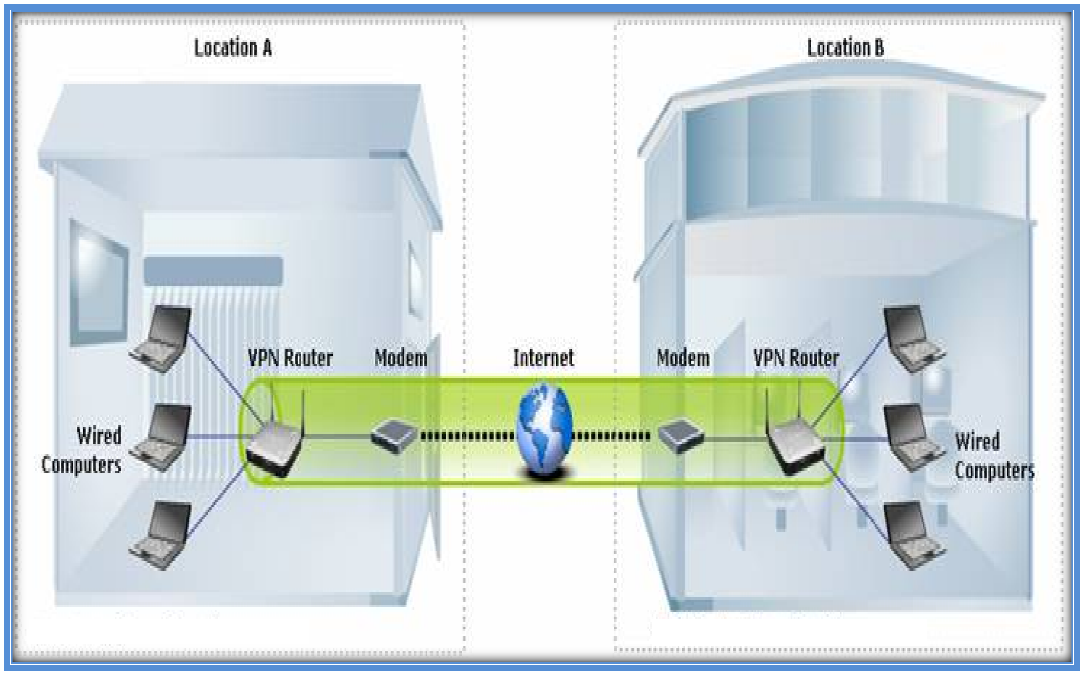


Figura 1.5VPN de Tercera Generación[3]

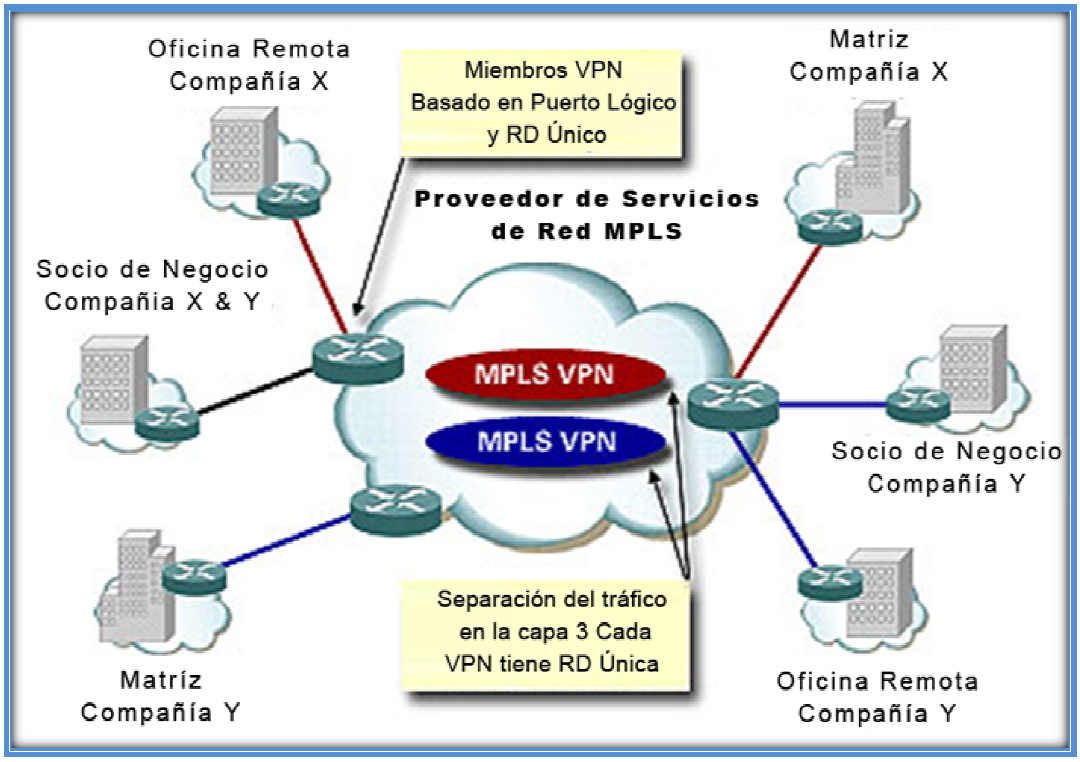


Figura 1.6VPN basada en MPLS [4]

[5]PE (*Provider Equipment*).-*Router* de frontera de la red del proveedor de servicio.

VPN de Nivel 3.- Enuna red IP / MPLS,estas VPNofrecen una solución de ruta completamente basada en el esquema de direcciones IPv4, escalable; su estándar está en el RFC4364 (febrero de 2006).

- **5ª Generación**: VPNs de nivel 2 terminadas en el PE y basadas en IP/MPLS.

VPN de nivel 2.-Proporciona un servicio de transporte multiprotocolo sobre infraestructura de nivel 2.

1.1.2 ¿QUÉ ES UNA VPN?

Se pueden encontrar muchas definiciones acerca de las VPNs, a continuación se citan algunas.

“Una VPN (*Virtual Private Network*) es una estructura de red corporativa implantada sobre una red de recursos de transmisión y conmutación públicos, que utiliza la misma gestión y políticas de acceso que se utilizan en las redes privadas. En la mayoría de los casos la red pública es Internet, pero también puede ser una red ATM o Frame Relay. Adicionalmente, puede definirse como una red privada que se extiende, mediante procesos de encapsulación y cifrado, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte, como la Internet.”[5]

“La VPN es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.”[6]

“Una Red Privada Virtual (VPN, *Virtual Private Network*) se construye a base de conexiones realizadas sobre una infraestructura compartida con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada real. El objetivo de las VPNs es el soporte de aplicaciones intranet / extranet,

integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables."[7]

"Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro. Las *firewalls* o ambos sitios permiten una conexión segura a través de Internet. Las VPNs son una alternativa de coste útil, para usar líneas alquiladas que conecten sucursales o para hacer negocios con clientes habituales. Los datos se encriptan y se envían a través de la conexión, protegiendo la información y el *password*."[8]

En base a las definiciones antes mencionadas, se puede decir: Las VPNs se crean en la infraestructura pública compartida, elaborando un entorno privado, confidencial y seguro. Posee iguales ventajas que las redes privadas:Conexión con protocolos de seguridad, acceso únicamente de personal autorizado a los servicios de la empresa (documentos, servidores de base de datos, aplicaciones específicas).

Una de las características importantes de las VPNs es que su implementación y uso no representa un costo elevado, haciéndolas accesibles para todas las empresas sean grandes o pequeñas.

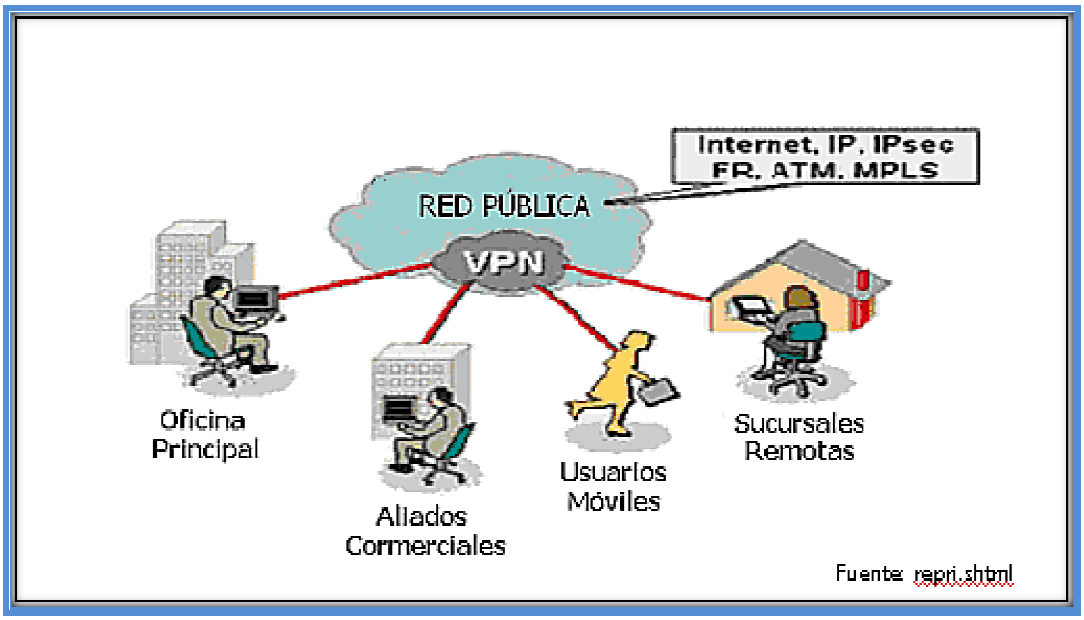


Figura 1.7 Usuarios VPN[9]

En la figura 1.7, se puede ver cómo las VPNs sirven para interconectar múltiples entornos.

1.2 FUNCIONAMIENTO DE UNA VPN

El Internet fue específicamente diseñado para el enrutamiento de tráfico de forma rápida entre dos puntos de enlace, para resolver problemas de escalabilidad,encontrados en las redes cuando utilizan enlaces punto a punto.

El Internet está compuesto por múltiples dispositivos de redes que son administradas por diferente número de organizaciones. Ninguna organización puede controlar o ser responsable de la privacidad o integridad de los datos trasmitidos. El Internet es visto algunas veces como un medio inseguro para transmitir datos, porque hay oportunidades de modificar y borrar los datos en su transmisión.

Las VPNs proporcionan un medio seguro para usar las fortalezas de la infraestructura del canal público de Internet como un canal propio para comunicación de datos, usando la tecnología de encriptación y encapsulamiento;de esta manera se crea un túnel privado a través de Internet.Se logra un proceso totalmente transparente para el usuario y para la mayoría de las aplicaciones, funcionando exactamente igual que cualquier otra conexión de red.

Cuando se crea la VPN cada equipo tiene una IP, mediante las cuales sus datos serán encriptados(el usuario simplemente tendrá que usar las IP's de la VPN). Luego de lograr la autenticación tiene acceso a la red local de la empresa, logrando así reemplazar con esta tecnología su infraestructura *dial-up*[6](módems ylíneas telefónicas).

---

[6]*Dial Up*.- Es una conexión por PSTN (Red Pública Telefónica Conmutada) para lograr el acceso a Internet, es relativamente económico pero lento. Se utiliza un módem para conectar la línea telefónica; posee velocidades de: 2400 bps hasta 56 kbps.

La VPN posee un protocolo especial para encapsular cada paquete origen en uno nuevo que incluya los campos de control para crear, gestionar y deshacer el túnel.

En la figura 1.8 se indica una conexión que utiliza Dial Up.

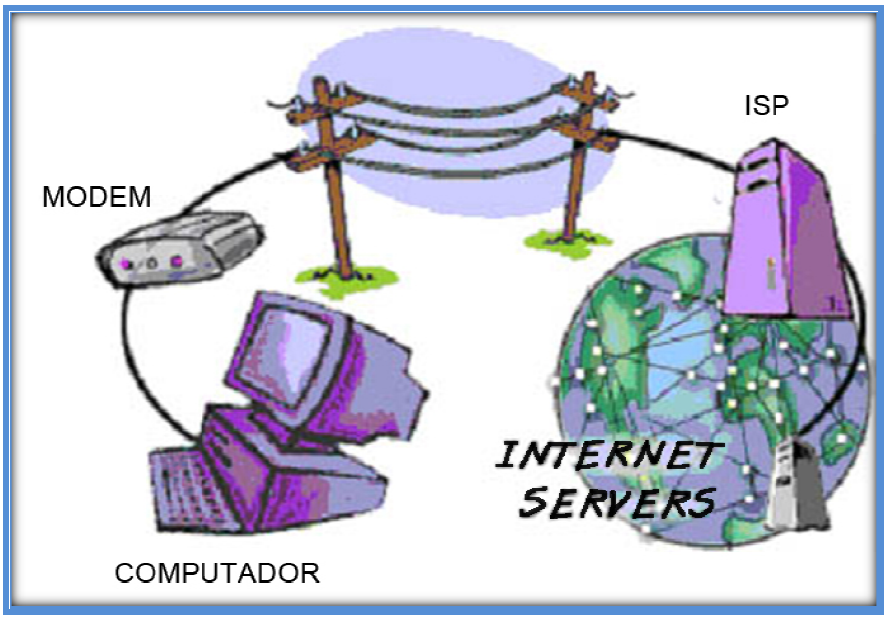


Figura 1.8 Conexión mediante *Dial Up*[10]

Se establece el túnel usando una PDU [7] determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel, sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver transparentemente el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, como se puede ver en la figura 1.9.

Como se puede apreciar en las figuras 1.10.a y 1.10.b se utiliza el protocolo GRE[8] para establecer el túnel a través de Internet, empleando protocolos de encaminamiento especializados en obtener el camino óptimo entre los extremos de la comunicación, estableciendo políticas de encaminamiento y seguridad.

---

[7]PDU (Unidad de datos de protocolo)

[8]GRE (*Generic Routing Encapsulation*)

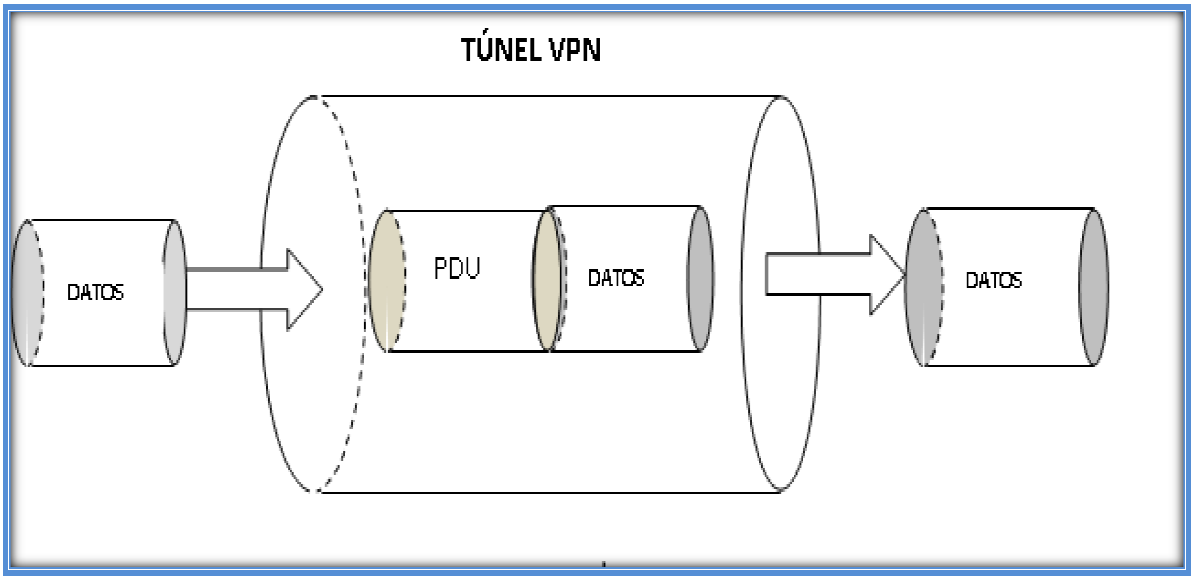


Figura 1.9 Encapsulamiento de Datos

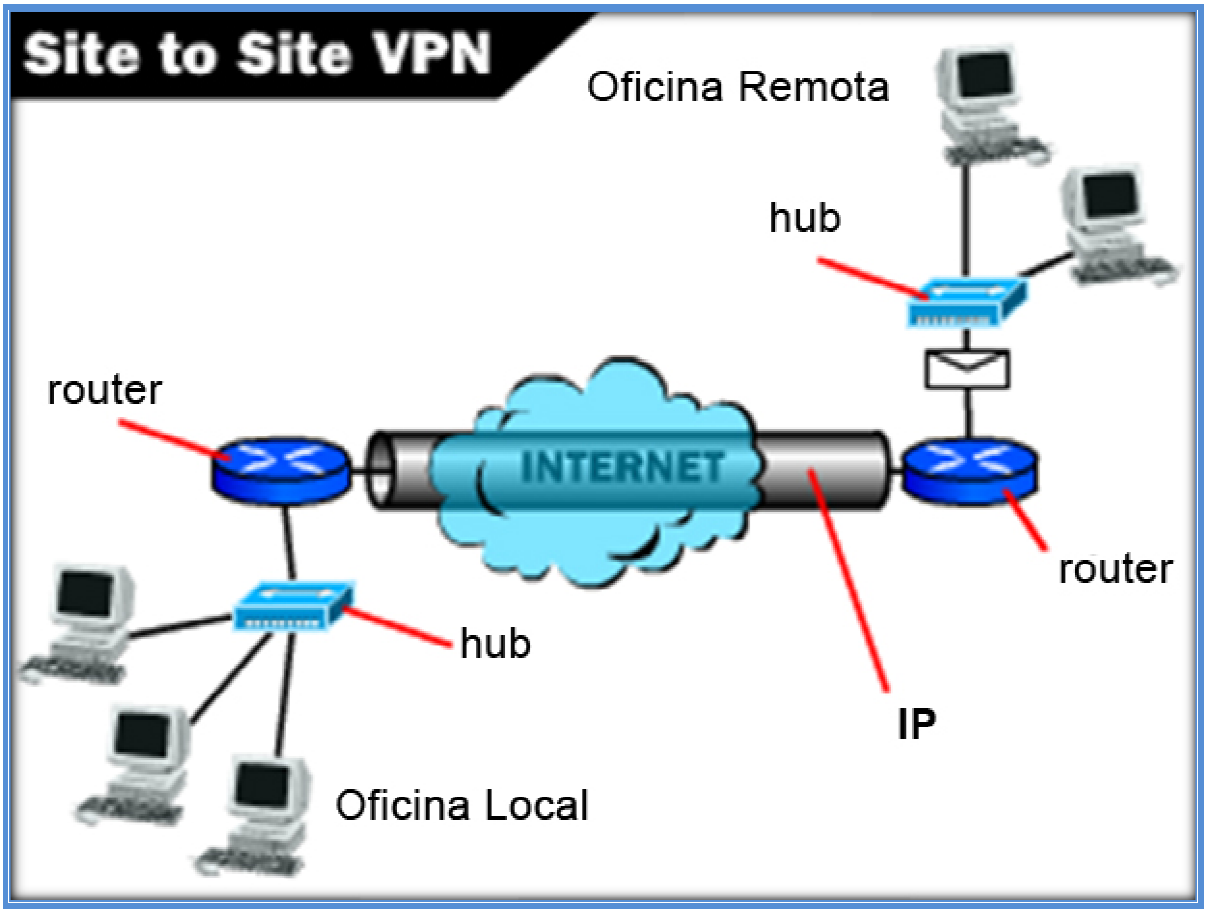


Figura 1.10aTúnel con Protocolo GRE[11]

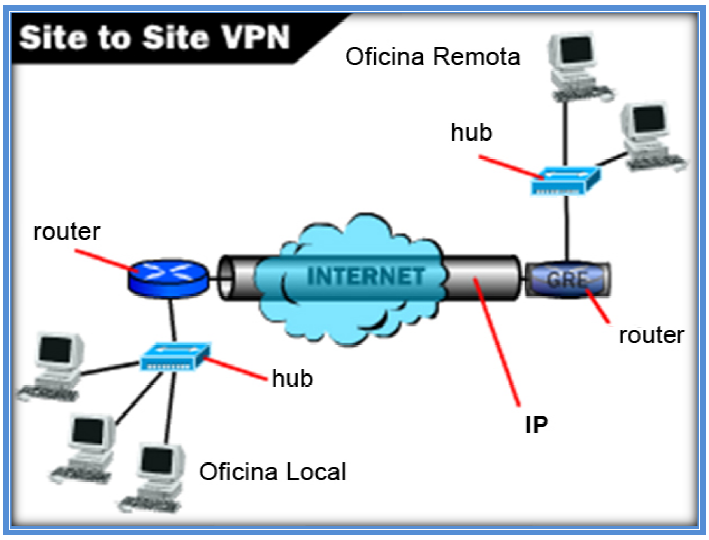


Figura 1.10bTúnel con Protocolo GRE[12]

1.2.1 SOLUCIONES VPNs EN EL MODELO OSI[9]

Las VPNs pueden ser construidas sobre protocolos de túnel que son implementados en las diferentes capas del modelo OSI. Como se puede apreciar en la figura 1.11 las características de túnel que se crea son determinadas por el protocolo de túnel empleado.

1.2.1.1 Capa 2 - Capa enlace de datos

En la capa enlace se realiza el direccionamiento físico de la red, acceso al medio, detección de errores, distribución ordenada de tramas [10] y control del flujo.

Teóricamente, las tecnologías implementadas en capa 2 pueden tunelizar cualquier tipo de paquetes y en la mayoría de los casos lo que se hace es establecer un dispositivo virtual con el cual se establece la conexión con el otro lado del túnel. Utiliza protocolos de túnel L2TP (*Layer 2 Tunneling Protocol*), L2F (*Layer2 Forwarding*) y PPTP (*Point to Point Tunneling Protocol*), estos protocolos utilizan autentificación de *password* para prevenir conexiones no autorizadas.

---

[9] OSI (*Open System Interconnection*)

[10]Tramas.- Unidades de información con sentido lógico para el intercambio de datos en la capa enlace

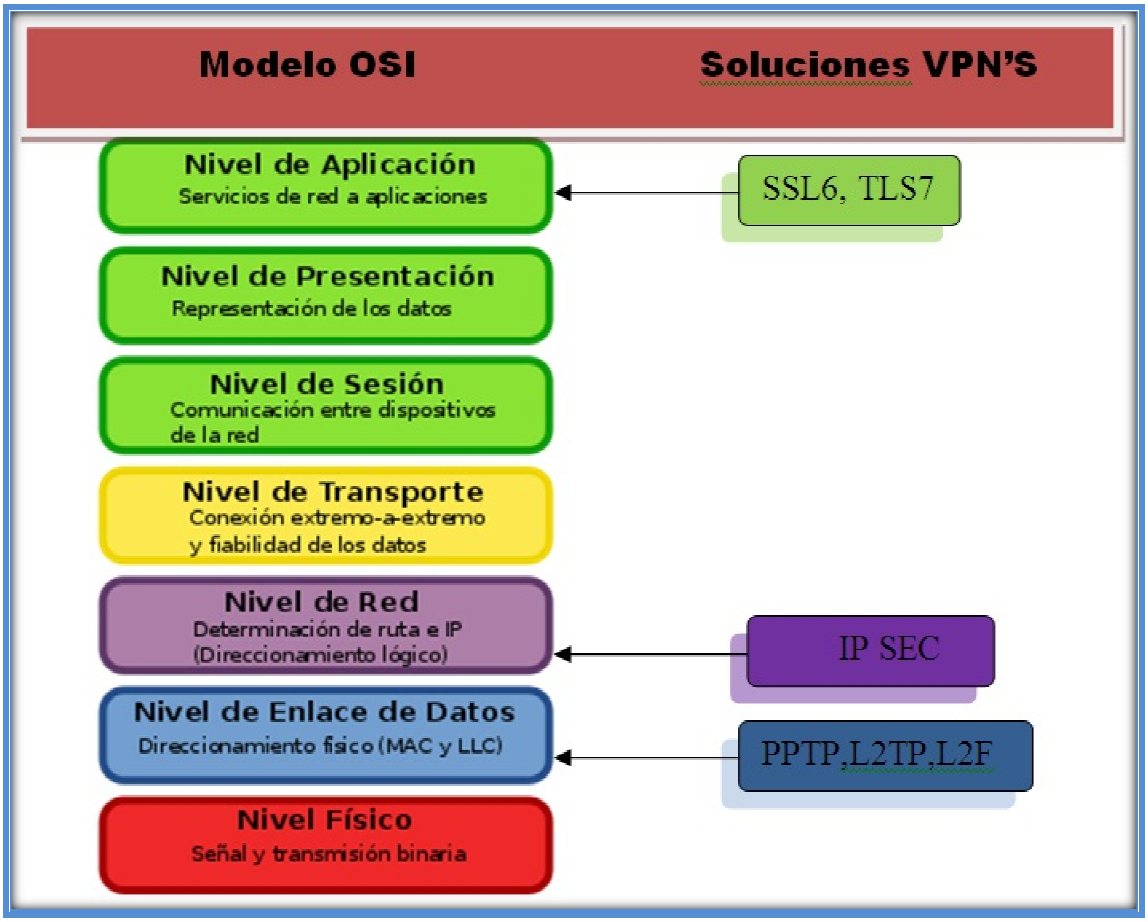


Figura 1.11Soluciones VPNs en el Modelo OSI

1.2.1.1.1 Protocolo Punto a Punto (PPP)

El protocolo punto a punto fue desarrollado por IETF (*Internet Engineering Task Force*) en 1993.

Permite la asignación dinámica de direcciones y soporta múltiples protocolos de capa 3, por lo que es compatible con diferentes fabricantes. Proveeconectividad entre enrutadores y clientes; la red puede poseer enlaces sincrónicos y asincrónicos.Proporciona un método que es estándar para el transporte de paquetes multiprotocolo; este transporte se realiza entre dos pares de *routers*que están a ambos extremos de la conexión, es una operación bidireccional y *full-duplex.*

Establecimiento de la sesión PPP

1. Establecimiento del enlace y negociación
2. Determinación de la calidad del enlace
3. Configuración del protocolo de capa red
4. Transferencia de datos
5. Comprobación
6. Terminación del enlace

Trama PPP

En la figura 1.12se pueden observar los bytes que son enviados al establecer una sesión PPP.

Bandera	Dirección	Control	Protocolo	Datos	FCS	Bandera
01111110	11111111	00000011	2 bytes	Longitud variable.	2 o 4 bytes	01111110

Figura 1.12 Trama PPP

Bandera de Inicio.- Indica el inicio de la trama transmitida.

Dirección.- Siempre tiene un valor de 11111111 (dirección de *broadcast*[11]). No se utilizandirecciones individuales debido a que solo hay dos estaciones.

Control.- Indica si se realizacontrol de la trama.
Cuando se aplica control, se asignan números consecutivos a cada trama. Caso contrario se envía: 00000011 y se crea un servicio de enlace no orientado a conexión.

[11]*Broadcast*.- transmisión que será recibida por todos los dispositivos en la red

Protocolo.- Indica según su valor el tipo de protocolo transportado por PPP, así si los datos transmitidos pertenecen a IPX (*Internet Exchange*), *AppleTalk*, NCP (*Network Control*), LCP(*Link Control Protocol*), XNS(*Xerox Network Services*), OSI(*Open System Interconnection*), IP(*Internet Protocol*) o CLNP(*Connectionless Network Protocol*). Si el primer bit de este campo es 1_L, los datos pertenecen a otros protocolos que se negocian mediante NCP.

Los identificadores de protocolo están especificados en el RFC 1661.

Los más importantes son:

- 0x0021 para IP.
- 0xc021 para LCP.
- 0xc023 para PAP.
- 0xc223 para CHAP.

Datos.- Es la carga útil de tamaño variable puede ser hasta 1500 bytes.

FCS (*Frame Check Sequence*).- Detección de errores de transmisión, se necesita calcular el CRC[12] del contenido de la trama y colocarlo en el campo FCS. Para verificar, el receptor calcula el CRCde la trama que recibe y lo compara con el valor que recibe en el FCS. Si se obtienen valores diferentes se descarta la trama por poseerbits erróneos.Se puede utilizar FCS de 2 o de 4 bytes.

Bandera de Fin.- Valor constante que indica la terminación de la trama trasmitida.Para transmisiones síncronas se emplea la técnica del *bit stuffing*[13] .En una línea asíncrona, por el contrario, se utiliza 01111101 como caracter de escape. Cuando este byte aparece en la trama, el caracter que le siga debe tener el sexto bit complementado.

---

[12] CRC (comprobación de redundancia cíclica).

[13] *bit stuffing* (relleno de bits).- consiste en insertar un cero cada vez que se encuentran cinco unos seguidos en el campo de datos.

1.2.1.1.2 Protocolo de túnel Punto a Punto (PPPTP)

PPTP es un protocolo desarrollado por Microsoft, U.S. *Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics* conocidas colectivamente como PPTP *Forum.*

Es una extensión de PPP que soporta control de flujos y túnel multiprotocolo sobre IP; es sencillo y fácil de implementar siendo utilizadoampliamente para VPNs proveyendo acceso remoto. Su desventajaes que no provee una fuerte encriptación para proteger la información y tampoco soporta métodos de autentificación basados en *tokens*.

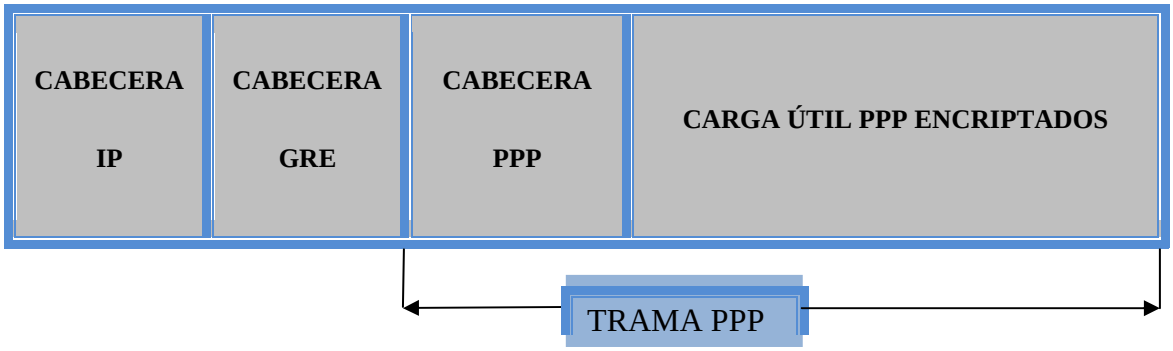


Figura 1.13 Trama PPTP

Protocolos utilizados por PPTP

a. **LCP (Protocolo de control de enlace)**. Da la posibilidad de actuar sobre variedad de ambientes, se lo utiliza para configurar, mantener y finalizar la conexión. Negocia: formatos de encapsulación, tamaño de paquetes, calidad del medio de transmisión.

b. **NCP (Protocolo de configuración de red)**. Se utiliza para la configuración de protocolos de red a ser utilizados. Luego de esta configuración los datagramas podrán ser enviados por el medio físico.

El protocolo más utilizado es el IPCP (*Internet Protocol Control Protocol*). Se encarga de la configuración, activación y desactivación de los módulos de IP en ambos extremos.

c. **GRE (Encapsulación genérica de ruteo)**. Este protocolo encapsula un paquete determinado dentro de un protocolo de transporte, el protocolo de transporte toma el paquete GRE y lo encapsula para su transmisión.

Seguridad PPTP

Existen tres áreas dentro de la seguridad:Autentificación, encriptación de datos y filtrado de paquetes PPTP.

Autentificación

Las cuentas de usuarios son configuradas para que sólo los usuarios específicos tengan acceso a la red a través del dominio de confianza. El uso de claves seguras es una de las mejores formas de autentificación exitosa del PPTP.

Encriptación de Datos

Se realiza en ambos sentidos de la transmisión, la información viaja encriptada por el túnel hasta ser desencriptada en el destino haciendo que los datos sean invisibles para el resto, dando un nivel adicional de seguridad.

Filtrado de Paquetes PPTP

Incrementa el rendimiento y fiabilidad de la seguridad de la red en el servidor PPTP.Acepta solo los paquetes PPTP de los usuarios autorizados,evitandoque el resto de paquetes entren en la VPN y en el servidor de PPTP.

1.2.1.1.3 Reenvío de capa 2 (L2F) (Layer 2 Forwarding)

Protocolo creadopor Cisco en las primeras etapas de desarrollo de las VPNs, para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas, utilizando PAP y CHAP para la autenticación de los usuarios remotos. Los túneles creados pueden soportar más de una conexión. Es capaz de encapsular los datos (PPP oSLIP[14]) que serán enviados a sus destinos.

Trabaja con un servicio de enlace llamado VDU[15], para acceder a la utilización de toda la infraestructura de Internet.

Existen dos niveles de autenticación del usuario:

- Autentifica el ISP[16](antes de establecer el túnel se debe autentificar)
- Autentifica después de conexión (se autentifica cuando se ha establecido la conexión con la pasarela corporativa)

El protocolo L2F requiere dos puntos a estandarizar:

- Encapsulamiento de los paquetes.- El ISP y los extremos deben negociar sobre qué paquetes encapsulará el protocolo.
- Administrador de conexión de L2F y MID[17].

Protocolos utilizados por L2F

a. **PAP (Protocolo de autenticación de *password*)**. Al establecer la conexión entre el servidor y el cliente, el cliente envía el nombre de usuario

[14]SLIP.- (*Serial Line Internet Protocol*) es un estándar de transmisión de datagrama IP, actualmente obsoleto.

[15]VDU.- (*Virtual Dial-Up)*

[16]ISP.- Proveedor de Servicio de Internet

[17]MID.- Dispositivo Móvil para conectividad a Internet

y contraseña para ser verificado, de ser aceptado se permite la conexión; de no ser aprobada se finaliza la conexión.

b. **CHAP (Protocolo de autentificación periódica del cliente)**. Una vez completada la conexión, el autenticador envía un mensaje de comprobación al usuario y *password;* el par responde con un valor calculado usando una función *hash*.Este valor es comparado con el que calcula el autenticador y si coinciden la comunicación continúa, caso contrario se cancela.

   Para esto se requiere que ambos extremos cuenten con la clave secreta.Esta tarea se repetirá aleatoriamente.

Formato general del paquete L2F

El paquete L2F encapsulado tiene la forma básica que se observa en la figura 1.14.

Figura 1.14 Trama L2F

1.2.1.1.4 Protocolo de Túnel de Capa 2 (L2TP) Layer 2 Tunneling Protocol

Se trata de un estándar abierto y disponible en la mayoría de plataformas: Windows, Linux, Mac, etc. Se implementa sobre IPSec y proporciona altos niveles de seguridad. Se pueden usar certificados de seguridad de clave pública para cifrar los datos y garantizar la identidad de los usuarios de la VPN.

Encapsula características PPTP y L2F como uno solo, resolviendo los problemas de interoperabilidad entre ambos protocolos. Permite el túnel del nivel de enlace de PPP, de forma que los paquetes IP, IPX y AppleTalk enviados de forma privada, puedan ser transportados por Internet.

Este protocolo posee un mecanismo para encapsular, que permite el transporte de diferentes protocolos a través de un enlace punto a punto provisto por un NAS[18] con ISDN, ADSL, PTSN en el extremo final. Combina las mejores características de los protocolos PPTP y L2F.

Permite trabajar con distintas redes como X25, ATM y también es capaz de trabajar con IPX o NETBEUI mejorando la limitación que se tenía en L2F. Puede ser utilizado sobre una WAN con *Frame Relay* sin necesidad de IP.

Requiere que haya conectividad entre los extremos del túnel orientado a paquetes. Puede ser utilizado en una red IP utilizando UDP.

L2TP permite la creación de múltiples túneles entre dos puntos, además de la posibilidad de crear distintos túneles para distintos QoS.

Formato del paquete L2TP

Se utilizan dos formatos de paquetes, dependiendode los mensajes que se desee enviar, éstos son:

- Mensajes de control.- se utilizan para: crear,mantenery eliminar túneles y llamadas utilizando un canal L2TP para garantizar la entrega de los mensajes.

[18]NAS.-Dispositivos de almacenamiento específicos a los que se accede desde los equipos a través de protocolos de red.

- Mensajes de datos.- se encapsulan en paquetes PPP que serán enviados por el túnel. En los mensajes de datos la entrega no está garantizada y en caso de que los mensajes se pierdan no serán reenviados.

En las figuras 1.15 y 1.16 se indíca como está compuesto un paquete L2TP, tanto para mensajes de datos como de control.

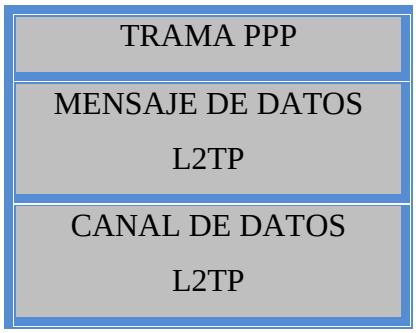


Figura 1.15 Formato del paquete L2TP (Mensaje de datos)

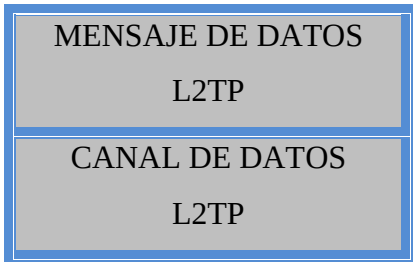


Figura 1.16 Formato del paquete L2TP (Mensaje de control)

1.2.1.2 Capa 3- Capa Red

Utiliza protocolos de túnel IPSec sobre IP. Este protocolo proporciona un canal seguro para los datos. Ofrece integridad, autenticación, control de acceso y confidencialidad para el envío de paquetes IP por Internet; especialmente utilizado para implementar VPN´s y conexiones de acceso remoto a redes privadas.

IPsec autentifica y encripta los datos añadiendo información en cada paquete de la capa de red que se transmite. IPsec se puede utilizar para encapsular cualquier tráfico de capa 3, pero no el tráfico de capas inferiores, por lo que no se podrá utilizar para protocolos no-IP o mensajes de *broadcast.* Su principal ventaja es

que puede ser usado prácticamente en cualquier plataforma existiendo una gran variedad de soluciones tanto de software como de hardware.

IPSec permite al usuario autentificar y/o cifrar cada uno de los paquetes IP. Al separar las aplicaciones de autentificación y encripción de paquetes, se definen a continuación las dos formas diferentes de usar IPSec a las que se denomina modos.

Modo Túnel. Todos los paquetes IP son encapsulados en un nuevo paquete y enviados a través del túnel siendo desencapsulados en el otro extremo y posteriormente dirigidos a su destinatario final. En este modo, se protegen las direcciones IP de emisor y receptor así como el resto de los datos de los paquetes.En la figura1.17 se muestra la trama IPsec en Modo túnel.

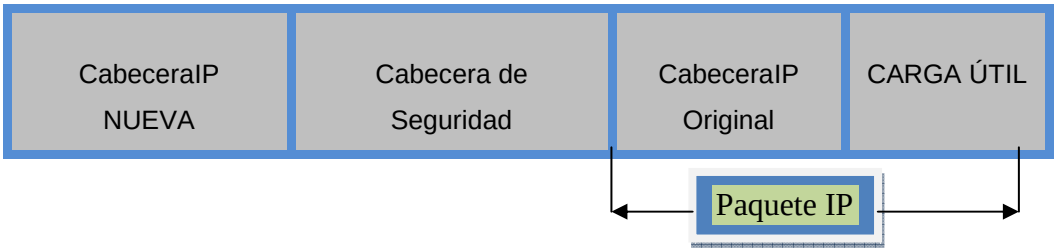


Figura 1.17 Trama IPsec- Modo Túnel

Modo Transporte. Solo la carga útil (payload) de la sección de datos es cifrada y encapsulada. La sobrecarga entonces, es sensiblemente menor que en el caso anteriorEn la figura 1.18 se puede observar la trama de IPsec en Modo transporte.

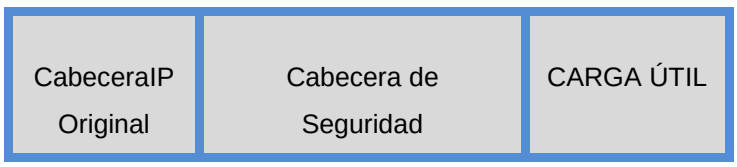


Figura 1.18 Trama IPsec- Modo Transporte

En la tabla 1.1 se indica la protección y peso que posee cada uno de los modos de la trama IPsec.

Modo IPsec	PROTEGE	PESO
Transporte	Datos	Sensiblemente menor que IP modo de Túnel
Túnel	Datos-Dirección	Sensiblemente mayor por proteger también la dirección

Tabla 1.1 **Comparación de Modo IP Transporte con IP Túnel**

Mientras que el modo de transporte es útil en muchas situaciones, el modo de túnel provee mayor seguridad contra ataques y monitoreos de tráfico que pueda ocurrir sobre la Internet.

1.2.1.3 Capa 7 – Capa Aplicación

También es posible establecer túneles en la capa de aplicación y de hecho son ampliamente utilizados hoy en día siendo algunas soluciones como SSL6 y TLS7. Existen otros productos como SSL-Explorer y algunos otros que ofrecen una combinación de gran flexibilidad, seguridad fuerte y facilidad de configuración. La seguridad se logra mediante cifrado del tráfico usando mecanismos SSL/TLS, los cuales han probado ser muy seguros y están siendo constantemente sometidos a mejoras y pruebas.

1.2.1.3.1 Protocolo Secure Sockets Layer (SSL)

Fue creado por la empresa *Netscape Communication* enla década de los 90. Es un protocolo criptográfico que proporciona: confidencialidad, autenticidad e integridad enuna comunicación cliente/servidor. Resulta muy flexible, ya que puede servir para seguridad potencialmente de otros servicios además de HTTP para Web, sin más que hacer pequeñas modificaciones en el programa que utilice el protocolo de transporte de datos TCP.

SSL proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, que puede elegirse entre DES(*Data Encryption Standard*), 3DES, RC2(Algoritmo de cifrado de flujo), RC4 o IDEA(*International Data Encryption Algorithm*), y cifrando la clave de sesión de los algoritmos anteriores mediante un algoritmo de cifrado de clave pública, (RSA comúnmente). La clave de sesión es la que se utiliza para cifrar los datos que vienen y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, permitiendo que a pesar de ser descifrada por un atacante en una transacción, no sirva para descifrar futuras transacciones.

MD5 o SHA se pueden usar como algoritmos de*hash*. La posibilidad de elegir entrevarios algoritmos hace a SSL muy flexible.

Durante el protocolo SSL, el cliente y el servidor intercambian una serie de mensajes para negociar las mejoras de seguridad.

1. Fasede saludo.-Sirve para ponerse de acuerdo quéalgoritmos criptográficos se van a utilizar.Se suelen utilizar los más fuertes en base a las posibilidades criptográficas del navegador; el servidor elegirá un conjunto u otro de algoritmos con una cierta longitud de claves.

2. Fase de autenticación.-El servidor envía al navegador su certificado que contiene su clave pública y solicita a su vez al cliente su certificado (sólo si la aplicación exige la autenticación de cliente).

3. Fase de creación de clave de sesión.-El cliente envía al servidor una clave maestra con la que se generará la clave de sesión para cifrar los datos intercambiados posteriormente, haciendo uso del algoritmo de cifrado simétrico acordado en la fase 1. El navegador envía cifrada esta clave maestra usando la clave pública del servidor que extrajo de su certificado en la fase 2. Posteriormente, ambos generarán idénticas claves de sesión a partir de la clave maestra generada por el navegador.

4. Fase Fin.-Se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente establecido. Una vez finalizada esta fase, ya se puede comenzar la sesión segura.

De ahí en adelante, durante la sesión segura abierta, SSL proporciona un canal de comunicaciones seguro entre los servidores Web y los clientes.

1.2.1.3.2 Protocolo *Transport Layer Security*(TLS)

El protocolo TLS es una evolución del protocolo SSL; establece una conexión segura por medio de un canal cifrado entre el cliente y servidor. Así el intercambio de información se realiza en un entorno seguro y libre de ataques.

Normalmente el servidor es el único que es autenticado, garantizando así su identidad, pero el cliente se mantiene sin autenticar, porque la autenticación mutua utiliza una infraestructura de claves públicas (o PKI) para los clientes.

Estos protocolos permiten: prevenir escuchas no autorizadas (*eavesdropping*), evitar la falsificación de la identidad del remitente y mantener la integridad del mensaje en una aplicación cliente-servidor.

Características de SSL

Seguridad criptográfica. El protocolo se debe emplear para establecer una conexión segura entre dos partes.

Interoperabilidad. Distintas aplicaciones deben poder intercambiar parámetros criptográficos sin necesidad de que ninguna conozca el código de la otra.

Extensibilidad. El protocolo permite la incorporación de nuevos algoritmos criptográficos.

Eficiencia. Los algoritmos criptográficos son costosos computacionalmente, por lo que el protocolo incluye un esquema de caché de sesiones para reducir el número de sesiones que deben inicializarse desde cero (usando criptografía de clave pública).

El protocolo TLS está dividido en dos niveles:

1. Protocolo de registro TLS (TLS *Record Protocol*).
2. Protocolo de mutuo acuerdo TLS (*TLS Handshake Protoco*l).

El protocolo de registroencapsula varios protocolos de más alto nivel, entre ellos el protocolo de mutuo acuerdo, permitiendo al servidor y al cliente autentificarse mutuamente y negociar un algoritmo de encriptación y sus claves antes de que el protocolo de aplicación transmita o reciba datos.

El Protocolo de Registro esimplementado sobre un protocolo de transporte fiable comoTCP, proporcionando seguridad en la conexión con dos propiedades:

a. La conexión es privada. Para encriptar los datos se usan algoritmos de cifrado simétrico. Las claves se generan para cada conexión y se basan en un secreto negociado por otro protocolo (como el de mutuo acuerdo). El protocolo también se puede usar sin encriptación.
b. La conexión es fiable. El transporte de mensajes incluye una verificación de integridad.

El protocolo de mutuo acuerdo proporciona seguridad en la conexión con tres propiedades básicas:

a. La identidad del interlocutor puede ser autentificada usando criptografía de clave pública. Esta autentificación puede ser opcional, pero generalmente es necesaria al menos para uno de los interlocutores.
b. La negociación de un secreto compartido es segura.

c. La negociación es fiable, nadie puede modificar la negociación sin ser detectado por los interlocutores.

1.3 CATEGORÍAS DE LAS VPNs

Estos últimos años gracias a la facilidad de poder trabajar desde cualquier lugar, inclusive desde el hogar, la rapidez y fiabilidad en las comunicaciones entre sucursales y oficinas centrales alrededor del mundo, es un parámetro crítico e importante para las organizaciones, donde los costos son un factor determinante, debido a esto se ha creado una gran cantidad de soluciones VPNs,que se han ido desarrollando como se puede apreciar en la figura 1.19

1.3.1 VPNsSEGÚN EL PUNTO DE TERMINACIÓN

Las VPNs según el punto de terminación son las siguientes:

- *Overlay* (Basadas en el CE)
- *Peer to Peer*(Basadas en el PE)

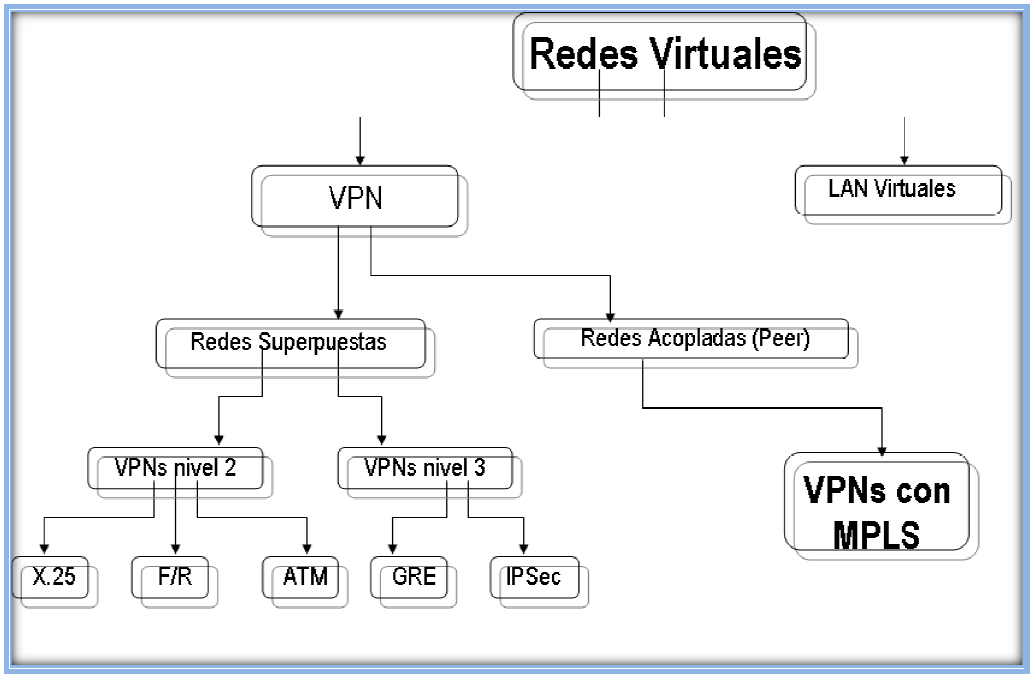


Figura1.19**Clasificación de las VPNs**[13]

1.3.1.1 VPN *Overlay*

Mediante la VPN se crea una simulación de línea dedicada utilizando un circuito virtual, que puede ser a base de: PVC[19] o SVC[20]. Son totalmente transparentes para el proveedor del servicio, que desconoce la estructura interna de red del cliente como se puede observar en las figuras 1.20a y 1.20b.

Las VPNs*Overlay* utilizan protocolos orientados a conexión y se pueden implementar utilizando tecnología de Nivel 1(ISDN, E1, T1, DS0), Nivel 2 (X.25, FR, ATM) y de nivel 3 (IP SEC, GRE).

Existen alternativas *Overlay*: túneles IP-IP como GRE o IPSec.

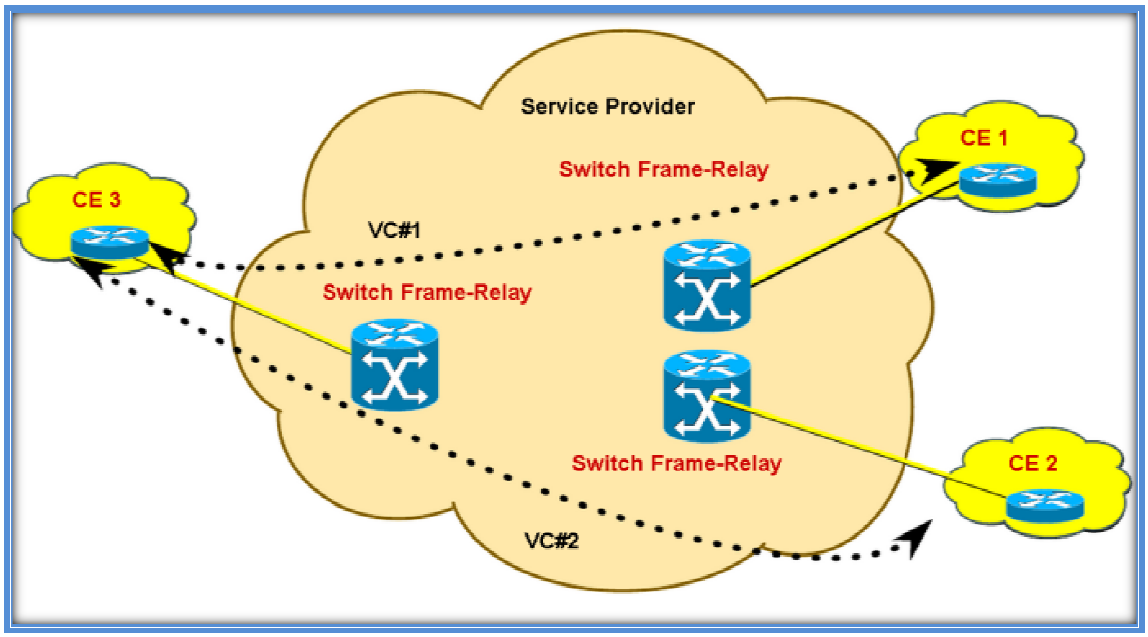


Figura 1.20aVPN *OVERLAY*[14]

[19]PVC.- Circuito Virtual Permanente

[20]SVC.- Circuito Virtual Conmutado

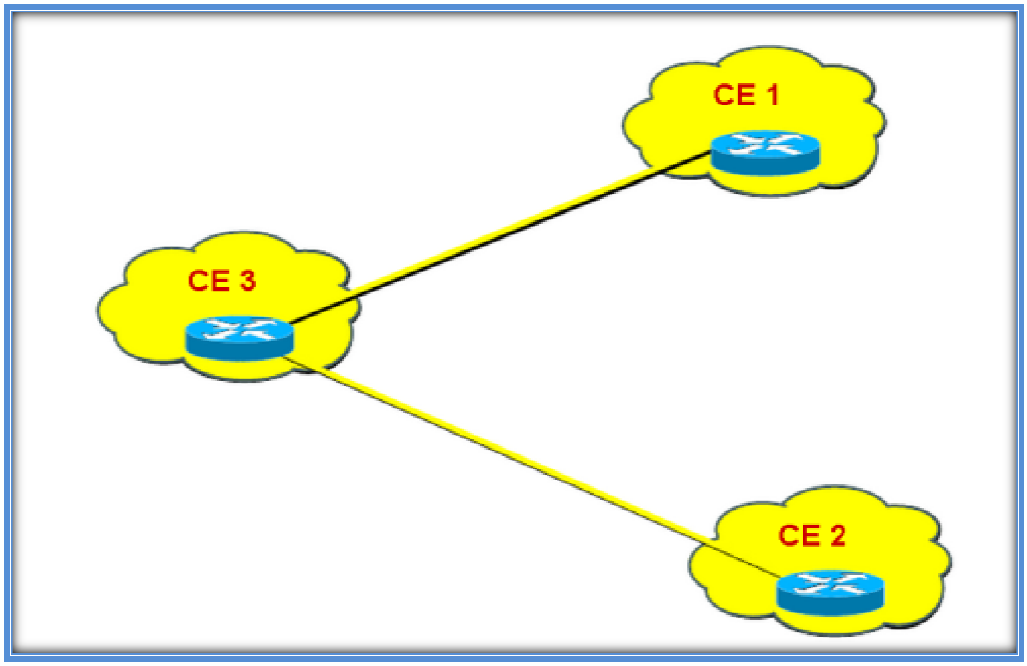


Figura 1. 20bVPN *OVERLAY*[15]

En la tabla 1.2 se indica las ventajas y desventajas que pueden ocurrir al utilizar una VPN Overlay

VENTAJAS	DESVENTAJAS
SIMPLES (separación entre el proveedor y el cliente)	Los VC se realizan manualmente
Los protocolos no dependen del soporte del proveedor	Existe *full mesh* por lo que no hay optimización del *routing*
Fácil de implementar.	Escalabilidad: Es complicado agregar nuevos sitios a la red
Permite la duplicidad de direcciones	Exigen al Proveedor del Servicio mayores costos operacionales y de administración, debido a que se introduce complejidad adicional en las VPNs de Nivel 2

Tabla 1.2 Ventajas y Desventajas de las VPNs Overlay

1.3.1.2 VPN *Peer to Peer*

Las VPNs*Peer-to-Peer* surgen como alternativa para solucionar varios de los problemas (desventajas) de las redes OVERLAY.

En el modelo que se muestra en la figura 1.21, se puede apreciar los circuitos virtuales en los cuales el PE es un *router* que intercambia información de ruteo directamente con el CE, interviniendo en la tabla de ruteo.

En la tabla 1.3se indica las ventajas y desventajas que pueden ocurrir al utilizar una VPN *Peer-to-peer*

VENTAJAS	DESVENTAJAS
Cada CE intercambia información de enrutamiento con un único (o unos pocos) PE.	No se pueden duplicar IPs, El Proveedor debe tener un plan de numeración IP para las VPN de los clientes.
El PE solo conoce la información de las VPNs conectadas	Desaparecen las ventajas de seguridad y aislación que existe en: las líneas dedicadas o el modelo *overlay*
Enrutamiento óptimo entre CE	Puede estar limitada la elección de protocolos de enrutamiento.
Más sencillo de dimensionar en ancho de banda	El proveedor de servicio necesita una información detallada sobre el enrutamiento IP.
Se pueden agregar nuevos sitios a la VPN con mayor facilidad	

Tabla 1.3 Ventajas y desventajas de la implementación de VPN`*s peer to peer*

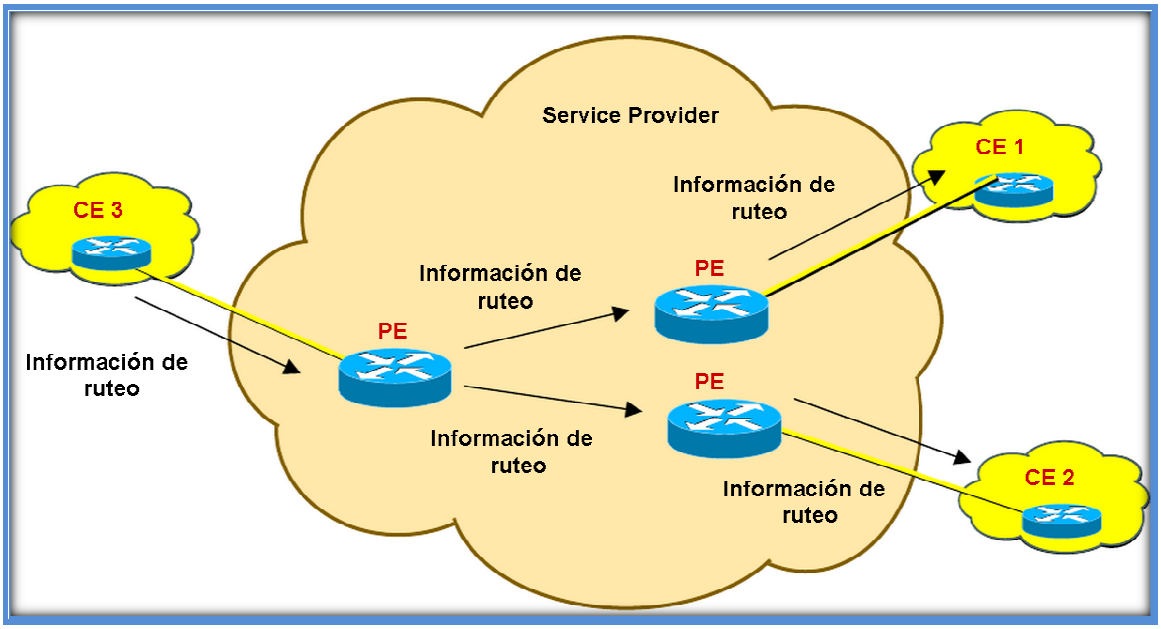


Figura 1.21 VPN *Peer to Peer*[16]

1.3.2 VPN Según el tráfico de cliente transportado

Las VPNs según su tráfico son las siguientes:

- VPN de nivel 2
- VPN de nivel 3

1.3.2.1 VPN de nivel 2

Proporcionan un servicio de transporte multiprotocolo sobre infraestructura de nivel 2, no existe aún una solución estándar y las soluciones existentes se basan en túneles sobre MPLS.[17]

Utiliza PVCs con encaminamiento basado en DLCI[21], los mismos que no proporcionan autenticación ni cifrado; su escalabilidad y flexibilidad son limitadas.

---

[21] DLCI (*Data Link Connection Identifier).*-Identificador de canal de circuito establecido en *Frame Relay,* se aloja en la trama e indica el circuito virtual establecido.

1.3.2.2 VPN de nivel 3

Las VPNs de Nivel 3 usan túneles GRE y sobre todo IPSec, cuentan con autenticación y cifrado de los datos en Internet con encaminamiento basado en IP del túnel.[18]

1.3.3 VPN SEGÚN EL NÚMERO DE SEDES CONECTADAS

Las VPNs según el número de sedes conectadas son las siguientes:

- Punto a punto: 2 sedes
- Multipunto: más de dos sedes

1.3.4 VPN SEGÚN LA TECNOLOGÍA DE TÚNELES

Las VPNs según la tecnología de túnel son las siguientes:

- Túneles IPSec, L2TP, PPTP, MPLS-LSP, ATM-VP/VC,
- Frame Relay VC, SONET/SDH VT, PPP/*Dial-up*

1.3.4.1 Túnel IPsec

La seguridad del tráfico de paquetes se proporciona a varias computadoras, puede incluso dar seguridad a toda la LAN por un único nodo.

1.3.4.1.1 Redes Ruteadas Privadas Virtuales (VPRNs, Virtual PrivateRouted Networks)

Simulan redes dedicadas de enrutadores IP entre los sitios de los clientes; aunque una VPRN transporte tráfico IP, ésta debe ser tratada como un dominio de enrutamiento separado desde la subyacente red del SP[22], ya que VPRN es

[22]SP.- Proveedor del servicio

probablemente usada por varios clientes asignando direcciones IP. Cada cliente se ve el mismo como el operador de la red y por lo tanto puede asignar las direcciones IP de la manera que desee.

1.3.4.1.2 Redes Conmutadas Privadas Virtuales (VPDNs, Virtual PrivateDial Networks)

Permite a los clientes que el SP le aprovisione y gestione los accesos conmutados a su red. En lugar de cada cliente configurar sus propios 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 acceso compartidos. Usando túneles desde el servidor de acceso del SP hasta un punto de acceso dentro de la red del cliente, se transportan secciones PPP para cada VPDN conocido como concentrador de acceso.

1.3.4.2 Túnel L2TP

Se crea encapsulando una trama L2TP en un paquete UDP, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Es el protocolo de encapsulamiento más externo IP, los protocolos IPSec pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.

1.3.5 VPN SEGÚN EL ALCANCE

Las VPN pueden dividirse en tres categorías según el alcance para la organización:

1.3.5.1 VPN de Acceso Remoto

Es una de las más utilizadas actualmente, debido a la necesidad que existe de mantenerse conectados a la empresa desde sitios remotos (oficinas comerciales,

domicilios, hotel, salas de esperas de aeropuertos, etc.), utilizando Internet como vínculo de acceso.

Al utilizar autenticación se consigue un nivel de acceso similar a estar directamente enlazado a la LAN de la empresa. El acceso puede ser mediante: líneas analógicas, digitales, RDSI o DSL.

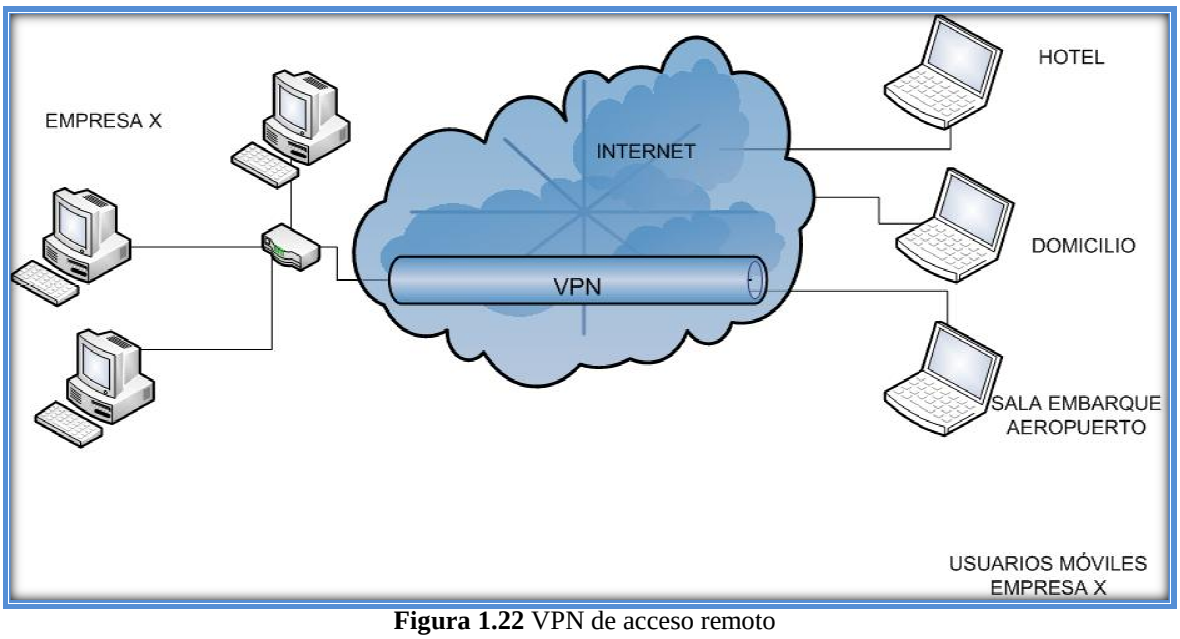


Figura 1.22 VPN de acceso remoto

En la figura 1.22se puede ver cómo un usuario que posee conexión a Internet establece una VPN con la LAN de la empresa desde los diferentes escenarios posibles.

1.3.5.2 VPN de Intranet

Se realiza para interconectar departamentos o dependencias de una misma empresa; generalmente son redes que requieren un alto nivel de aislamiento y seguridad, así como garantías de calidad de servicio para aplicaciones críticas. Por estas razones no muchas organizaciones utilizan Internet para este tipo de VPN. Las VPN de Intranet han sido generalmente implementadas con tecnologías tradicionales como X.25, *Frame Relay* o ATM, es decir utilizan la propia red como medio de conexión.

Es muy común implementar VPNs de Intranet en redes LAN inalámbricas.

En la figura 1.23 se indica como varios departamentos de la empresa “X” estan interconectados mediante una VPN

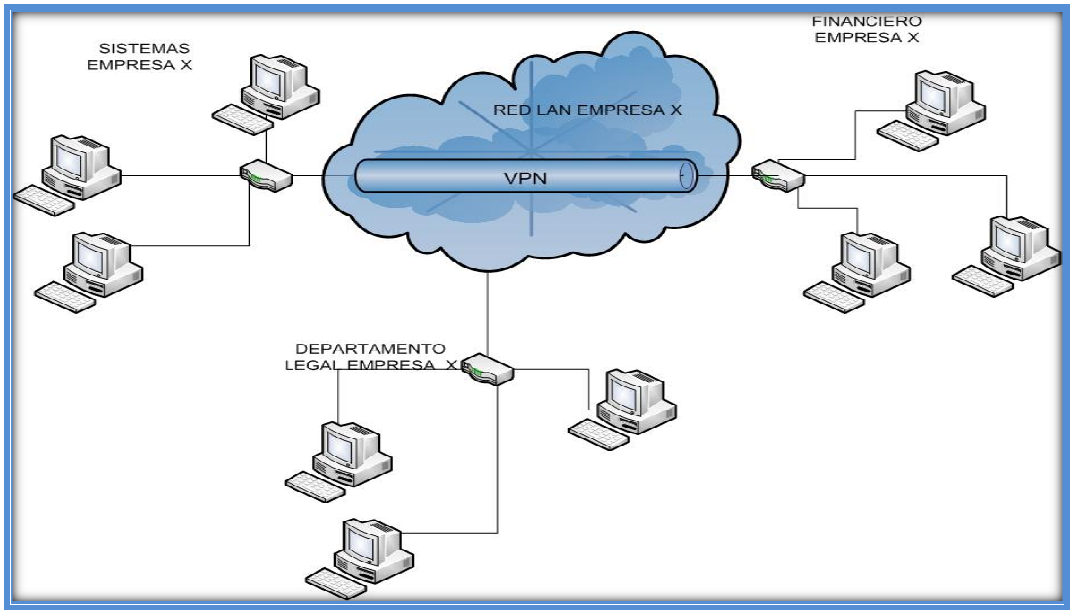


Figura 1.23 VPN de Intranet

1.3.5.3 VPN de Extranet

Las VPNs de Extranet se utilizan para interconectar diferentes sitios ubicados en diversas zonas geográficas de una organización, o diferentes organizaciones. Esta configuración presenta menos requerimientos de calidad de servicio y hace al Internet más adaptable para este tipo de VPN. (figura 1.24)

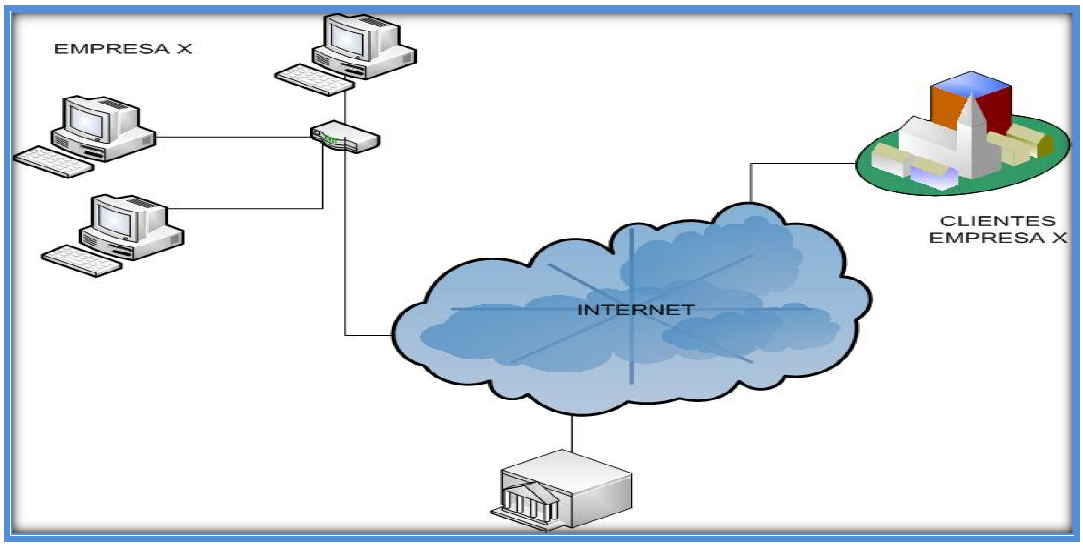


Figura 1.24VPN de Extranet

1.4 TIPOS DE SEGURIDAD QUE SE PUEDEN UTILIZAR EN LA TRANSMISIÓN DE DATOS

1.4.1 ENCRIPTACIÓN

La criptografía es el estudio del cifrado y descifrado de la información mediante técnicas matemáticas que hagan posible el intercambio de mensajes de tal forma que sólo puedan ser leídos por las personas a quienes van dirigidos.[19]

La criptografía entre otras presenta las siguientes características:

- Garantiza la privacidad de los datos transmitidos en la comunicación.
- Asegura la confiabilidad de la información transmitida, así como la autenticación en los dos sentidos, verificando al emisor y al receptor, que sea realmente quien dice ser, yque la información que se envía sea auténtica (habitualmente denominado criptograma)esto es que, no haya sido modificada en su tránsito.

Cabe resaltar que solo se protege los datos y no la cabecera.Para la encriptación de información se utilizan complejos algoritmos matemáticos, los más usados son: DES, 3DES, AES, RSA, IDEA.

1.4.1.1 Algoritmo de Encriptación DES (*Data Encription Standard*)

Es un estándar de encriptación de datos del gobierno de Estados Unidos, consiste encifrar bloques de 64 bits con una clave de 56 bits. Se proporciona 64 bits para la clave, sin embargo el bitmenos significativo de cada byte de la clave no se usa para el cifrado y podría ser utilizado como bit de paridad.

En la figura 1.25 se indica como está compuesta la clave de 64 bits de algoritmo DES

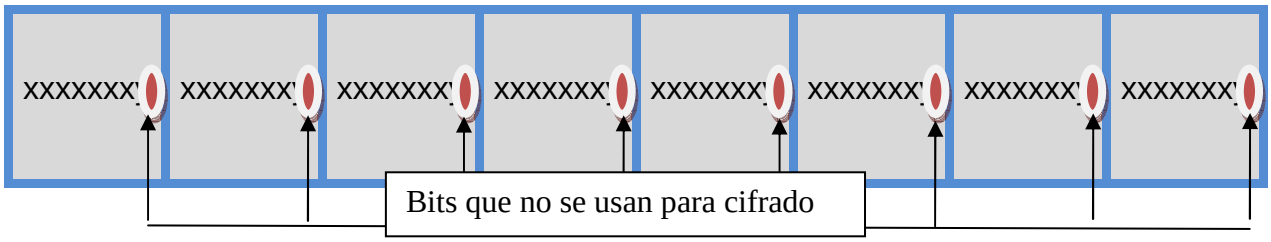


Figura 1.25 Clave de 64 bits del algoritmo DES

1.4.1.2 Algoritmo de Encriptación 3DES (Triple DES)

Cuando se descubrió que una clave de 56 bits no era suficiente para evitar un ataque de fuerza bruta, 3DES fue elegido como forma de agrandar la longitud de la clave sin necesidad de cambiar de algoritmo de cifrado,fue desarrollado por IBM en 1978.Utiliza bloques de datos de 64 bits, los cuales son cifrados con DES usando una clave K1, después descifrados usando K2, y finalmente cifrados de nuevo usando K1. Esto aumenta el tamaño de clave a 112 bits (8 bits de K1 y 8 bits de K2 son descartados por PC1), lo cual dificulta el ataque de fuerza bruta. Pero en cambio es preciso triplicar el número de operaciones de cifrado, haciendo este método de cifrado muchísimo más seguro y lento a la vez.

3DES ha sido paulatinamente reemplazado por el algoritmo AES. Sin embargo, la mayoría de las tarjetas de crédito y otros medios de pago electrónicos lo mantienen como estándar.

1.4.1.3 Algoritmo de Encriptación AES (*Advanced Encryption Standard*)

Utiliza un tamaño de bloque de 128 bits y la clave puede ser de: 128, 192 o 256 bits. Técnicamente es mejor que 3DES.

El cifrado consiste de una operación básica llamada ronda[23] que se repite un número de veces. Significa que el cifrado está compuesto de una serie de sustituciones y permutaciones que se suceden unas a otras.El número de rondas en AES depende del tamaño de la clave:

[23]Ronda.- Son las repeticiones de los cuatro pasos para lograr la encriptación.

- 10 rondas para 128bits
- 12 rondas para 192 bits
- 14 rondas para 256 bits

AES trabaja sobre una estructura conocida como el estado AES; esuna reordenación del bloque en una matriz de 4×4. Además, la mayoría de las operaciones de AES se pueden describir como operaciones en el cuerpo finito[24]. Esto le proporciona a AES una descripción algebraica bastante sencilla.

AES puede llegar a ser hasta 6 veces más rápido, y hasta ahora no se ha encontrado ninguna vulnerabilidad.

1.4.1.4 Algoritmo de Encriptación RSA

Es un algoritmo asimétrico para cifrar bloques, que utiliza una clave pública. El algoritmo fue descrito en 1977 por Ron Rivest, Adi Shamir y Len Adleman; las letras RSA son las iniciales de sus apellidos.

1.4.1.5 Algoritmo de Encriptación IDEA (*International Data Encryption Algorithm*)

"La codificación se hace mediante un proceso que se conoce como encripción, que manejan algoritmos sofisticados que solo pueden ser interpretados por servidores Web y visores de Internet que soporten el mismo protocolo de encriptación" [20]

1.4.2 ENCAPSULAMIENTO

Al realizar encapsulamiento se encriptan: los datos y la cabecera, luego se coloca una nueva cabecera utilizando protocolos como: IPSec y L2TP.

---

[24]Esuna estructura algebraica en la cual para las operaciones de adición y multiplicación ,existe un inverso aditivo y un inverso multiplicativo, que permiten efectuar las operaciones de sustracción y división (excepto la división por cero), posee un número finito de elementos

“Es necesario que el mismo protocolo se utilice en ambos lados para poder codificar en el lado emisor y decodificar en el lado receptor.”[21]

1.4.3 AUTENTICACIÓN

Autenticación es un proceso que determina si una persona está autorizada a enviar o recibir información.

En una red privada y pública, la autenticación se desarrolla comúnmente a través de claves de acceso (*passwords*) que pueden ser: asignadas o autodeclaradas; con su conocimiento se presume que el usuario es auténtico y puede acceder a la red.

1.4.3.1 Algoritmos de *Hashing*

Para garantizar que los datos no han sido modificados en el trayecto se pueden usar algoritmos de *hashing* que generen claves. Los más utilizados son: SHA, MD4, MD5.

Hash.-Método con el cual se generan claves o llaves para representar de manera única a un documento. Es un algoritmo unidireccional, solo encripta no puede desencriptar lo que se ha encriptado.

1.4.3.2 SHA (*Secure Hash Algorithm*)

SHA es un sistema de funciones *hash* criptográficas relacionadas y publicadas por el *National Institute of Standards and Technology* (NIST).SHA fue oficialmente publicado en 1993. Muchas veces se lo llama no oficialmente SHA-0 para evitar confusiones con SHA-1 que fue publicada 2 años después.

SHA crea una salida resumen (información cifrada) de 160 bits (20 bytes), el mensaje puede tener un tamaño máximo de 264 bits.

SHA1 es muy común para los desarrolladores en .net, para crear un sitio web, y proveer una clave segura de usuarios mediante un método de criptografía. Haceque una cadena de texto de cualquier longitud se convierta en una cadena de40 caracterescon cifrando, este método no tiene reversa.

1.4.3.3 MD4 (*Message-Digest Algorithm* 4)

MD4 es un algoritmo de resumen del mensaje (el cuarto en la serie). Implementa una función criptográfica *hash* para el uso en comprobaciones de integridad de mensajes.

1.4.3.4 MD5 (*Message-Digest Algorithm* 5)

MD5 fue diseñadopara verificar la integridad de los datos. Es un algoritmo criptográfico que toma como entrada una cadena de cualquier longitud y genera una cadena arbitraria de 128 bits; es ampliamente utilizadoal descargar archivos grandes de la web,encontrando en ellos *hash* o *fingerprint* MD5. Una vez descargado, se aplica el algoritmo MD5 sobre el archivo de la PC, y si el *hash* resultante coincide con el *hash* del archivo original significa que ambos son idénticos (con una probabilidad de error infinitesimal). Sirve para asegurarse que los datos no han sido manipulados durante su transmisión, o no se ha producido algún error durante dicha transmisión.

1.4.3.5 HMAC (*Hash-base del Código de autenticación de mensajes)*

HMAC fue publicado por primera vez en 1996 por *Mihir Bellare, Ran Canetti, y Hugo Krawczyk.* FIPS PUB 198 generaliza y normaliza el uso de HMAC.

La autenticación de mensajesse realiza mediante la construcción de un mensaje código de autenticación MAC, basado en funciones criptográficas*hash* que se conoce comoHMAC.El propósito de un MAC es la de autenticar la fuente del mensaje y su integridadsin el uso de mecanismos adicionales. HMAC se utiliza

para verificar simultáneamente la integridad de los datos y la autenticidad de un mensaje.

Cualquier otra función *hash* criptográfica, como MD5 o SHA-1, se puede utilizar en el cálculo de un HMAC, el resultado se denomina algoritmo de MAC HMAC-MD5 o HMAC-SHA1 en consecuencia. La fuerza criptográfica de HMAC depende de la fuerza criptográfica de la función *hash* empleada.[22]

1.4.3.6 EAP (*Extensible Authentication Protocol*)

EAP fue diseñado para utilizarse en la autenticación para acceso a la red, sin necesidad de tener conectividad IP; solamente provee el suficiente soporte para el transporte confiable de protocolos de autenticación.Es una estructura de soporte, no un mecanismo específico de autenticación, aunque provee algunas funciones comunes y negociaciones para los mecanismos de autenticación,estos mecanismos son llamados métodos EAP.

EAP solamente soporta un solo paquete en transmisión. EAP no puede transportar eficientemente datos robustos, a diferencia de protocolos de capas superiores como TCP.

EAP provee soporte para retransmisión, aunque no soporta control de orden de recepción de tramas, ni fragmentación y re-ensamblaje;el ordenamiento de paquetes se asume que es brindado por las capas inferiores.

1.4.3.7 CHAP (*Challenge Handshake Authentication Protocol*)

CHAP(Protocolo de autenticación por desafío mutuo) es un método de autentificación remota o inalámbrica, empleado por diversos proveedores de servicios, que verifica periódicamente la identidad del cliente remoto usando un intercambio de información. La verificación se basa en un secreto compartido.

Pasos para la verificación de Identidades:

1. Una vez establecido el enlace, el autentificador solicita la verificación del usuario.

2. El usuario envía un valor calculado usando una función *hash* de un solo sentido, como la suma de comprobación MD5.

3. El autentificador compara la respuesta con su propio cálculo de la función *hash*. Si el valor concuerda, se informa la verificación, de lo contrario se termina la conexión.

4. Aleatoriamente el autentificador verifica al usuario, repitiendo el proceso.

CHAP protege contra los ataques de REPLAY mediante el uso de un identificador que se va incrementando y un valor de verificación variable.

1.4.3.7.1 MS CHAP

MS-CHAP fue creado por Microsoft,para autenticar estaciones de trabajo remotas, integrando la funcionalidad a la que los usuarios de redes LAN están habituados con los algoritmos *hash* utilizados en las redes Windows. MS-CHAP utiliza un mecanismo de desafío y respuesta para autenticar conexiones sin enviar contraseñas.

MS-CHAP utiliza el algoritmo *hash*MD4 y el algoritmo de cifrado DES, para generar el desafío y la respuesta; posee mecanismos para informar acerca de errores de conexión y para cambiar la contraseña del usuario.

1.4.3.7.2 MS CHAP versión 2

Windows Server 2003 posee MS-CHAP v2, que proporciona autenticación mutua, la generación de claves de cifrado de datos iniciales más seguras para cifrado punto a punto de Microsoft (MPPE) y distintas claves de cifrado para los datos enviados y los datos recibidos. Para reducir al mínimo el riesgo de que una contraseña se vea comprometida durante su cambio, no se admiten métodos más antiguos que el cambio de contraseña de MS-CHAP.

1.4.3.8 SPAP (*Shiva Password Authentication Protocol*)

El Protocolo de autenticación de contraseñas de Shiva, es un protocolo de autenticación simple, de contraseña cifrada, compatible con servidores de acceso remoto de *Shiva*.

El cliente de acceso remoto envía una contraseña cifrada al servidor de acceso remoto, utilizando un algoritmo de cifrado bidireccional. El servidor de acceso remoto descifra la contraseña y utiliza el formato sin cifrar para autenticar al cliente de acceso remoto.

1.4.3.9 PAP (*Password Authentication Protocol*)

Es un protocolo de autenticación simple en el que el nombre de usuario y la contraseña se envían al servidor sin cifrar para ser verificada, al ser aceptado el cliente se permite la conexión; De no aprobarse al cliente se finaliza la conexión.

PAP se lo utiliza para conectar a servidores de acceso remoto antiguos basados en UNIX que no admiten métodos de autenticación más seguros.

1.4.3.10 Grupo *Hellman*

Se utilizan para determinar la longitud de los números primos base, utilizados durante el proceso de intercambio de claves. La eficacia criptográfica de cualquier clave derivada depende en parte de la eficacia del grupo Diffie-Hellman en el que se basan los números primos.

El grupo 2048 es más eficaz que el grupo 2, y a la vez es más eficaz que el grupo 1. A continuación se detallan los bits de protección de clave por cada grupo:

El grupo 1 proporciona 768 bits
El grupo 2 proporciona 1024 bits
El grupo 2048 proporciona 2048 bits.

Los interlocutores tienen que mantener grupos coincidentes para que sea posible la negociación. El grupo no se puede cambiar durante la negociación.

El grupo *Diffie-Hellman* se configura como parte de las opciones de intercambio de claves del modo principal. Las nuevas claves de sesión generadas en el modo rápido se obtienen a partir del material de clave principal del modo principal Diffie-*Hellman*, salvo en el caso de que esté habilitada la confidencialidad directa perfecta (PFS) de clave principal o de clave de sesión. Si está habilitada PFS de clave principal o de clave de sesión, tendrá lugar un nuevo intercambio Diffie-*Hellman* para obtener nuevo material de generación de claves cada vez que sea necesaria una nueva clave de sesión. La diferencia entre PFS de clave principal y PFS de clave de sesión estriba en que la primera requiere volver a autenticar la asociación de seguridad de modo principal además del intercambio *Diffie-Hellman.*

El *fingerprint* resultante tiene una longitud fija, independiente del tamaño del mensaje de entrada.[25]Es muy fácil identificar cuando se producen errores en la transmisión, por lo diferente de su *hash* MD5.

1.4.4 AUTORIZACIÓN

Los usuarios dependiendo de su autorización pueden acceder a los recursos, según los perfiles asignados a cada uno de ellos.

1.4.5 CONFIDENCIALIDAD

Los datos viajan a través de Internet, considerado un medio inseguro, haciéndolos susceptibles de interceptación, por lo que es fundamental el cifrado de los mismos.De este modo, la información no puede ser interpretada por nadie más que los destinatarios.

1.5 REQUERIMIENTOS BÁSICOS DE UNA VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que ésta proporcione[23]:

- Identificación de usuario
- Administración de direcciones
- Codificación de datos
- Administración de claves
- Soporte a protocolos múltiples

1.5.1 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

[25]*Fingerprint.*-se refiere a la autentificación única, similar a una huella digital.

proporcionar registros estadísticos que muestren: quien accesó, qué información y cuándo.

1.5.2 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.

1.5.3 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.

1.5.4 ADMINISTRACIÓN DE CLAVES

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

1.5.5 SOPORTE A PROTOCOLOS MÚLTIPLES

Las VPNs deben tener capacidad de manejar los protocolos utilizados en la red pública(protocolo de internet (IP), el intercambio de paquete de internet (IPX) entre otros).

CAPÍTULO 2. ESTUDIO DE LAS ALTERNATIVAS DE IMPLEMENTACIÓN DE UNA VPN

2.1 IMPLEMENTACIÓN MEDIANTE SOFTWARE

Actualmente las implementaciones de VPNs mediante Software son muy comunes, debido a sus mínimos requerimientos. Entre las más utilizadas se tienen:

- VPN Windows Server 2003
- VPN LogMeIn Hamachi

2.1.1 USOS DE LA VPN MEDIANTE SOFTWARE

- **Crearuna LAN en Internet**. La cual sea segura y exclusiva para varios usuarios, como si estuvieran conectados mediante un cable físico.
- **Tener Acceso remoto**. Controlar remotamente cualquier máquina de la red mediante un escritorio remoto.
- **Acceso a unidades de red y archivos**. Acceder a los archivos y a las unidades de red más importantes o necesarias para cumplir con las necesidades de los usuarios.
- **Seguridad**.Mediante cifrado y autenticación propia del programa.

2.1.2 VPNs WINDOWS SERVER 2003

La VPN con Windows Server 2003 es una ampliación de la red privada,siendo creadasobre redes públicas.La VPN de acceso remoto y de enrutador a enrutador se implementa mediante protocolos PPTP o L2TP y cuenta con seguridad IPSec.

Existen dos ediciones de *Windows Server* 2003,*Web Edition* y *Standard Edition*, en ambas se pueden crear hasta 1000 puertos del Protocolo de túnel PPTP y hasta 1000 puertos del Protocolo de túnelL2TP.

- Windows Server 2003*Web Edition*solo puede aceptar una VPN cada vez.
- Windows Server 2003*Standard Edition*, puede aceptar hasta 1000 conexiones VPN simultáneas.

2.1.2.1 Consideraciones básicas para instalación de una VPN

Para la instalación de una VPN se debe tener en cuenta las siguientes consideraciones:

- ***Firewall* deWindows.**- Configurar la característica Servidor de seguridad básico de Enrutamiento y acceso remoto al instalar la VPN, éste remplazará al *firewall* de Windows que debe mantenerse deshabilitado.

- **Conexión compartida a Internet**.-Se debe mantener deshabilitada en el servidor que se configurará la VPN: Enrutamiento y acceso remoto,debido a la incompatibilidad.

- **Asistente para configuración de seguridad**.- Está instalado y se debe mantener habilitado

- **Interfaz de red**.- Se debe determinar la interfaz de red que se desea utilizar para conectar a Internet y la que se conectará a la VPN. Al momento de la instalación se debe elegir la interfaz de red que se coloca en un computador para conectar a Internet, ésta debe ser la correcta o si no el servidor VPN de acceso remoto no funcionará adecuadamente.

- **Direcciones IP.-** Las direcciones IP de los clientes remotos pueden ser asignadas de dos maneras:

- Disponerde un servidor DHCP[26]en la VPN, éste concederá hasta 10 direcciones IP a la vez, y las asignará a los clientes remotos.
- No disponer de un servidor DHCP en la VPN, el servidor VPN de acceso remoto puede generar y asignar direcciones IP a los clientes remotos de forma automática. Para que el servidor VPN de acceso remoto asigne direcciones IP dentro de un rango se debe especificarlo.

Nota: Al configurar un servidor de RRAS, debe determinar si el servidor de acceso remoto utilizará el Protocolo de configuración dinámica de host (DHCP) o un conjunto de direcciones IP estáticas para obtener las direcciones de los clientes de acceso telefónico. Si utiliza un conjunto de direcciones IP estáticas, debe determinar si el conjunto será de intervalos de direcciones que son un subconjunto de direcciones de la red IP a la que está conectado el servidor u otra subred aparte. Si los intervalos de direcciones del conjunto de direcciones IP estáticas representan a otra subred, asegúrese de que las rutas de los intervalos de direcciones existen en los enrutadores de la intranet, para que el tráfico hacia los clientes de acceso remoto conectados se reenvíe al servidor de acceso remoto.

- **Autenticación de los Clientes VPN**.- Existen dos formas de autentificar a los clientes VPNs.

  - Mediante un servidor RADIUS[27].Es útil un servidor RADIUS cuando se desea instalar varios servidores VPN de acceso remoto, puntos de acceso inalámbrico u otros clientes RADIUS en la red privada.
  - Mediante el servidor Autenticación de VPN de acceso remoto que se encuentra configurado.

[26]DHCP.- Protocolo dinámico de configuración de *host*

[27]RADIUS.-*Remote Authentication dial In User Service*

- **Envío de mensajes DHCP de los clientes VPN**.- En el caso de que se desee que los clientes VPN envíen mensajes DHCP al servidor DHCP de la VPN, para lo cual hay dos consideraciones.
    - Si el servidor DHCP se encuentra en la misma subred que el servidor VPN de acceso remoto, los mensajes DHCP de los clientes VPN podrán alcanzar el servidor DHCP una vez establecida la conexión VPN.
    - Siel servidor DHCP está situado en una subred distinta de la del servidor VPN de acceso remoto, el enrutador entre ambas subredes debe retransmitir mensajes DHCP entre los clientes y el servidor. Si el enrutador ejecuta un sistema operativo Windows Server 2003, podrá configurar el servicio de Agente de retransmisión DHCP en el enrutador para reenviar mensajes DHCP entre las subredes.

- **Disponibilidad de cuentas de usuario**.- Los usuarios que desean acceder a la red, deben tener cuentas de usuario en el servidor VPN de acceso remoto o en *Active Directory*. Todas las cuentas de usuario situadas en servidores independientes o controladores de dominio contienen propiedades que determinan si el usuario se puede conectar.

2.1.2.2 Requerimientos para crear una VPN mediante Windows Server 2003

Los requerimientos para crear una VPN utilizando Windows Server 2003 son los siguientes:

- Un servidor con Windows Server 2003
- Computador configurado L2TP / IPsec
- Acceso a Internet

2.1.2.3 Parámetros de diseño de la VPN de acceso remoto[1]

Al diseñar una VPN, la seguridad es uno de los parámetros más importantes; depende de la seguridad del servidor VPN de acceso remoto,que debe estar

configurado correctamente, el ofrecer seguridad óptima cubriendo las necesidades de la red. Debe disponer de dos interfaces de red, una con conexión a Internet y otra con conexión a la red privada. La conexión a Internet debe ser una conexión dedicada con suficiente ancho de banda para que los usuarios VPNspuedan conectarse a la red privada y los usuarios de la red privada conectarse a Internet.

Para implementar conexiones VPN de acceso remoto se deben considerar los siguientes parámetros:

1. **Tipo de conexión.-**Se puede elegir entreconexiones L2TP/IPSec o basadas en PPTP.
   - PPTP se puede utilizar con una variedad de clientes de Microsoft, (Windows 95, 98, Millennium Edition, NT 4.0,2000 y XP). PPTP no necesita infraestructura de claves públicas para emitir certificados de equipo. Contiene cifrado, proporcionando confidencialidad de los datos. PPTP no proporciona integridad de los datos, ni autenticación del origen de datos.
   - L2TP sólo se puede utilizar con equipos cliente que ejecuten Windows 2000 o XP. Admite como autenticación para seguridad de protocolo IPsec certificados de equipo o una clave previamente compartida. El método de autenticación recomendado es autenticación de certificados de equipo; requiere una clave pública para emitir certificados de equipo al servidor VPN y a todos los equipos cliente VPN. Mediante IPSec, las conexiones VPN L2TP/IPSec proporcionan confidencialidad, integridad y autenticación de los datos.

2. **Instalar certificados**

   Si se desea crear VPN de acceso remoto L2TP/IPSec utilizando la autenticación mediante certificados de equipo para IPSec, es necesario instalar en el cliente y el servidor VPN, certificados de equipo también denominados certificados de máquina.

3. **Configurar filtros de paquetes del servidor de seguridad**

   Al tener un servidor de seguridad, se deben configurar los filtros de paquetes, para permitir el tráfico entre los clientes y el servidor VPN.

4. **Crear una directiva de acceso remoto para las conexiones VPN de acceso remoto**

   Se puede crear una directiva que requiera que las conexiones VPN de acceso remoto usen métodos de autenticación y refuerzo de cifrado específicos.

5. **Usar un servidor IAS[28]**

   Al tener varios servidores VPN ejecutando Windows Server 2003, se deben configurar las directivas de acceso remoto y el registro para cada servidor VPN.

   Se logra un mejoraprovechamiento de las directivas de acceso remoto y registros centralizados, configurando los servidores VPN como clientes deRADIUS de un único equipo.

   También deberá utilizar un servidor IAS si dispone de servidores VPN que ejecutan Windows NT 4.0 con el Servicio de enrutamiento y acceso remoto (RRAS, *Routing and Remote Access Service*) y desea aprovechar las directivas de acceso remoto de los productos de la familia de Windows Server 2003. No puede configurar servidores VPN que ejecuten Windows NT 4.0 como clientes RADIUS. Deberá actualizar un servidor VPN que ejecute Windows NT 4.0 a servidor VPN que ejecute Windows NT 4.0 y RRAS.

   Las principales características de IAS son:

   - Interoperabilidad RADIUS con Juniper, Cisco, Linux, etc.
   - Integración con *Active Directory*® para autenticación y autorización.

[28]IAS.- Servicio de Autenticación de Internet

- Soporta EAP(*Extensible Authentication Protocol*)
- Soporta políticas de acceso remoto
- Depende de una clave compartida

6. **Usar *Connection Manager***

   Cuando se tiene una gran VPN de acceso remoto, puede utilizar *Connection Manager* y el Kit de administración de *Connection Manager* para proporcionar un marcador personalizado con conexiones VPN configuradas previamente a todos los clientes de acceso remoto de la organización.

2.1.2.4 Configuraciones para crear una VPN con Windows Server 2003

Para crear la VPN se debe configurar el servicio de enrutamiento y acceso remoto, en el que se puede ejecutar el asistente de instalación del servidor de enrutamiento y acceso remoto para obtener rutas de acceso parecidas a las soluciones que se quiere implementar. Si se desea realizar más configuraciones del servidor, se las puede hacer el momento que finalice el asistente, o se puede elegir la ruta de acceso de configuración personalizada.

2.1.2.4.1 Configuración del Servidor de la VPN

1. Seleccionar*Herramientas administrativas*, donde se encuentra *Enrutamiento y acceso remoto*.

2. Dentro de *Enrutamiento* y *acceso remoto*, dar clic con el botón secundario del mouseen el nombre del servidor, hacer clic en *Configurar* y *habilitar Enrutamiento y acceso remoto*.

   Enrutamiento y acceso remoto, proporciona acceso remoto seguro a redes privadas. Se lo utiliza para configurar:

   - Puerta de enlace de la VPN.

- Conexión segura entre dos redes privadas
- Servidor de acceso remoto de acceso telefónico.
- Traducción de direcciones de red (NAT).
- Enrutamiento LAN.
- Servidor de seguridad básico.

En la figura 2.1 se indica el paso 1 y 2 para configurar el servidor de la VPN

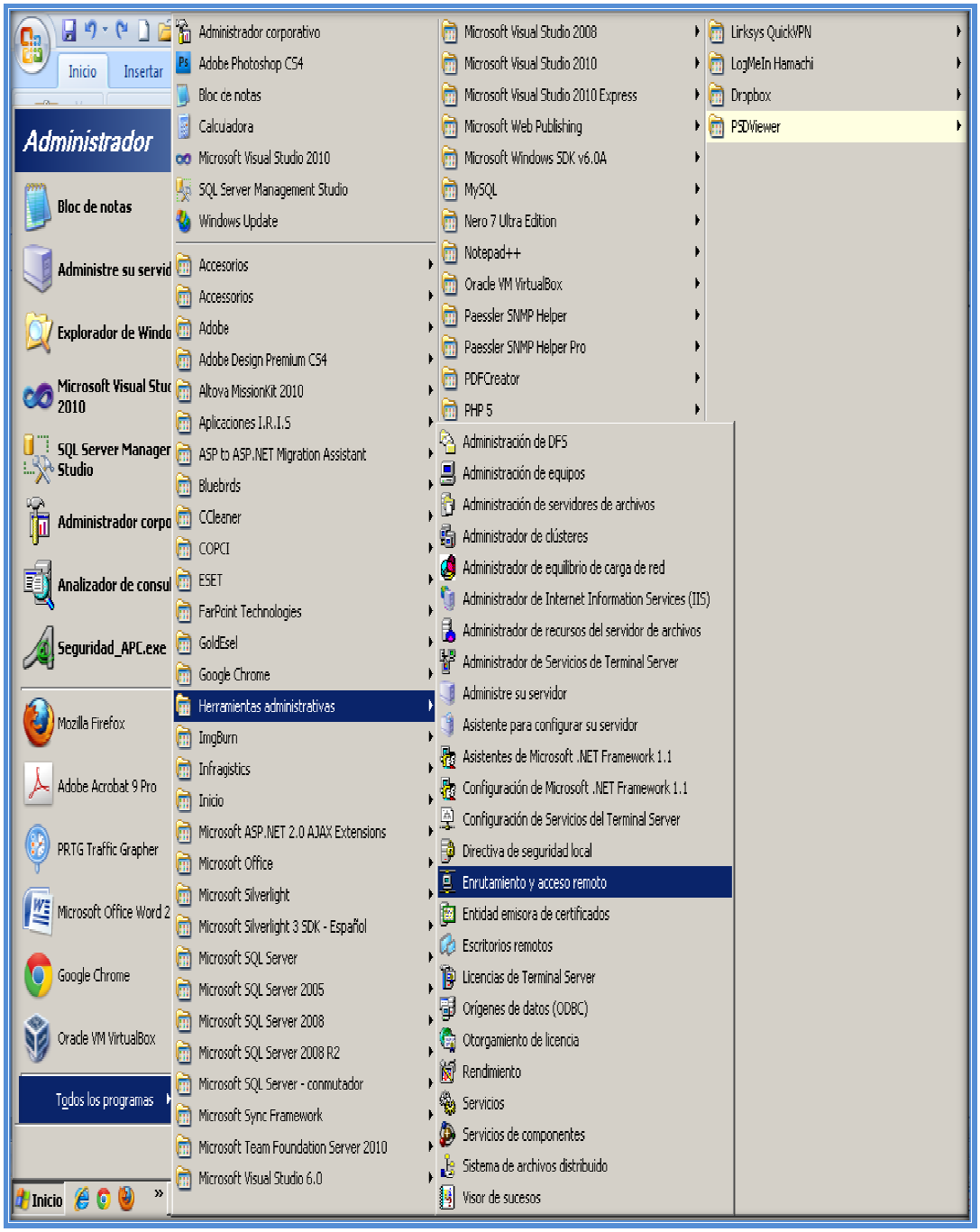


Figura 2.1 Enrutamiento y acceso remoto Windows Server 2003

En la figura 2.2 se indica la selección del servidor dentro de: enrutamiento y acceso remoto.

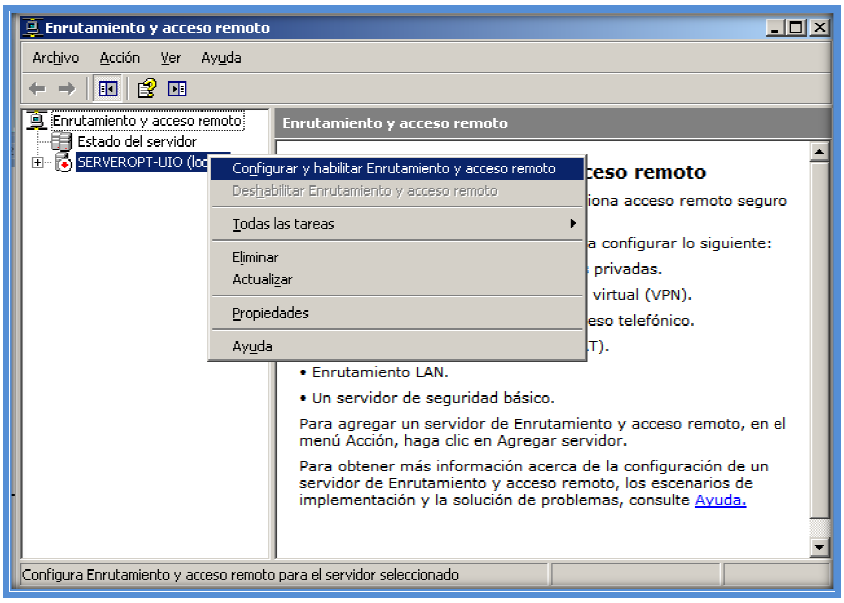


Figura 2.2 Enrutamiento y acceso remoto al servidor

3. En el *Asistente para instalación del servidor de enrutamiento y acceso remoto* hacer clic en *Siguiente.(figura 2.3)*

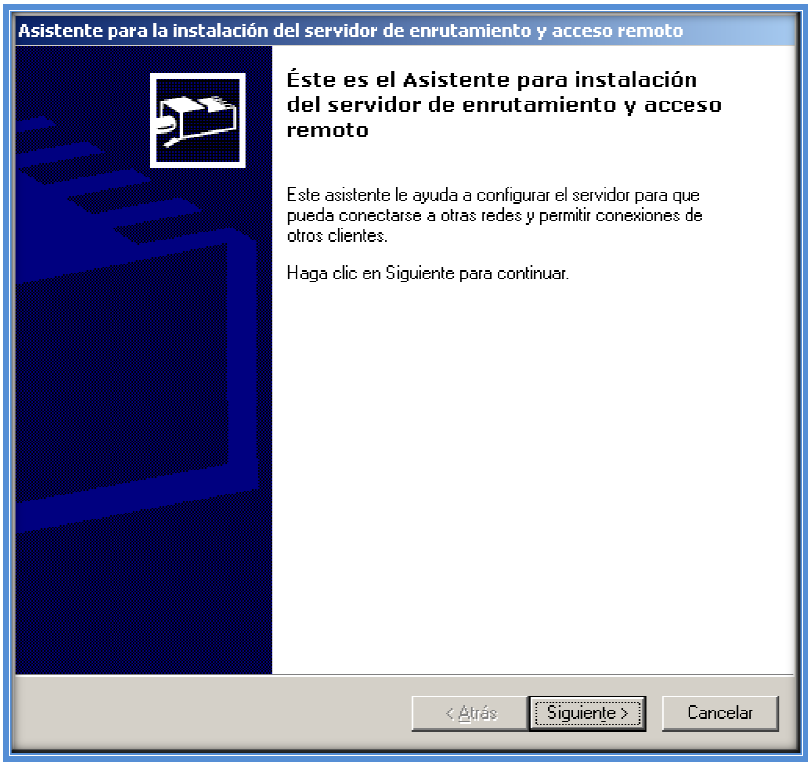


Figura 2.3 Asistente para instalación del servidor de enrutamiento y acceso remoto

4. Seleccionar *Acceso remoto* (*acceso telefónico o red privada virtual*) y, a continuación, clic en *Siguiente*. (Ver figura 2.4)

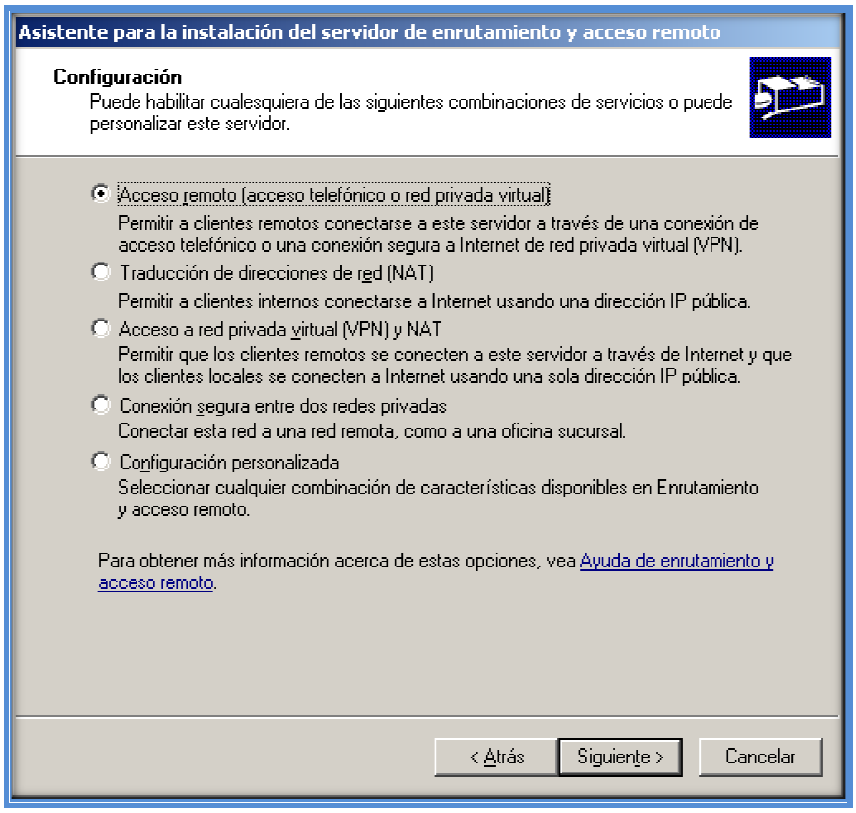


Figura 2.4 Configuración en modo de acceso remoto

5. Seleccionar VPN como se muestra en la figura 2.5, dar clic en *Siguiente*.

6. Seleccionar la interfaz de red, mediante la cual funcionará la VPN sitio a sitio. Seleccionar la opción *habilitar seguridad*, dar clic en *Siguiente*.

7. Seleccionar en *Asignación de direcciones* IP, la opción automáticamente, dar clic en *Siguiente*.

8. En *administrar servidores de acceso remoto múltiples*, se debe mantener la selección predeterminada, y dar clic en *Siguiente*.

   Nota: Si tiene más de un servidor de acceso remoto, en lugar de administrar las directivas de acceso remoto de todos ellos por separado,

puede configurar un solo servidor con el Servicio de autenticación Internet (IAS) como servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) y configurar los servidores de acceso remoto como clientes RADIUS. El servidor IAS proporciona autenticación, autorización, contabilidad y auditoría centralizadas para el acceso remoto.

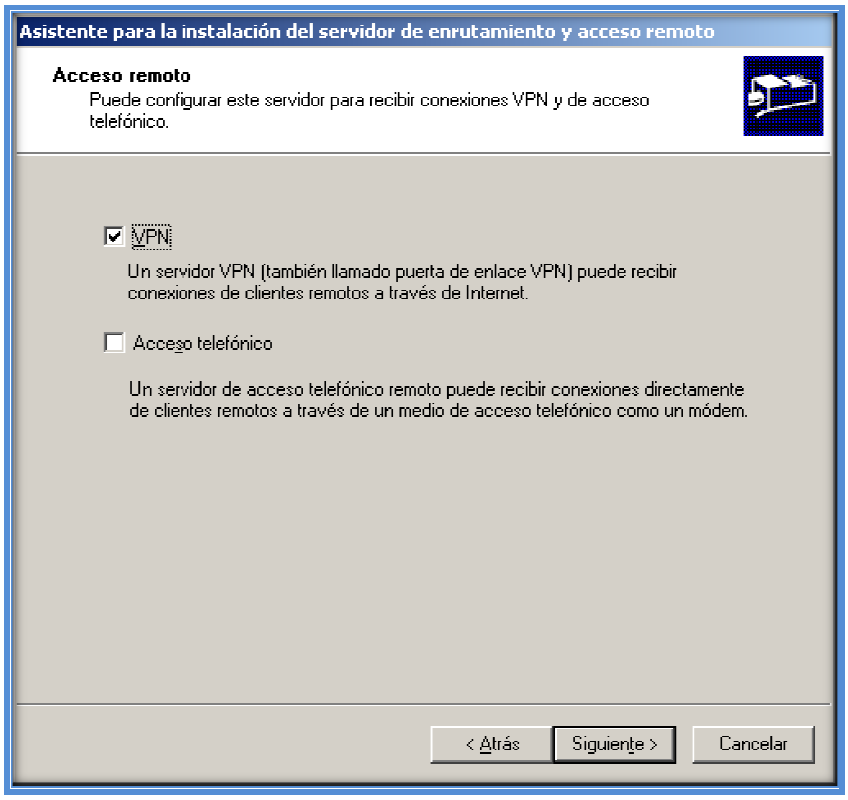


Figura 2.5 Configuración VPN en el acceso remoto

9. Por último dar clic en *finalizar* para terminar la configuración del enrutamiento y acceso remoto.

10. Como se puede observar en la figura2.6,en *enrutamiento y acceso remoto*, dar clic en aceptar para confirmar los requisitos de Retransmisión DHCP.

    Nota: De manera predeterminada, los servicios DHCP que proporciona RRAS automáticamente controlan todos los requisitos de la retransmisión DHCP. En una situación en que haya otro servidor DHCP, debe asegurarse deque el servidor está configurado para retransmitir las solicitudes DHCP[2].

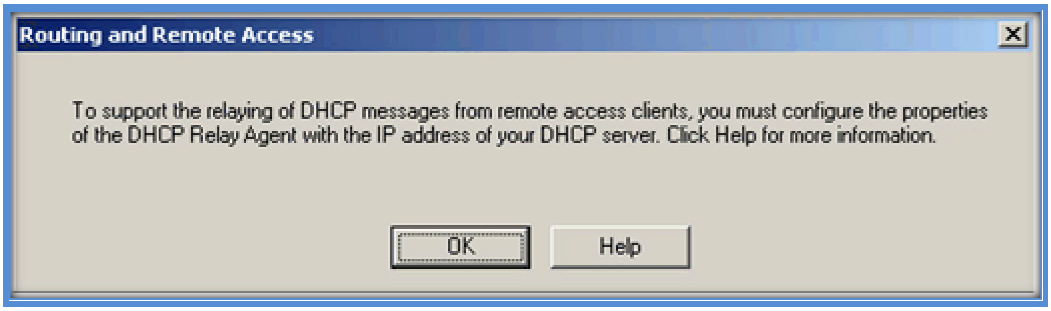


Figura 2.6 Requisitos de retransmisión DHCP

Si se desea crear una VPN Sitio a Sitio, se deben configurar los dos servidores que se unirán a la VPN

2.1.2.4.2 Configuración del Cliente VPN

Los primeros 3 pasos son iguales a los seguidos para configurar el servidor VPN

1. Seleccionar*Herramientas administrativas*, donde se encuentra *Enrutamiento y acceso remoto*.

2. Dentro de *Enrutamiento y acceso remoto*, dar clic con el botón secundario del mouseen el nombre del cliente VPN, hacer clic en *Configurar y habilitarEnrutamiento y acceso remoto*.

3. En el Asistente para la instalación del servidor de enrutamiento y acceso remoto hacer clic en *Siguiente*.

4. Seleccionar la opción *configuración personalizada*, hacer clic en Siguiente.

5. Seleccionar la opción de *conexiones de marcado a petición* (utilizadas para enrutamiento de sucursales), hacer clic en *Siguiente*.

6. Seleccionar *Finalizar*, para terminar la configuración del enrutamiento y acceso remoto.

7. Para empezar el servicio RRAS, se debe hacer clic en *Sí,* del cuadro de diálogo Enrutamiento y acceso remoto.

Para realizar una VPN de acceso remoto se configura el servidor VPN y el cliente remoto VPN.

2.1.2.4.3 Configuración de la clave compartida de IPSec

Se preconfigura el cliente L2TP y el servidor L2TP de Windows Server 2003, para la autenticación de IPSec basada en certificados. El momento de iniciar una conexión de L2TP sobre IPSec se crea automáticamente una directiva de IPSec, para establecer el intercambio de claves de Internet (IKE),que usarán la autenticación basada en certificados durante la negociación de la configuración de seguridad para L2TP. Es necesario tener instalado un certificado de equipo en el cliente L2TP y el servidor L2TP para establecer correctamente la conexión L2TP sobre IPSec. Ambos certificados de equipo deben proceder de la misma autoridad emisora de certificados (CA) o el certificado raíz de la CA de cada equipo debe estar instalado como CA raíz de confianza en el almacén de certificados raíz de confianza del otro.

En algunos casos, no se desea tener un método de autenticación IPSec basado en certificados para las conexiones VPN de enrutador a enrutador basadas en L2TP. En este caso, la directiva IPSec se puede configurar manualmente para que use claves previamente compartidas al crear conexiones VPN de enrutador a enrutador. Esta clave de autenticación compartida previamente actúa como una contraseña sencilla en la negociación de IKE. Si ambos extremos pueden probar que conocen la misma contraseña, pueden confiar uno en otro y continuarán con la negociación de claves de cifrado simétricas y privadas y la configuración específica de seguridad para el tráfico L2TP.
Normalmente, se considera que el uso de una clave compartida previamente de IKE no es tan seguro como el uso de certificados, porque la autenticación de IKE

(y la confianza implícita) depende sólo del valor de la clave, que se almacena como texto sin formato en la directiva de IPSec. Cualquier usuario que vea la directiva puede ver el valor de la clave compartida previamente. Si un usuario malintencionado ve la clave compartida previamente, podría configurar su sistema para que pueda establecer la seguridad IPSec con el sistema de otro usuario. Sin embargo, la conexión L2TP requiere autenticación en el nivel de usuario mediante un Protocolo punto a punto (PPP). Por ello, un usuario malintencionado tendría que conocer la clave compartida previamente y las credenciales de usuario correctas para poder establecer la conexión L2TP sobre IPSec.

a. Configuración de la clave compartida de IPSec en el servidor de respuesta (Quito)

1. Seleccionar*Herramientas administrativas*, donde se encuentra *Enrutamiento y acceso remoto.*

2. Dentro de *Enrutamiento y acceso remoto*, dar clic con el botón secundario del mouseen el nombre del servidor VPN, hacer clic en *Propiedades*.

3. En Propiedades del servidor, seleccionar *Seguridad*. Activar la selección *Permitir la directiva personalizada IPSEC para la conexión L2TP*, se debe ingresar la clave previamente compartida (12345), como se muestra en la figura 2.7y, hacer clic en *Aceptar.*

b. Configuración de la clave compartida de IPSec en el servidor de llamada (Guayaquil)

1. Seleccionar *Herramientas administrativas*, donde se encuentra *Enrutamiento y acceso remoto.*

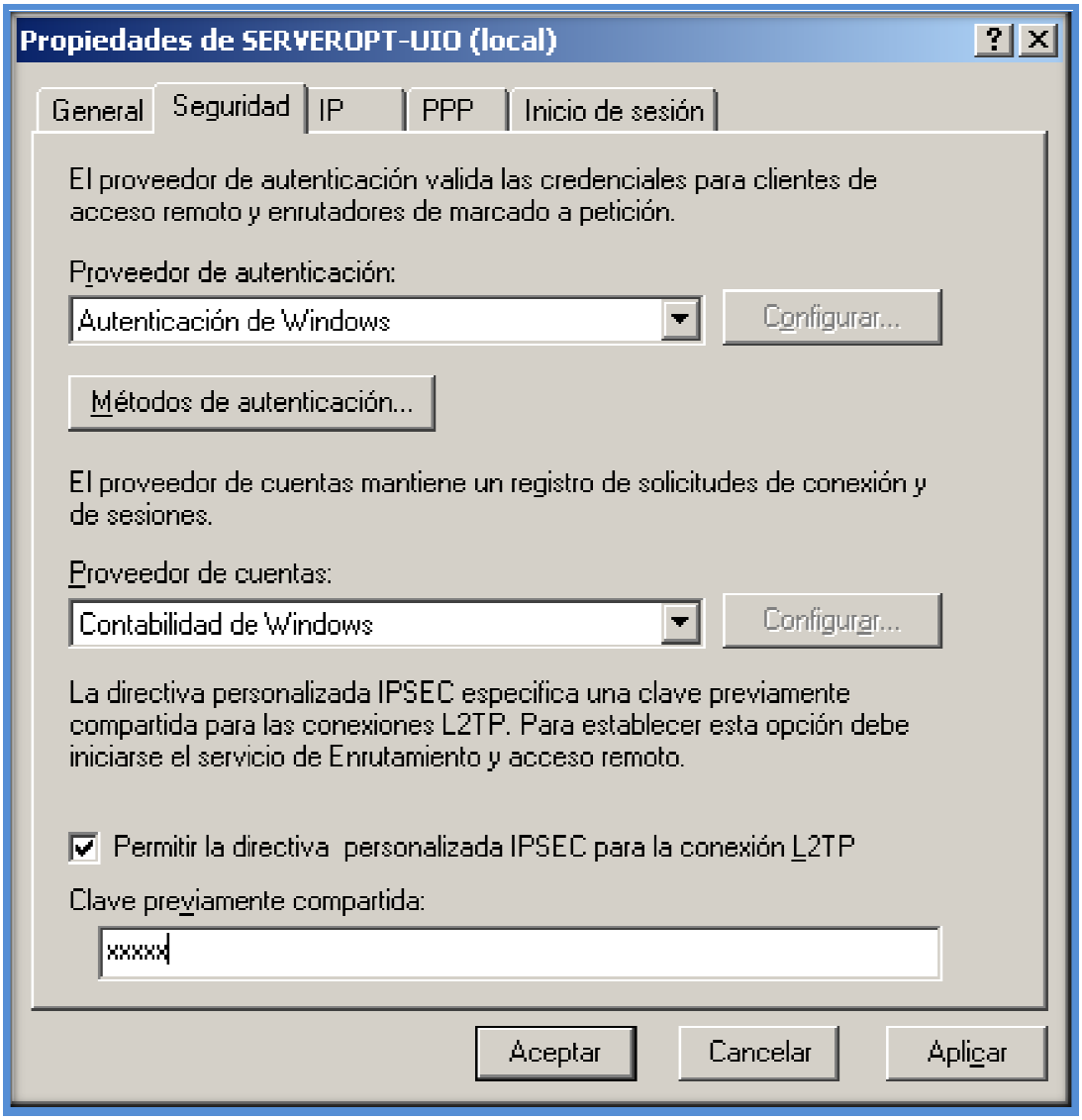


Figura 2.7 Establecer una clave compartida previamente en el enrutador de respuesta

2. Dentro de *Enrutamiento y acceso remoto*, dar clic para que se despliegue el árbol del servidor de llamada, hacer clic en *interfaces de red*, dar doble clic en la VPN que se creó (VPN-Optimsoft).

3. En Propiedades de VPN-Optimsoft, Seleccionar *seguridad*,activar el botón *Configuración IPSec*.

4. En *Configuración IPSec*, Activar *usar clave previamente compartida al autenticar,* se debe escribir la clave previamente compartida (12345) como se muestra en la figura 2.8 , dar doble clic Aceptar.

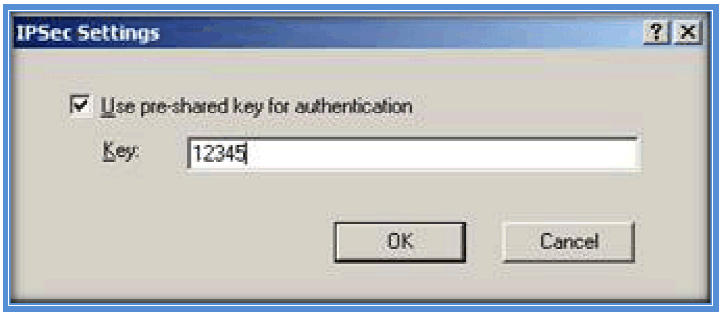


Figura 2.8 Clave compartida previamente en el enrutador de llamada

2.1.2.5 VPNs de nivel 2 con Microsoft

Microsoft puede crear VPN de nivel 2, utilizando el *software* de los siguientes servidores:

- NT 4.0. con SP3 y *Option Pack*
- Windows 2000. Con RRAS + IAS (RADIUS)
- Windows 2003. Con RRAS + IAS (RADIUS)

2.1.2.6 Problemática de las VPNs

Los problemas que se presentan al usar VPN utilizando software Windows Server 2003son los siguientes:

- Seguridad al extender TODA la red a un equipo externo.
- Necesidad de conectar diferentes tipos de dispositivos.
- Conectividad de *Firewalls y routers* con NAT[29].
- Dificultades para instalar y mantener los clientes.
- Alto TCO [30] debido al mantenimiento.

---

[29]NAT.-*Network Address Translation*.-Estándar para la utilización de una o más direcciones IP para conectar varias computadoras a una red (especialmente Internet). Cada computadora tiene una dirección IP distinta (generalmente no válida para Internet). Fue desarrollada por la IETF.

[30]TCO.- *Total Cost of Ownership*.- Método para determinar costos directos e indirectos

2.1.3 LOGMEIN HAMACHI

Es un software de servicio VPN hospedado mediante el cual se pueden conectar dispositivos y redes de manera segura, ampliando la conectividad de red de tipo LAN a usuarios móviles, equipos distribuidos y aplicaciones empresariales (SICE Profesional[31]). Permite crear de manera sencilla redes virtuales seguras mediante solicitudes a través de redes públicas y privadas. Hamachi puede ser administrado de forma segura desde cualquier sitio a través de la web.

Hamachi se lo puede obtener de forma gratuita o comercial, entre ellas existen algunas diferencias que se pueden observar en el Anexo A.

2.1.3.1 Funcionamiento de LogmeIn Hamachi

Para crear la VPN se utiliza el protocolo UDP[32], no orientado a conexión de la capa de transporte del modelo TCP/IP, el mismo que por ser muy simple no proporciona detección de errores. Se utiliza un servidor de enlace para localizar los extremos e iniciar la conexión entre ellos, creando una conexión *peer-to-peer*, la misma que una vez establecida es directa y el tráfico deja de fluir a través de los servidores.

2.1.3.2 Ventajas de LogmeIn Hamachi

Las principales ventajas al utilizar LogmeIn Hamachi se detallan a continuación:

- No requiere configuración adicional
- Compatible con sistemas: Windows 2000, XP, 2003, Vista y 7. También existen versiones de la consola de Hamachi para Linux y OS X.
- Actualización del programa sin perder la configuración existente.
- No tiene conflicto con el *firewall* existente de la red.

---

[31] SICE Profesional.- Sistema Integrado de Comercio Exterior (desarrollado por la empresa Optimsoft)

[32] UDP.- Protocolo de datagrama de usuario, protocolo de la capa de transporte, no tiene garantía de entrega de mensaje, utiliza datagramas

- Se puede crear una VPN fácilmente en aproximadamente 10 minutos de instalación sin necesidad de hardware.
- Se crea un túnel seguro ya que las comunicaciones son cifradas
- Es administrable desde la web.
- Es gratuita para uso no comercial

2.1.3.3 Seguridades de LogMeIn Hamachi

La empresa para mantener estándares de calidad, revisa continuamente la confidencialidad de la información, contratando empresas acreditadas e independientes de auditoría externa.Con lo que se garantiza seguridad y protección de los datos transmitidos.

La seguridad y protección de los datos, se logra utilizando algoritmos y protocolos estándar para el cifrado y la autenticación. Nadie podrá ver, ni tener acceso a los datos que se trasmiten entre los equipos que se conectan utilizando Hamachi, ni siquiera el proveedor del servicio.

2.1.3.3.1 Arquitectura

Para comunicarse los dos extremos de la VPN, necesitan establecer una autenticación mutua y tener un acuerdo de claves de sesión. El tráfico del envío de información es en forma directa evitando los servidores propios del programa (LogMeIn Hamachi); el tráfico se asegura y cifra en los terminales, inclusive el que debe retransmitirse a través de los servidores.

2.1.3.3.2 Autenticación

Se realiza la autenticación al inicio de una conexión para garantizar que el intercambio de datos se realice entre las partes correctas.

Se siguen los siguientes pasos para la autenticación e inicio de la sesión:

1. Los servidores autentican a los nodos con un par de claves RSA.
2. El nodo envía su identificador y utiliza su clave privada para firmar el desafío del servidor.
3. El servidor verifica la firma y autentica al cliente.
4. Los nodos autentican a los servidores con un par de claves RSA.
5. El nodo se conecta con el servidor, anuncia la clave que espera tenga el servidor.
6. Si el servidor posee la clave solicitada, comienza la secuencia de inicio de sesión.

2.1.3.3.3 Cifrado

El cifrado es un método que codifica y decodifica varios fragmentos de información para poder enviarlos de forma segura de un punto a otro.

Cuando cualquiera de las dos entidades intercambia datos entre sí, se produce un protocolo de intercambio de claves junto con la fase de autenticación obligatoria. El protocolo de intercambio de claves es Diffie-Hellman con el grupo 2048 bits como se define en RFC 3526.

- Una vez que se ha establecido una clave de sesión, se utiliza el cifrado AES-256-CBC para el cifrado y descifrado de datos, como se define en RFC 2406.
- Los paquetes se autentican con la variante HMAC-SHA-1-96 (RFC 2404) de HMAC-SHA1 (RFC 2104).
- Los paquetes se enumeran para evitar ataques de retransmisión.

2.1.3.3.4 Administración

La administración puede realizarse por cada uno de los interlocutores para ayudar a mantener la seguridad de sus redes.

Las siguientes funciones están disponibles para las redes basadas en clientes:

- Protección de contraseña
- Bloqueo de red
- Aprobación de miembros
- Expulsión de miembros
- Prohibición de miembros

2.1.3.3.5 Administración Centralizada

Si se tiene una empresa que posee varias redes y nodos, la alternativa recomendada para administrar redes virtuales es con LogMeIn.com. Mediante la web se puede acceder a los controles de red estándar. Utilizando LogMeIn Central, se definen varios usuarios que inicien la sesión para administrar la(s) red(es),tal como se muestra en la figura 2.9.

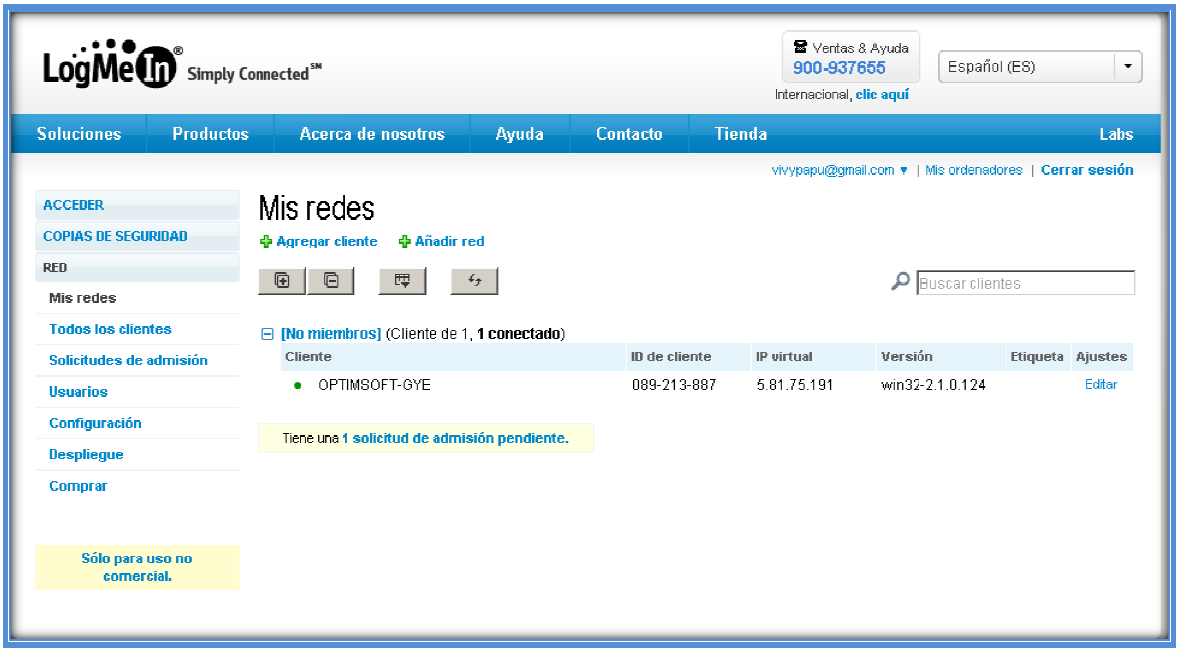


Figura 2.9 Administración de redes Hamachi desde la web[3]

2.1.3.4 Instalación centralizada de software

Es muy fácil ser parte de una red virtual sin necesidad de movilizarse, tan solo se envía al usuario un vínculo para que descargue e instale; en cuestión de pocos minutos se es parte de una red virtual específica.

2.1.3.5 Tipos de redes en LogMeIn Hamachi

2.1.3.5.1 Redes virtuales de puerta de enlace

Los usuarios remotos tienenacceso seguro a la red privada, y a los recursos que se encuentran en ella, utilizando una puerta de enlace centralizada de LogMeIn Hamachi sin necesidad de modificar *firewall* ni *routers* de la red.(figura 2.10)

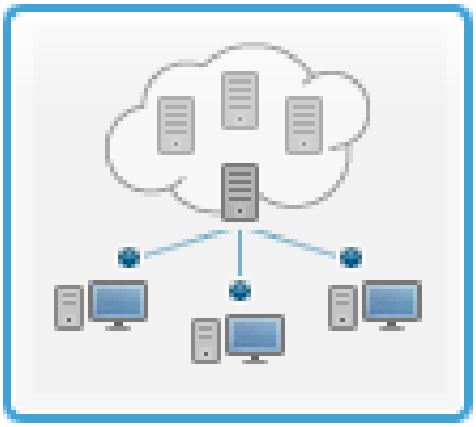


Figura 2.10 Red Virtual de puerta de enlace[4]

2.1.3.5.2 Redes virtuales de concentrador y radio

Los usuarios remotos tienen acceso seguro a ordenadores específicos de la red, sin importar su ubicación y sin tener que modificar*firewall* ni *routers* de red. (figura 2.11)

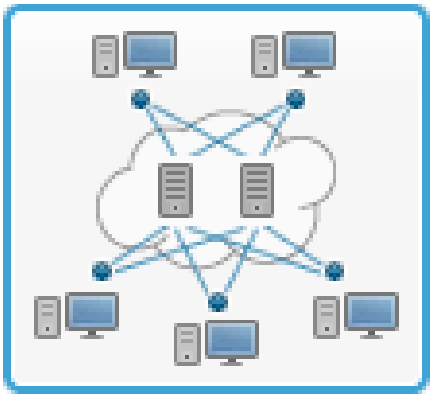


Figura 2.11 Red Virtual de concentrador y radio[4]

2.1.3.5.3 Redes Virtuales de malla

Se crea una interconexión entre todos los clientes de la red, creandouna red de malla virtual, que permite a los equipos remotos conectarse directamente entre sí y tener acceso a todos los recursos de red que necesiten.(figura 2.12)

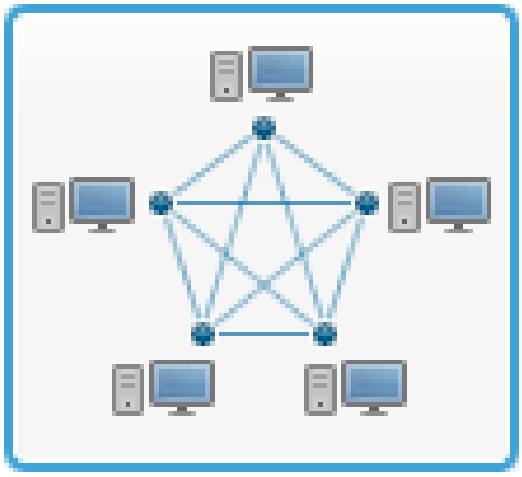


Figura 2.12 Red Virtual de malla[5]

2.1.3.6 Requerimientos para crear VPN con LogmeIn Hamachi

Para crear una VPN con LogmeIn Hamachi se necesita lo siguiente:

- Servidor en el que se ha instalado el programa LogmeIn Hamachi
- Computador en el que se ha instalado el programa LogmeIn Hamachi
- Acceso a Internet

2.1.3.7 Configuración para crear la VPN con LogmeIn Hamachi

Instalación del programa

1. Descargar e instalar LogMeIn Hamachi (www.logmein.com) en los equipos que se desee configurar la VPN.

2. Ejecutar el asistente, aceptar las condiciones legales, elegir la ubicación de la aplicación y el inicio (automático o no).

3. Para tener una mayor seguridad se selecciona Deshabilitar servicios vulnerables de Windows sobre Hamachi.

4. Seleccionarel tipo de Hamachi que se desea utilizar,no comercial (gratuita) o comercial, dar clic en Instalar.

Configuración de la VPN

1. Activarla VPN mediante el botón de Encendido.

2. Introducir un nombre que identifique al equipo

3. Seleccionar *Crear nueva red*, ingresando el nombre que identificará a la red y la contraseña para establecer la conexión, hacer clic en*Crear*.

Unirse a la red

4. Activaral usuario con el que se va a crear la VPN con el botón de encendido

5. Introducirel nombre que identifique el equipo en la red a la cual va a pertenecer.

6. Dar clic en *Crear o unirse a una red*, seleccionar *Unirse a una red existente*. En el cuadro de diálogo que aparece se debe ingresar el nombre de la red y la contraseña correcta.

7. Dar clic en*Unirse*.Una vez que se ha unido a una red, ésta aparecerá así como los equipos que se encuentran en la red.

2.2 IMPLEMENTACIÓN MEDIANTE HARDWARE

Para crear la VPN se utilizan los equipos de la red, que deben tener características propias para crear VPNs, exigiendo una configuración específica,para encriptar, dando mayor seguridad.

Estas VPNs son mayormente utilizadas en empresas que dependen en gran medida del rendimiento,el cual se logra al garantizarque los equipos de la red se concentren en sus tareas previstas, en lugar de compartir sus recursos para la VPN.

2.2.1 INSTALACIÓN DE LA VPN MEDIANTE HARDWARE

Puede ser instalada por el vendedor del equipo o personal capacitado. Se debe tomar en cuenta que siempre un hardware de VPN, requiere una formación adicional para el personal de la empresa, para gestionaro solucionar problemas que se presenten en la red.

Las VPNs de hardware son usadas más en conexiones sitio a sitio.

2.2.2 CLASES DE VPNMEDIANTE HARDWARE

2.2.2.1 Sitio a sitio

Son las VPNs que se realizan utilizando *routers* a los extremos, entre los cuales se conecta y crea la VPN, se configura la VPN para acceder a los recursos de las redes que están conectadas a los *routers*,como se puede apreciar en la figura 2.13.

2.2.2.1.1 Requisitos para crear una VPN sitio a sitio utilizando *Hardware*

- Dos *routers* que posean la característica de VPN

- Conexión a Internet

En la figura 2.13 se indica una VPN sitio a sitio utilizando*routers*

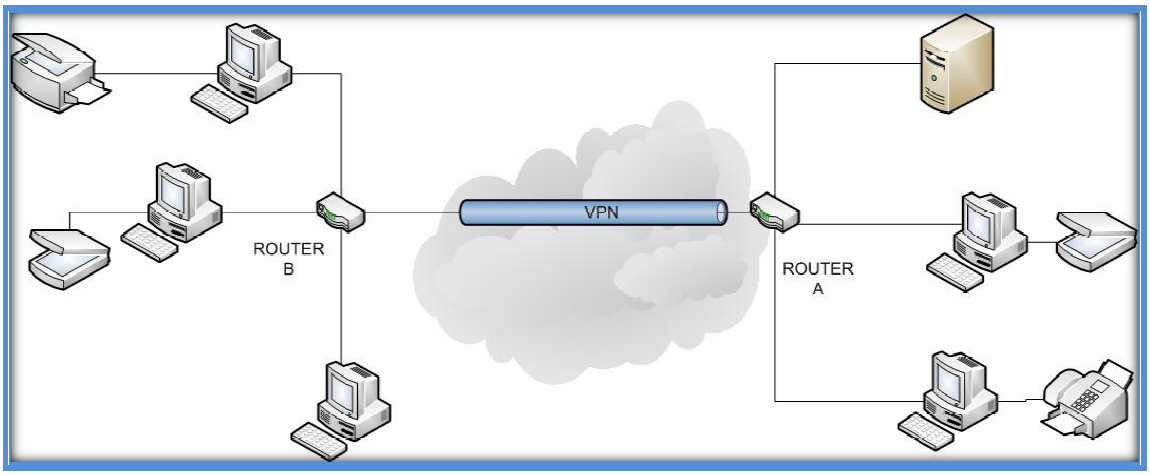


Figura 2.13VPN sitio a sitio de *Hardware*

2.2.2.2 Acceso Remoto

Se crea la VPN, utilizando en un extremo el Software QuickVPN para configurar la VPN en una computadora remota o laptop, que posee un único nombre de usuario y contraseña para acceder en forma segura a la red que posee al otro extremo un *Router* VPN.

El programa QuickVPN Linksys es compatible con Microsoft (Windows 2000 y XP).

2.2.2.2.1 Requisitos para crear una VPN de acceso remoto mediante Hardware[6]

- Un *router* que posea la característica de VPN
- Un computador en el que se instale el Software QuickVPN
- Conexión a Internet

2.2.3 VENTAJAS DE UTILIZAR VPN CON HARDWARE[6]

- Posee una mayor seguridad, debido a que utiliza un dispositivo independiente de la red para crear la VPN.

- Este dispositivo es dedicado únicamente a gestionar la autenticación, cifrado y otras funciones de VPN.
- Proporciona un *firewall* de hardware.
- Brindan un equilibrio de capacidad al manejar grandes cargas de los clientes.
- La administración se gestiona a través de una interfaz de navegador Web.

En la figura 2.14 se indica una VPN de acceso remoto utilizando un solo *router*

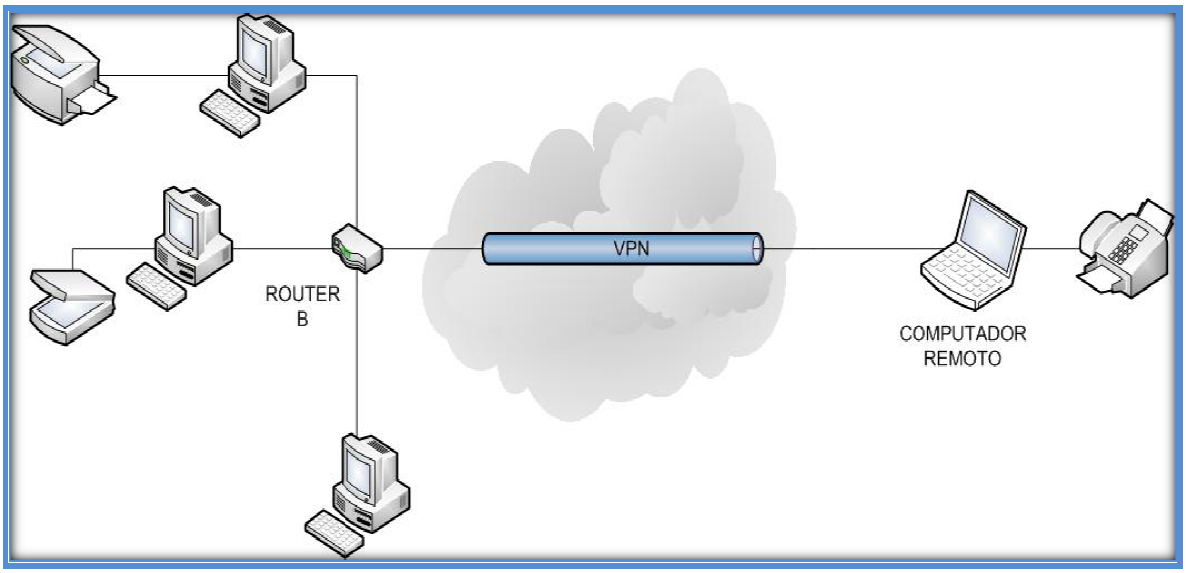


Figura 2.14VPN de acceso remoto con *hardware*

2.2.4 CONFIGURACIÓN DE VPN MEDIANTE HARDWARE

Se necesita configurar primero cada *router* que se desea interconectar.

1. En la ventana de configuración del *router*, hacer clic en *Estado*, para en el *router* registrar la Dirección IP de Internet.

2. Hacer clic en *Estado* y dar clic en *Red Local*para registrar la Dirección IP.

Se debe verificar que la Dirección IP Local de los dos *routers*sean diferentes. Observar que la Dirección IP Local del *Router* A sea la del Grupo Seguro Remoto del *Router* B.

Establecimiento del túnel en el *router* de Quito

1. En la ventana de configuración del *router* basada en la red, hacer clic en *VPN* y seleccionar la pestaña *VPN IPSec*.

2. Seleccionar la Entrada de Túnel que desea crear.

3. Seleccionar el Túnel VPN que desee utilizar y Habilitar.

4. Ingresar el Nombre de Túnel que desea crear.

5. En la parte de Grupo Seguro Local, seleccionare ingresar los valores correspondientes a: Subred, Dirección IP o Rango IP.

6. En la parte de Grupo Seguro Remoto seleccionare ingresar los valores correspondientes a: Subred, Dirección IP, Rango IP (del *router* remoto).

7. En la parte de Puente de Acceso de Seguridad Remoto, seleccionar Dirección IP, ingresar la dirección IP (de Internet del *router* remoto).

8. Seleccionar en Encripción, el nivel de encripción que se desea habilitar(el nivel de Encripción debe ser el mismo en los dos *routers* para establecer el túnel VPN).

9. Seleccionar en Autenticación,el método que desea habilitar en el túnel. (el método de Autenticación debe ser el mismo en los dos *routers* para establecer el túnel VPN).

10. En la parte de Intercambio de Clave, seleccionar Auto (IKE).

11. Debe estar seleccionado PFS[33], para asegurar que el intercambio inicial de clave y las propuestas IKE sean de manera segura.

12. Ingresar la clave que habilitará el túnel en Clave Pre-Compartida

13. Ingresar el tiempo que se desea que dure la clave en *Clave De Por Vida IPSec.* (las Claves: Pre-Compartida y De Por Vida IPSec deben ser las mismas en los dos *routers*).

14. Por último se debe guardar la configuración.

Establecimiento del túnel en el *router* de Guayaquil

1. En la página de configuración del *router* basada en la red, hacer clic en *VPN* y seleccionar la pestaña *VPN IPSec*.

2. Seleccionar la Entrada de Túnel que desea crear.

3. Seleccionar el Túnel VPN que desee utilizar y Habilitar.

4. Ingresar el Nombre de Túnel que desea crear.

5. En la parte de Grupo Seguro Local, seleccionare ingresar los valores correspondientes a: Subred, Dirección IP o Rango IP.

6. En la parte de Grupo Seguro Remoto seleccionare ingresar los valores correspondientes a: Subred, Dirección IP, Rango IP (del *router* remoto).

7. En la parte de Puente de Acceso de Seguridad Remoto, seleccionar Dirección IP, ingresar la dirección IP (de Internet del *router* remoto)

[33]PFS.- Confidencialidad Directa Secreta

8. Seleccionar en Encripción, el nivel de encripción que se desea habilitar (el nivel de Encripción debe ser el mismo en los dos *routers* para establecer el túnel VPN).

9. Seleccionar en Autenticación, el método que desea habilitar en el túnel. (el método de Autenticación debe ser el mismo en los dos *routers* para establecer el túnel VPN).

10. En la parte de Intercambio de Clave, seleccionar Auto (IKE).

11. Debe estar seleccionado PFS[34], para asegurar que el intercambio inicial de clave y las propuestas IKE sean de manera segura.

12. Ingresar la clave que habilitará el túnel en Clave Pre-Compartida

13. Ingresar el tiempo que se desea que dure la clave en *Clave De Por Vida IPSec.* (las Claves: Pre-Compartida y De Por Vida IPSec deben ser las mismas en los dos *routers*).

14. Por último se debe guardar la configuración.

Una vez configurado el *router* de Guayaquil, se debe seleccionar *Resumen VPN* y hacer clic en *Reinicio* para conectarse al túnel VPN.

2.2.5 PROTOCOLOS QUE SE UTILIZAN

Los protocolos que se seleccionarán al crear la VPN, servirán para dar mayor confiabilidad y seguridad.

[34]PFS.- Confidencialidad Directa Secreta

2.2.5.1 Protocolos de Encriptación disponibles en el *Router Linksys* WRV 200

Los protocolos de encriptación que se pueden seleccionar en el *router Linksys* WRV 2000 son:

- 3DES
- AES 192
- AES 256
- AES 128

2.2.5.2 Protocolos de Autenticación disponibles en el *Router Linksys* WRV 200

Los protocolos de autentificación que posee el *router Linksys* WRV 2000 son:

- MD5
- SHA1

2.3 IMPLEMENTACIÓN MEDIANTE *FIREWALL*

2.3.1 INTRODUCCIÓN A ISA SERVER 2004

El *firewall*ISA[35]SERVER, permite implementar VPNs de manera que los usuarios remotos puedan conectarse con un servidor VPN o con una red entera mediante un túnel VPN configurado a través del Internet; adicionalmente permite conectar dos redes locales ubicadas físicamente en distintos lugares de manera segura por medio del Internet.

Una de las ventajas de ISA Server 2004 es que las reglas del *firewall* se aplican a las VPN. A diferencia de otros productos que brindan acceso completo, las VPN de ISA Server 2004 están expuestas al control de las reglas de acceso, con lo que

[35]ISA.- *Internet Security and Acceleration*

cuando un cliente establece una conexión mediante una VPN en ISA Server,accederá sólo a los recursos que necesita para hacer su trabajo y no a otros.

2.3.2 CLASES DE VPN CON ISA SERVER

Isa Server posee dos tipos de conexiones VPN, depende de las necesidades el seleccionar una de ellas:

- VPN de Acceso Remoto
- VPN Sitio a Sitio

2.3.2.1 VPN de Acceso Remoto

Se usa mayormente en clientes remotos individuales. Tienen riesgo de ser puestos en cuarentena por el firewall ISA SERVER.Cuando los clientes son colocados en cuarentena van a una red de clientes de VPN en cuarentena, hasta que cumplan con los requisitos de seguridad corporativa, en el cual se verifica, y luego pueden ser añadidos a la red de clientes de la VPN.

Los clientes VPN que no cumplan con los requisitos, se les permite conectarse a los recursos de la red interna, dándole el acceso sólo a los recursos necesarios para restaurar el cumplimiento de seguridad, pero no se le permitirá el acceso general a los recursos corporativos.

Ambas redes de clientes VPN están sujetas a las políticas de acceso del firewall ISA Server, de este modo se puede controlar el acceso de cliente de VPN a los recursos de red.

2.3.2.1.1 Protocolos para VPN de acceso remoto

Isa Server utiliza dos tipos de protocolos de túnel para la VPN de acceso remoto, con el fin de dar mayor seguridad.

a.-*Point-to-Point Tunneling Protocol* (PPTP)

b.-*Layer Two Tunneling Protocol* (L2TP)

2.3.2.1.2 Funcionamiento de la VPN de Acceso Remoto

El funcionamiento de la VPN de acceso remoto se basa en los siguientes pasos:

1. Se establece una conexión a Internet
2. Se utiliza el software de cliente VPN, a través de los protocolos de túnel (PPTP o L2TP) para establecer la conexión con la empresa.
3. Los datos viajan a través del tunel VPN de forma cifrada (sea por MPPE o IPSec) que a la vez es una conexión privada.

2.3.2.2 VPN Sitio a Sitio

Se usa para conectar redes enteras entre sí. Además existe una puerta de enlace y ambas redes son final de conexión.

En la figura 2.15 se indica las VPNs formadas entre 2 sucursales y su oficina principal utilizando Isa Server 2004

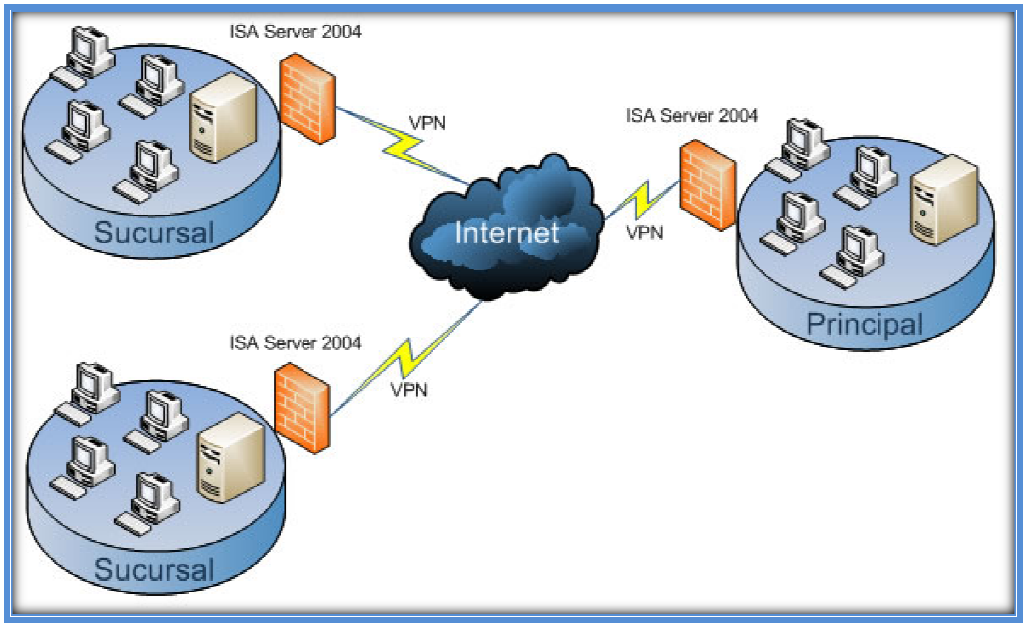


Figura 2.15 VPN mediante *Firewall* ISA Server 2004[7]

2.3.2.2.1 Protocolos para VPN de Sitio a Sitio

Isa Serverutiliza tres tipos de protocolos de túnel para resguardar la información de la VPN de Sitio a Sitio:

a) *Point-to-Point Tunneling Protocol* (PPTP)
b) *Layer Two Tunneling Protocol* (L2TP)
c) Modo Túnel IPSec.

En la tabla 2.1 se observa las características que posee cada uno de los protocolos, se debe decir cuál de ellosse va a utilizar, tomando en cuenta su uso, seguridad y particularidades.

PROTOCOLO	USO	SEGURIDAD	OBSERVACIONES
Modo de túnel IPSec	Conexión a un servidor VPN que no sea Microsoft	Alta	Única compatible para servidores diferentes a Microsoft
L2TP a través de IPSec	Conexión exclusiva con servidores: ISA Server 2004 ISA Server 2000 VPN de Windows	Alta	Se puede usar en acceso remoto. Más sencillo que el Modo de túnel IPSec. Utiliza cifrado IPSecpor lo que no se le considera más seguro que PPP.
PPTP	Conexión exclusiva con servidores: ISA Server 2004 ISA Server 2000 VPN de Windows	Moderada	Se puede usar en acceso remoto. Más sencillo para configurar.

Tabla 2. 1 Comparación de protocolos para VPN[8]

2.3.2.2.2 Configuración básica para crear una VPN sitio a sitio mediante ISA Server con IPSec

Al configurar una VPN de sitio a sitio con ISA Server, se crea una nuevared. Se deben seguir los siguientes pasos para configurarla red.

1. Abrir Microsoft ISA Server Management.

2. Seleccionar Redes privadas virtuales (VPN).
3. En Detalles, hacer clic en Sitios remotos.
4. En Tareas, hacer clic en Agregar red de sitio remoto para iniciar el Asistente para nueva red.
5. En la página Bienvenido, escribir el nombre de la nueva red, hacer clic en Siguiente (el nombre de la redpuede tener máximo 200 caracteres).
6. En Protocolo VPN, seleccionar el modo de túnel del protocolo de seguridad IP (IPSec), hacer clic en Siguiente.
7. En Configuración de la conexión, ingresar las direcciones IP de los servidores VPN local y remoto. (La Dirección IP de la puerta de enlace de VPN remota es la dirección IP que conecta el servidor VPN remoto con Internet).
8. En Redes, ingresar a Redes de acceso. Seleccione la red que representa la puerta de enlace de VPN del equipo servidor ISA (es la red externa, porque la conexión VPN se realizará a través de Internet). Hacer clic en Aceptar.
9. En Dirección IP de puerta de enlace de VPN local, seleccione la dirección IP del adaptador de red que conecta el equipo servidor ISA con la red que se seleccionó en el paso anterior.
10. En Autenticación IPSec, seleccionar Usar clave previamente compartida al autenticar, escribir la clave previamente compartida, hacer clic en siguiente. (método de autenticación IPSec predeterminado para la solución de túnel IPSec).
11. En Direcciones de red, hacer clic en Agregar,escribir el intervalo de direcciones de la red remota. (información que se puede obtener del administrador de la red remota).
12. En Resumen, revisar la configuración y hacer clic en Finalizar.
13. En Detalles del servidor ISA, hacer clic en Aplicar para que los cambios se ejecuten.

2.3.3 VERIFICACIÓN DE CLIENTES DE LA VPN

Las credenciales que son recibidas por ISA SERVER cuando un usuario se conecta usando la conexión de cliente VPN, puede variar dependiendo del escenario de conexión.

2.3.3.1 Verificación por conexión

Cuando un usuario VPN establece la conexión desde un computador cliente de la VPN, ISA SERVER asocia las credenciales del usuario que inicia la VPN con la conexión; si otros usuarios utilizan esa conexión ISA SERVER no recibe sus credenciales, pero seguirá asociando el tráfico a las credenciales utilizadas para establecer la conexión.

Un ejemplo es: si el equipo cliente está configurado para actuar como un dispositivo NAT, esto permite que la conexión VPN pueda compartirse entrevarios usuarios en diferentes equipos.

En la figura 2.16 se indica cómo se usa una sola credencial para la verificación por conexión de la VPN.

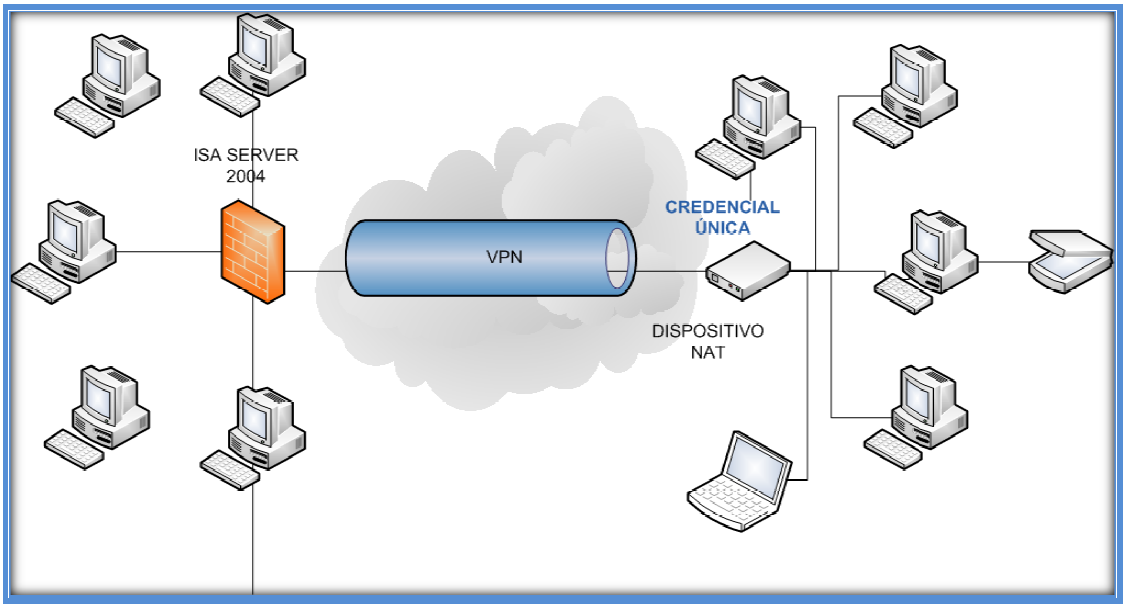


Figura 2.16VPN con verificación por conexión

2.3.3.2 Verificación por usuario

Cuando el Host o los equipos conectados a él, tienen un cliente firewall instalado y configurado correctamente, éstos se unirán a la red de clientes VPN, pero ISA SERVER verifica las credenciales de cada usuario, en lugar de las credenciales del host.

En la figura 2.17 se indica como cada usuario posee su propia credencial para poder ingresar a la VPN.

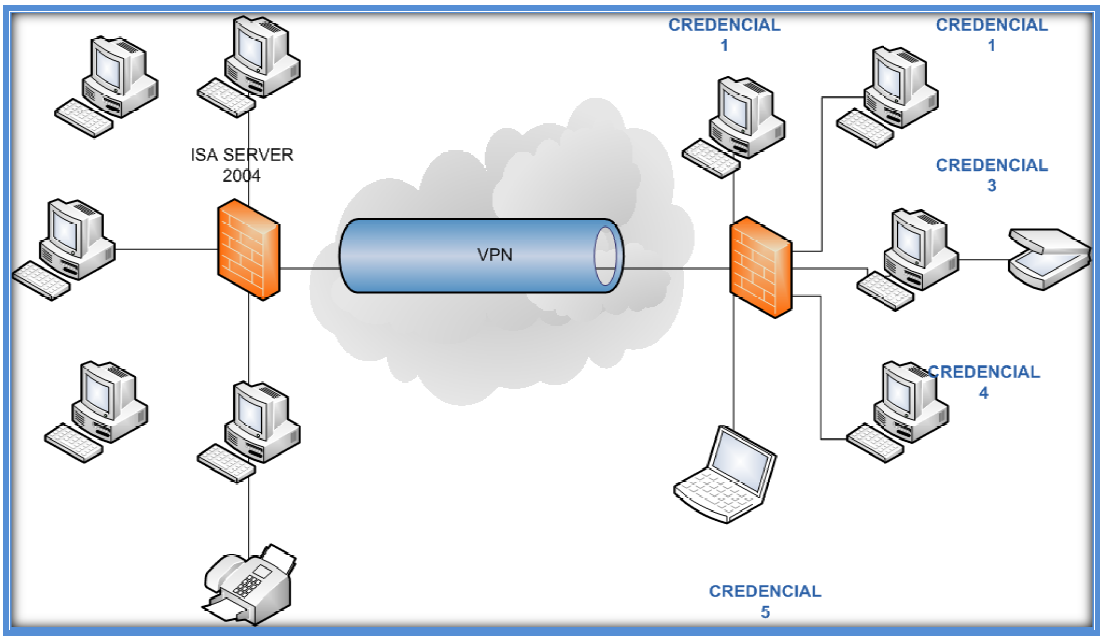


Figura 2.17VPN con verificación por usuario

2.4 ANÁLISIS COMPARATIVO DE LAS ALTERNATIVAS DE IMPLEMENTACIÓN

En la tabla 2.2 se pueden observar las tres opciones que se hananalizado como alternativa de implementación, Además de sus diferentes aplicaciones y requerimientos, es importante comprender las ventajas y desventajas que conlleva el implementar cada una de ellas.

Microsoft Server requiere una configuración dedicada, posee: menor rendimiento, problemas en cuanto a conectividad, dificultades para instalar y mantener los clientes, por lo cual no es una alternativa óptima para el presente caso.

LogmeIn Hamachi es una de las opciones que no tiene conflicto con *firewal;*, su inconveniente,se tieneen el mayor tiempo de respuesta, por lo que no constituye la mejor alternativa.

Isa Server 2004 realmente es la VPN que mayores dificultades presenta debido a que se crean conflictos en la red tales como: todo cliente debe primero pasar por cuarentena, muchos de los equipos de la empresa no tienen compatibilidad con este *firewall*, es necesario un mayor conocimiento de configuración. Por estas razones no es la alternativa óptima para la empresa.

La VPN creada mediante *hardware*con el *Router* WVR200 es la mejor alternativa para la empresa ya que en primera instancia posee mayor seguridad,equilibrio de capacidad con grandes cargas de clientes, y su costo inicial es realmente bajo en función a su vida útil.

Existen diversos protocolos que pueden ser utilizados en la VPN seleccionada, es muy importante saber cuál es el que brinda la seguridad que se necesita.

2.5 ANÁLISIS DE COSTOS DE LA IMPLEMENTACIÓN DE LA VPN

Para implementar la VPN en la empresa Optimsoft entre las oficinas de Quito y Guayaquil, se tienen las siguientes alternativas con sus costos iniciales de implementación y los costos mensuales para mantener el funcionamiento de la VPN (precios incluyen IVA).

A continuación se realiza una descripción de costos de las VPNs propuestas.

Tabla 2. 2 Cuadro comparativo de alternativas de implementación de VPN (Pag. 1 de 2)

VPN		Costo	Protocolos	Características	Ventajas	Desventajas	Clases de VPNs
SOFTWARE	**Microsoft Server 2003**	Licencia programa $ 469 por equipo	RIP OSPF DHCP PPTP L2TP	Ideal para empresas que son implementadas por la misma organización. Menor rendimiento y configuración más delicada. Más configurables e ideales cuando hay problemas de interoperatividad. Realizar enrutamiento inteligente de manera mucho más fácil	Soporta EAP Políticas de acceso remoto Depende de una clave compartida	Problemas de conectividad de *Firewalls y routers* con NAT. Dificultades para instalar y mantener los clientes. Alto TCO por mantenimiento.	Acceso Remoto
	LogmeIn Hamachi	Suscripción anual $ 199 por año	MODP 2048		Cifrado, autenticación. No configuración adicional Compatible con: Windows 2000, XP, 2003, Vista y 7, Linux y OS X. Actualización del programa sin perder la configuración existente. No conflicto con firewall existente. Instalación: 10 minutos sin hardware. Túnel seguro Administrable desde la web. Gratuita para uso no comercial	Mayor tiempo de respuesta	Sitio a Sito Acceso Remoto

HARDWARE	**ROUTER** **WVR200**	$ 80 por router	Encriptación 3DES AES 192 AES 256 AES 128 Autenticación MD5 SHA1	Los routers encriptan Son seguros y proveen mayor rapidez en transmisión de datos Gran rendimiento Fácil configuración Dispositivo dedicado sólo limitado por su propio hardware. Muchas soluciones de hardware VPN ofrecen el equilibrio de carga .	Mayor seguridad, dispositivo independiente de la red. Autenticación, cifrado y otras funciones de VPN Firewall de hardware. Equilibrio de capacidad con grandes cargas de los clientes. Administración mediante interfaz de navegador Web.	Costo inicial del equipo Capacitación del personal técnico	Sitio a Sitio Acceso Remoto
FIREWALL	**ISA** **SERVER** **2004**	Licencia programa $ 500 por equipo	IPSec L2TP a través IPSec PPTP	Posee traducción de direcciones NAT Menor rendimiento por no ser especializado en encriptación Mayor seguridad propia del firewall	Las reglas del firewall se aplican a las VPN. Están expuestas al control de las reglas de acceso No se necesita instalar un software de terceros	Necesario mayor conocimiento de configuración Colocación en cuarentena de los clientes VPN	Sitio a Sitio Acceso Remoto

2.5.1 VPN DE SOFTWARE

Costos iníciales

Cantidad	Descripción	Costo
1	Programa Windows Server 2003 para Quito	$ 469.00
1	Programa Windows Server 2003 para Guayaquil	$ 469.00
		$ 938.00

Costos mensuales

Cantidad	Descripción	Costo
1	Conexión a Internet (corporativo TV Cable 1Mbps) Quito	$ 79.90
1	Conexión a Internet (TV Cable 1Mbps) Guayaquil	$ 34.90
		$ 114.80

Al implementar una VPN utilizando Windows Server 2003, es necesaria una inversión inicial de $938 y además se requiere un gasto fijo mensual de $114.80; debe tomarse en cuenta que la inversión inicial debe darse cada año por motivo de renovación de licencias, siendo el análisis válido para un año a partir de la compra del programa.

2.5.2 VPN DE HARDWARE

Costos iníciales

Cantidad	Descripción	Costo
1	*Router* WRV 200 Quito	$ 80.00
1	*Router* WRV 200 Guayaquil	$ 80.00
		$ 160.00

Costos mensuales

Cantidad	Descripción	Costo
1	Conexión a Internet (corporativo TV Cable 1Mbps) Quito	$ 79.90
1	Conexión a Internet (TV Cable 1Mbps) Guayaquil	$ 34.90
		$ 114.80

Al implementar una VPN utilizando los *Routers* WVR200, es necesario una inversión inicial de $160 que es un costo realmente bajo debido a su larga vida útil y además se requiere un gasto fijo mensual de $114.80 por motivos de la conexión a Internet que es un gasto que se requiere hacer en cualquiera de las alternativas.

2.5.3 VPN DE FIREWALL

Costos iníciales

Cantidad	Descripción	Costo
1	Firewall ISA Server 2004 Quito	$ 500.00
1	Firewall ISA Server 2004 Guayaquil	$ 500.00
		$ 1,000.00

Costos mensuales

Cantidad	Descripción	Costo
1	Conexión a Internet (corporativo TV Cable 1Mbps) Quito	$ 79.90
1	Conexión a Internet (TV Cable 1Mbps) Guayaquil	$ 34.90
		$ 114.80

Al implementar una VPN utilizando Isa Server 2004, se requiere una inversión inicial de $1000 y además un gasto fijo mensual de $114.80. Debe tomarse en cuenta que la inversión inicial debe darse cada año por motivo de renovación del *firewall*, siendo el análisis válido para un año a partir de la compra del programa.

Según el análisis de costos detallado en cada alternativa de implementación, la opción más económica sería implementar la VPN mediante Hardware, que además provee una mayor seguridad y rendimiento, por ser equipo dedicado a esta función.

2.6 PROTOCOLOS DE SEGURIDAD

Es necesario saber que protocolos se pueden utilizar en cada una de las alternativas de VPN.

Las características de los protocolos se encuentran en el capítulo 1.4

2.6.1 PROTOCOLOS PARA VPNs MEDIANTE SOFTWARE

2.6.1.1 LogmeInHamachi

Los protocolos que se utilizan para proveer seguridad a la VPN creada son:

- Protocolo de cifradoAES-256
- Protocolo RSA
- Protocolo de autenticaciónHMAC-SHA-1
- Protocolo de intercambio de clave*Diffie-Hellman* con el grupo 2048 bits

2.6.1.2 Windows Server 2003

Los protocolos que utiliza Windows para dar seguridad a la VPN son:

- Protocolos de conexión: L2TP/IPSec o basadas en PPTP.
- Protocolo EAP
- Protocolo de autenticación MS-CHAPv2
- Protocolo de autenticación MS-CHAP
- Protocolo de autenticación CHAP
- Protocolo de autenticación SPAP
- Contraseña no cifrada PAP

2.6.2 PROTOCOLOS PARA VPNs MEDIANTE *HARDWARE*

Existe una variedad en los protocolos que se utilizan para proveer seguridad a la VPN creada:

- Protocolo de encriptación3 DES
- Protocolo de encriptación AES 192
- Protocolo de encriptación AES 256
- Protocolo de encriptación AES 128
- Protocolo de autenticación MD5

- Protocolo de autenticación SHA1

2.6.3 PROTOCOLOS PARA VPNs MEDIANTE *FIREWALL*

Son realmente pocos los protocolos que se utilizan en las VPNs mediante *firewall:*

- Protocolos de conexión L2TPa través de IPSec
- Protocolos de conexiónPPTP
- Protocolo IPSec

2.6.4 PROTOCOLOS DE TÚNEL

Los protocolos PPTP, L2F y L2TP se enfocan principalmente a las VPN de acceso remoto, mientras que IPSec se enfoca mayormente en las soluciones VPN de sitio a sitio.

2.6.4.1 Comparación entre PPTP y L2TP

- Con PPTP, el cifrado de datos comienza después de que la conexión se procese (y, por supuesto, después de la autentificación PPP). Con L2TP/IPSec, el cifrado de datos empieza antes de la conexión PPP negociando una asociación de seguridad IPSec.
- Las conexiones PPTP usan MPPE, un método de cifrado basado en el algoritmo de encriptación Rivest-Shamir-Aldeman (RSA) RC-4, y usan llaves de 40, 56 o 128 bits. Las conexiones L2TP/IPSec usan *Data Encryption Standard* (DES), con llaves de 56 bits para DES o tres llaves de 56 bits para 3-DES. Los datos se cifran en bloques (bloques de 64 bits para el caso de DES).
- Las conexiones PPTP requieren sólo autentificación a nivel de usuario a través de un protocolo de autentificación basado en PPP. Las conexiones

L2TP/IPSec requieren el mismo nivel de autentificación a nivel de usuario y, además nivel de autentificación de máquina usando certificados digitales.

2.6.5 PROTOCOLO DE CONFIGURACIÓN DINÁMICA DHCP

El protocolo de configuración dinámica de Host o DHCP es un protocolo que permite a los administradores de red automatizar y gestionar de manera centralizada la asignación de direcciones del protocolo Internet (IP) en una red de una organización o de un proveedor de servicios de Internet (ISP). Usando el conjunto de protocolos de Internet (TCP/IP), cada ordenador que puede conectarse a Internet necesita una dirección IP exclusiva. Cuando una organización configura los ordenadores de diferentes usuarios para que éstos se conecten a Internet, debe asignar una dirección IP a cada ordenador.

Sin DHCP, la dirección IP debe ingresarse manualmente en cada ordenador, y si los ordenadores cambian de sitio a otro lugar de la red, hay que introducir una nueva dirección IP. DHCP permite al administrador de la red supervisar y distribuir las direcciones IP de forma centralizada enviando automáticamente una nueva dirección IP cada vez que un ordenador se conecta en un lugar diferente de la red o cuando llama al ISP.

DHCP usa el concepto de "alquiler" o "préstamo" de dirección IP, cuyo significado es que una dirección IP determinada será válida para un ordenador durante un cierto período de tiempo. La duración del préstamo puede variar dependiendo de cuánto tiempo suele conectarse a Internet el usuario de una ubicación determinada. Es especialmente útil en educación y en otros entornos en los que los usuarios cambian con frecuencia. Utilizando "préstamos" muy cortos, DHCP puede reconfigurar dinámicamente las redes en las cuales hay más ordenadores que direcciones IP disponibles.

CAPÍTULO 3. DISEÑO E IMPLEMENTACIÓN DE LA VPN

En este capítulo se establecerá tanto el número de equipos de usuario como el número de conexiones promedio al servidor. Además se analizaráel software que permite el acceso a la base de datos de importaciones.

Posteriormente se realiza el diseño de la VPN en función del tráfico requerido. Finalmente con el diseño se configura el enlace VPN de prueba, y la conexión con la base de datos de importación.

3.1 ANÁLISIS DE LA SITUACIÓN ACTUAL DEL TRÁFICO, APLICACIONES Y SERVICIOS EN LA RED DE LA EMPRESA OPTIMSOFT

3.1.1 MONITOREO DE LA RED QUITO

Se realiza el análisis de la situación actual del tráfico, mediante el monitoreo de la tarjeta de red del servidor Quito, ya que en este servidor se encuentra la base de datos db_impo a la cual se va a interconectar desde Guayaquil.

Los datos que se obtuvieron durante el monitoreo con el programa PRTG *Traffic Grapher* se puedenobservar en la figura 3.1. El servidor en ocasiones llega a utilizar gran cantidad del AB total, esto depende directamente de la cantidad de documentación que se respalda en el servidor y su uso para ser modificado.

En el servidor se encuentran: la base de datos db_impo y la base de datos de los documentos escaneados, la que ocupa una gran parte del AB.

Ladocumentación del monitoreo desde Enero 2012 aDiciembre2012,se encuentra en el Anexo B.Refleja que los meses de mayor tráfico son:Octubre 106,72 KB/s

por los muchos trámites que se realizan por motivo de mercaderías para navidad; Enero91,38KB/s; Noviembre 74.70 KB/s.

En el monitoreo se observa que existen cortes, esto se debe que en la empresa solo se trabaja de Lunes a Viernes o son días festivos.

Los picos individuales están: 14 de Julio 2012 (21,424 KB/s) a pesar de ser sábado ese día se trabajo por tener muchos trámites retrasados en su ingreso en la base de datos. 26 de Enero 2012 (16,383 KB/s)

En la figura 3.1 se indica el monitoreo de la tarjeta de red del servidor Quito que se realizó desde Enero del 2012 a Diciembre del 2012.

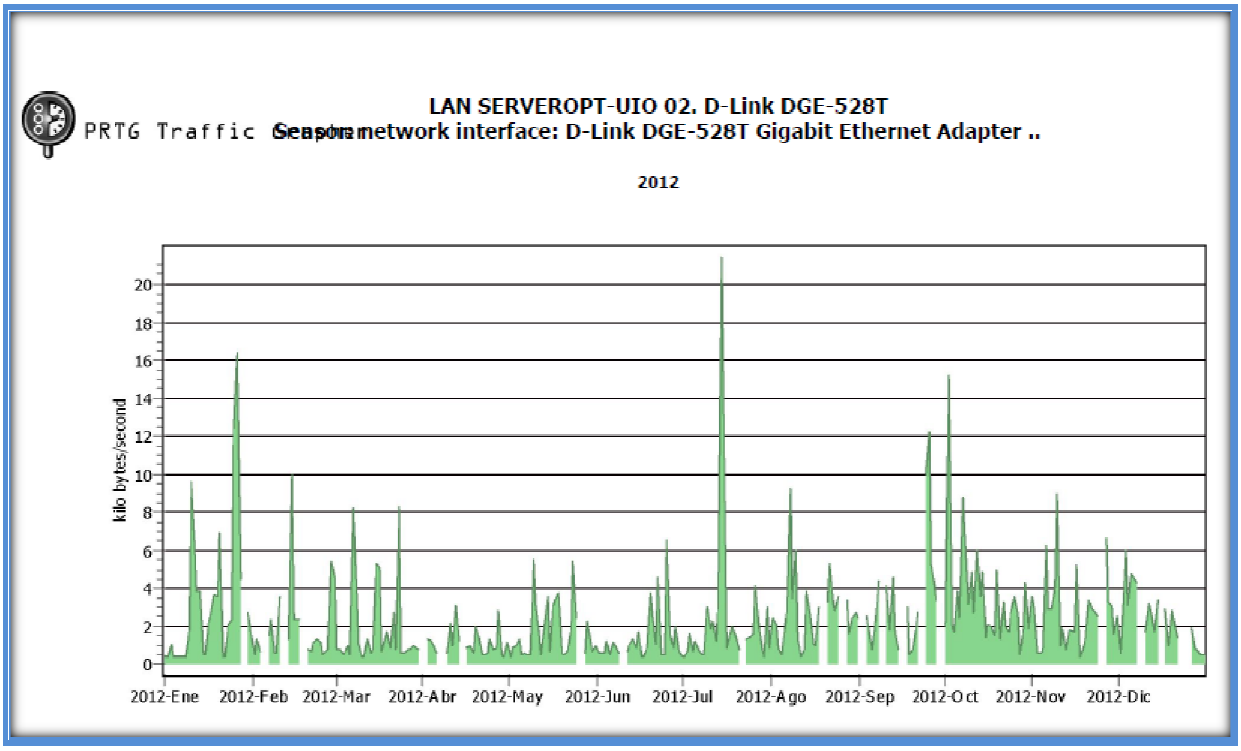


Figura 3.1 Monitoreo de la tarjeta de red del servidorUIO

3.1.2 DESCRIPCIÓN DE LA EMPRESA

Los datos siguientes que corresponden a la descripción de la empresa fueron proporcionados por la empresa Optimsoft Cia. Ltda.

3.1.2.1 Antecedentes de la empresa Optimsoft Cia. Ltda.

OPTIMSOFT CIA. LTDA., es una empresa que brinda servicios, asesoría y capacitación, en el área de COMERCIO EXTERIOR. Cuenta con los siguientes servicios:

- TRÁMITES DE ADUANA O NACIONALIZACIÓN
- TRÁMITES DE ADUANA O NACIONALIZACIÓN *IN HOUSE*
- CONSULTORÍA Y CAPACITACIÓN EN COMERCIO EXTERIOR
- SISTEMAS INTEGRADOS DE COMERCIO EXTERIOR - SICE

Es una empresa líder en el mercado, que brinda servicios a nivel nacional e internacional. Siendo una empresa joven, cuenta con amplia aceptación en el mercado, logrado en base a un alto nivel técnico, calidad en productos y servicios, trato profesional al cliente, garantía en el cumplimiento de los plazos y costos acordados con el cliente.

3.1.2.1.1 Trámites de Aduana o Nacionalización

La empresa ofrece además los siguientes servicios aduaneros:

Importaciones:

1. Registro de Datos en la SENAE[36]
2. Apertura de Documentos Previos
3. Retiro de guías de Transporte (En caso de Importaciones)

[36]SENAE.- Servicio Nacional de Aduana del Ecuador

4. Elaboración de documentación para desaduanización
5. Trámite de Desaduanización
6. Transporte
7. Entrega de la mercancía importada

Exportaciones:

1. Registro de Datos en la SENAE
2. Certificados
3. Orden de Embarque
4. Trámites Aduaneros

Ingreso de mercancías al amparo de regímenes especiales:

1. Importación temporal con reexportación en el mismo estado.
2. Importación amparada en el régimen de maquila.
3. Importación de bienes a Depósito Industrial para la fabricación de productos destinados a la exportación.
4. Importación temporal para perfeccionamiento activo, (materias primas, bienes intermedios y envases), que luego serán exportados.
5. Importación de bienes para exhibición en Ferias Nacionales o Internacionales.
6. Presentación de estados auditados de importaciones realizadas.
7. Control y Cancelación de Garantías.

Trámites Legales:

1. Trámite de Reintegro de Tributos (*DRAW BACK*).
2. Impugnación de Aforo sobre Valoración o Clasificación Arancelaria.
3. Impugnaciones a Rectificaciones de Tributos.
4. Reclamos de Pago Indebido.

Otros servicios:

1. Transporte interno de mercancías.
2. Servicio integral de movilización de carga desde y hacia cualquier país con tercerización de prestigiosas empresas asociadas.

3.1.2.1.2 Trámites de Aduana o Nacionalización - In House

Crea un nuevo concepto de servicio, con el objetivo de que el cliente pueda mantener un mayor control sobre todas sus operaciones aduaneras en forma directa.Para lo cual proporciona todo el contingente dentro de su empresa como: Personal capacitado con experiencia en el área de comercio exterior, Sistemas integrados de comercio exterior, equipos informáticos, accesos directos a Aduana, etc.

El cliente proporciona únicamente un espacio físico dentro de su empresa, y comunicaciones como Internet dedicado.

3.1.2.1.3 Consultoría y Capacitación en Comercio Exterior

Mantienepermanentemente actualizados a los clientes sobre los constantes cambios que surgen en las áreas de Comercio Exterior, para lo cual desarrollados ámbitos de actividad que son: Capacitación y Consultoría.

En el ámbito de Capacitación desarrollacursos relativos a reformas trascendentales que tienen influencia en las diversas actividades del Comercio Exterior Ecuatoriano, relacionadas con la parte informática y con la normativa legal aduanera.

En lo que tiene relación con la Consultoría, resuelve desde impugnaciones a problemas o litigios de carácter aduanero, hasta reclamos de carácter administrativo, tributario, de clasificación arancelaria y de valor en aduana de las

mercancías; así como también reclamos por pago indebido de importaciones aduaneras ya ejecutadas.

3.1.2.1.4 Sistemas Integrados de Comercio Exterior - SICE

Permite a los Operadores de Comercio Exterior realizar todas sus operaciones aduaneras (manejo, control y optimización) de importación y exportación con la aduana del Ecuador.

Optimiza recursos, cálculos rutinarios y el trabajo operativo que se utilizan en negocios de Comercio Exterior mediante el especialista que puede garantizarle total eficacia y seguridad.

Mediante SICE Profesional se logra que los recursos humanos, materiales y tecnológicos produzcan la mayor rentabilidad para la empresa y no se pierda energía, tiempo, dinero, y principalmente, visión.

3.1.2.2 Objetivo de la empresa Optimsoft Cia. Ltda.[1]

El objetivo de la empresa Optimsoft Cia. Ltda. es brindar óptimos servicios y soluciones informáticas integradas, que permitan administrar, controlar y optimizar las operaciones de Comercio Exterior, de tal manera que el nivel ejecutivo y el personal de la organización pueda disponer de información y conocimiento que faciliten la toma de decisiones, así como sus tareas y mejoren su productividad.

Se integra toda la información requerida, así como también se dispone de un sistema de consultas muy versátil que permite:

- Mejorar la manipulación y almacenamiento de la información.
- Disponer de una metodología de ingreso y consulta de datos amigable a los usuarios.

- Agilitar el proceso de obtención de información por medio de consultas para el respectivo análisis.
- Obtener los reportes necesarios para la gestión de la organización.
- Personalizar los sistemas de Comercio Exterior con la finalidad de diseñarlo de acuerdo con las necesidades específicas de la organización y si es necesario integrarlo a otros sistemas internos.

3.1.2.3 Misión de la Empresa[2]

Desarrollar productos y servicios de alta calidad para los operadores de Comercio Exterior a nivel nacional e internacional, y por medio de éstos satisfacer las necesidades de sus clientes, las expectativas de sus accionistas y colaboradores; contribuyendo de esta forma al desarrollo del país y generar una sociedad más justa.

3.1.2.4 Visión de la Empresa

"Siempre ser líder en las actividades de comercio exterior a nivel nacional e internacional. Sustentada en experiencia, alto nivel tecnológico e infraestructura. Permitiendo aplicar permanentemente la calidad y excelencia en nuestros productos y servicios."[2]

3.1.2.5 Valores de la Empresa[2]

- Honestidad
- Respeto
- Compromiso
- Lealtad
- Fe y perseverancia
- Solidaridad
- Práctica de la verdadera amistad
- Igualdad de oportunidades

- Orden, puntualidad y disciplina

3.1.2.6 Sistemas de Información

La empresa Optimsoft cuenta con los siguientes sistemas transaccionales para el manejo de sus procesos internos, tanto de Comercio Exterior como de mercadeo:

- SICE Profesional
- Easy Marketing
- SICE ProScan

También utiliza sistemas en línea para el manejo de sus procesos internos:

- Google Apps (gratuito) que se utiliza en las siguientes aplicaciones:
    - Correo Gmail
    - Google Calendar
    - Google Docs

3.1.2.6.1 Sistema SICE Profesional

La VPN que se implementará permitirá acceder a la base de datos db_impo que corresponde al Sistema SICE Profesional, por lo que se realizará un análisis más detallado del sistema, para poder tener claro todas las consideraciones al momento del diseño de la VPN.

a. Antecedentes de la Creación del Sistema SICE Profesional

La ingeniería de software aplicada a los sistemas de comercialización permite a los profesionales de las empresas hacer un mejor uso de su talento, dedicándose a tareas de análisis y decisión, dejando los cálculos rutinarios y trabajo operativo al computador.

Debido a los constantes cambios que sufre el área de Comercio Exterior, es de imperiosa necesidad contar con una plataforma de sistemas que soporten nuevos requerimientos tecnológicos y se adapten rápidamente a las nuevas condiciones del mercado. La solución tecnológica SICE Profesional en su versión actual 2011.0.5, facilita el trabajo de las personas de Comercio Exterior.

b. Alcance del Sistema SICE Profesional

El sistema SICE Profesional v 2011.0.5, comprende los siguientes módulos generales:

Aranceles y legislación aduanera

- ARANCEL NACIONAL DE IMPORTACIONES (Derechos, tasas, autorizaciones previas, exoneraciones, etc.)
- ÍNDICE COMERCIAL DE MERCADERÍAS
- ÍNDICE ALFABÉTICO DE LA NOMENCLATURA
- ÍNDICE DE VEHÍCULOS AUTOMOTORES-REPUESTOS
- CONSULTAS CON DIFERENTES CRITERIOS
- LEGISLACIÓN ADUANERA (Ley orgánica de aduanas, reglamento de la LOA, ley y reglamento consolidados, instructivo para el llenado del DAU[37] y DAV[38], etc.)

Importaciones

- Apertura de pedidos o trámites
- Ingreso de ítems
- Notas de pedido

[37]DAU.- Declaración Aduanera Única

[38]DAV.- Declaración Andina de Valor

- Declaración aduanera única (DAUA, B, C)
- Autoliquidación de pagos de impuestos aduaneros (pre liquidación – presupuestación)
- Declaración Andina de Valor (DAV)
- Control y seguimiento de las importaciones (estado en que se encuentra la importación)
- Análisis *lead time* (control de tiempos del proceso de importación).
- Análisis *landed cost* (liquidación de costos del proceso de importación).
- Liquidación de costos por ítem
- Consultas / estadísticas / reportes de las importaciones (historias)
- Productos-proveedores / proveedores-productos
- Maestro de exportadores / proveedores, maestro de clientes / importadores, etc.
- Consulta / mantenimiento de catálogos (países, puertos, almacenes, tipos de cambio, etc.)
- Manejo de regionales, agencias
- Importación de productos de la empresa
- Codificación internacional

Teledespacho

- Captura de certificados de inspección desde la www.aduana.gob.ec
- Captura de manifiestos electrónicos desde la www.aduana.gob.ec
- Captura de tipos de cambios desde la www.aduana.gob.ec
- Envío- recepción de DAU-e, DAV automático y directamente
- Interfaz de conexión para envío, recepción automática
- Validación local de envíos de información
- Generación automáticas de DAU’s para envío, vía *email* o dispositivo físico
- Reporte para corrección de errores local
- Reporte de errores por transmisión electrónica
- Control de estados de la declaración por envío

- Control de proveedores y facturas por proveedor
- Ayudas sobre teledespacho en línea

c. Características

- Arquitectura cliente – servidor.
- Base de datos SQL Server 2000, Visual Basic 6.0
- Soporta multi-empresa / multi-agente, multi-usuario.
- Posee esquema de seguridades (Usuarios, roles, transacciones autorizadas).
- Sistema paramétrico, permite configurar el sistema de acuerdo a los catálogos e información propia de la entidad.
- Sistema fácilmente personalizable de acuerdo a las necesidades propias de cada entidad.
- Integración con nuevos módulos o ya existentes en la entidad.
- Desarrollo de interfaces con otros módulos de la entidad.
- Importación y exportación de archivos.
- Controles automáticos sobre todos los Convenios Bilaterales y Multilaterales (ALADI, Comunidad Andina), etc.

d. Requerimientos para ejecutar el Sistema SICE Profesional

- SERVIDOR: Equipo con procesador Pentium IV o superior, 1GB en memoria RAM, 150 MB de espacio libre en disco
- CLIENTES: Equipo con procesador Pentium III o superior, 512 MB en memoria RAM, 100 MB de espacio libre en disco
- Sistema Operativo para servidor Windows NT, 2000, o XP.
- BDD, SQL Server 2000 o mayor.
- Internet y correo seguro (Para Teledespacho).
- MS-Officce 2003 o superior (Interacción con Excel para reportes).
- Recomendable Impresora matricial para formularios preimpresos.

e. Escenario de funcionamiento del sistema SICE Profesional

Se debe resaltar que en la actualidad el Sistema SICE Profesional solo se implementa en redes LAN. El uso de una VPN se hace indispensable debido a que la empresa y muchos clientes tienen su base de datos centralizada en una Oficina Matriz y se requiere acceder a la base de datos db_impo, donde se encuentra almacenada la información, desde usuarios remotos u oficinas en otras ciudades (sucursales).

3.1.2.6.2 Análisis de la Base de Datos de importaciones (db_impo[39])

El sistema SICE Profesional utiliza la base de datos de importaciones denominada **db_impo**, la cual está creada en el motor de base de datos Microsoft SQL Server 2000. El servidor donde se encuentra dicha base de datos db_impo cuenta con las siguientes especificaciones:

- Sistema Operativo: Microsoft Windows Server 2003 R2 *Enterprise Edition*, *Service pack 2*
- Procesador: Intel Corel 2 Quad de 2.66GHz
- Memoria RAM: 3.96GB

El servidor de base de datos de la empresa Optimsoft utiliza los 4 procesadores que posee, y su seguridad se basa en proporcionar autentificación mediante cuentas de SQL, con las propiedades que se detallan en las figuras3.2a y 3.2b.

En la figura 3.3, se puede observar las características de la base de datos db_impo a la que seaccederá mediante el sistema SICE Profesionalusando la VPN.

[39]db_impo: Base de importaciones del software SICE Profesional

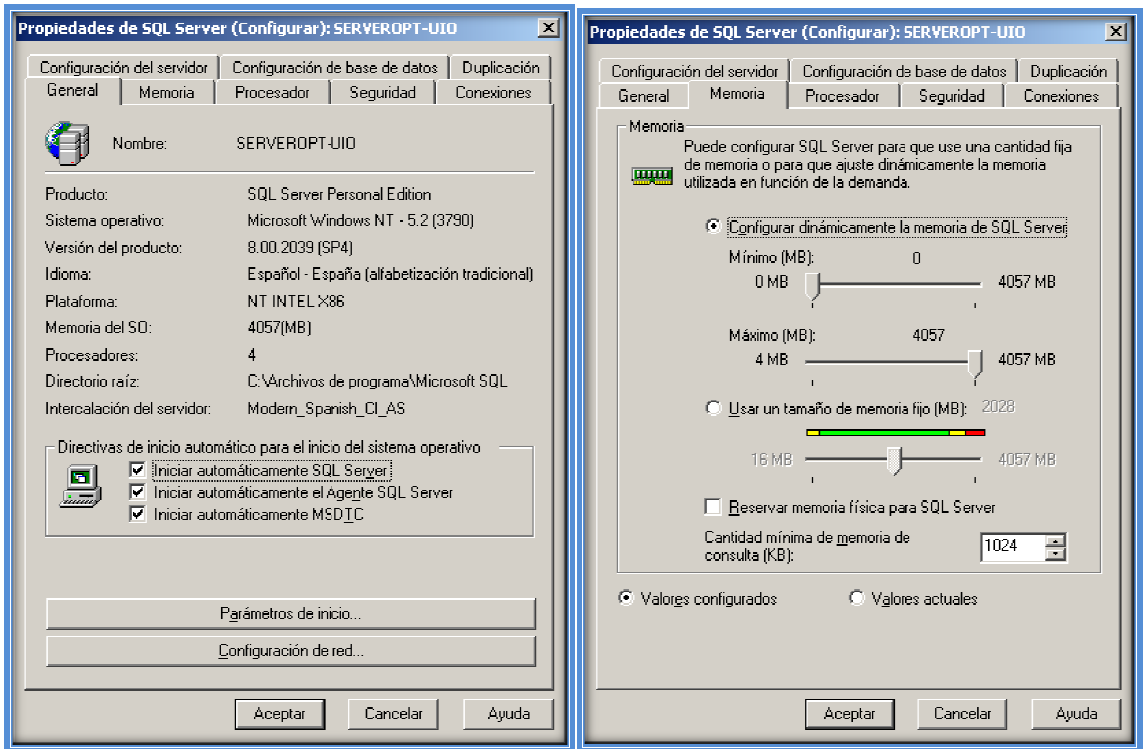


Figura 3.2a Propiedades del servidor SQL de la empresa Optimsoft Cia. Ltda.

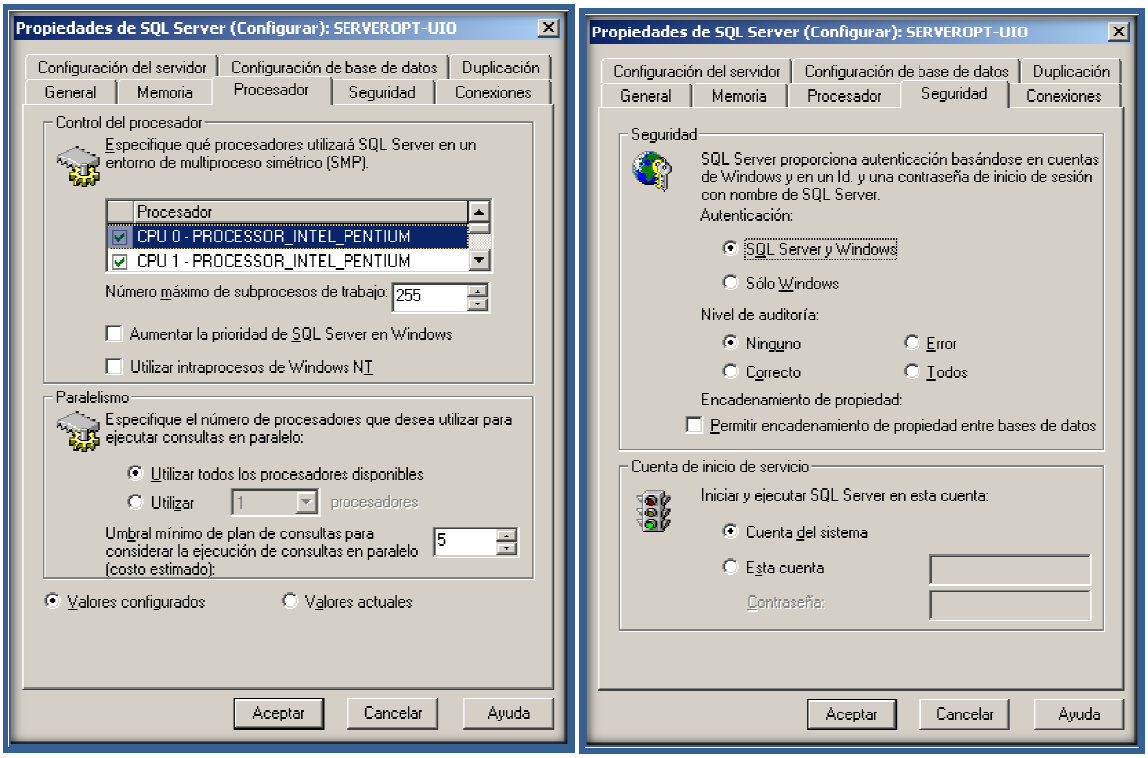


Figura 3.2b Propiedades del servidor SQL de la empresa Optimsoft Cia. Ltda.

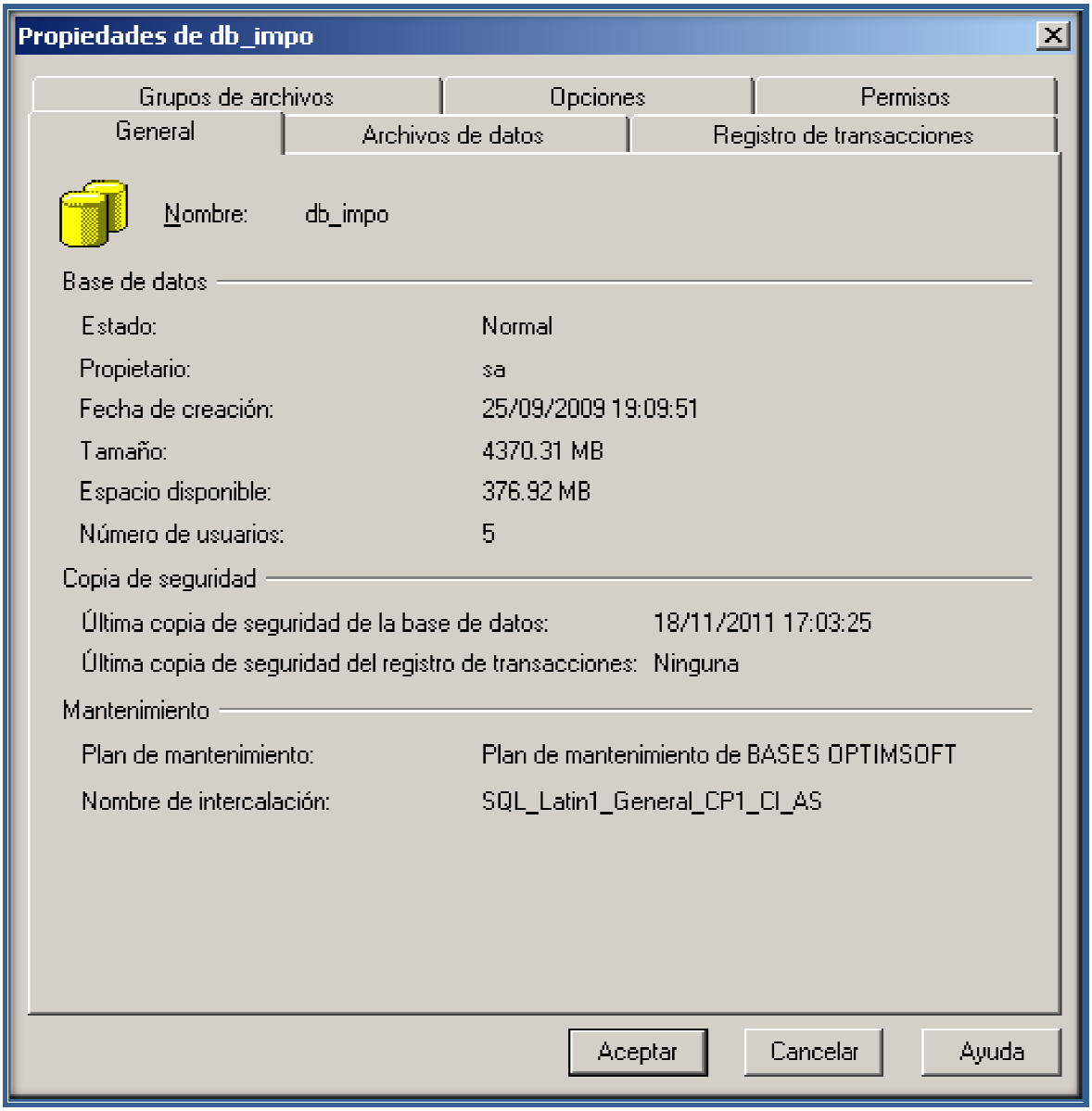


Figura 3.3 Características de la Base de Datos db_impo

3.1.2.6.3 SICE Pro Scan

SICE Pro Scan, es un sistema de digitalización de trámites de Aduana en importaciones y exportaciones.

Permite digitalizar los documentos de un trámite como DAU, DAV, Factura Comercial, Guías, Póliza, etc., apoyados en interfaces de usuario muy sencillas y en base de datos muy segura.Mediante esta aplicación el Operador de Comercio

Exterior puede dar cumplimiento a las exigencias y disposiciones de la Corporación Aduanera Ecuatoriana

Solución utilizada por pequeñas, medianas y grandes empresas que desarrollan la actividad de Agentes de Aduana,debido a que permite archivar digitalmente la documentación generada en los trámites de importación o exportación para su posterior consulta una vez terminado el trámite. Proporciona la máxima facilidad de uso y el mayor rendimiento aún en las necesidades de negocio más exigentes.

3.1.2.6.4 Easy Marketing

Es una herramienta que permite Administrar y Controlar procesos de ventas, *marketing*, negocios y servicio al cliente.

Es una herramienta de análisis, mejora la toma de decisiones de su organización, automatiza los procesos de ventas, mercadeo y maximiza los niveles de Servicio al Cliente.

Posee una Base de Datos de más de 6.000 registros de empresas de todo el sector productivo a nivel nacional, los cuales pueden ser segmentados de acuerdo al mercado objetivo.

3.1.2.7 Esquema actual de la red Optimsoft Matriz Quito

Como se puede observar en la figura 3.4 (Red Optimsoft Matriz-Quito) la empresa tiene 5 departamentos:

Departamento de Contabilidad.- Se encarga de la parte financiera de la empresa, maneja cobros y emisión de facturas a clientes tanto de Quito como de Guayaquil; se encuentra una sola persona a cargo de este Departamento.

Departamento de Operaciones.- Se encargan de todo lo correspondiente a Comercio Exterior, como desaduanización, e ingreso de documentos escaneados a la base de datos; se encuentran 3 personas a cargo.

Departamento de Producción.- Es donde se realiza el mercadeo, venta y suscripción a los productos que tiene la empresa; está a cargo de este Departamento una persona.
Departamento de Sistemas.- Es donde se encargan de la transmisión de datos para la sucursal y también del desarrollo de nuevos productos en el área informática y de soporte a clientes del sistema SICE Profesional.

Departamento de Recepción.- Se encarga de la atención al cliente y direccionarlo al departamento que corresponda en cualquier requerimiento.

3.1.2.8 Esquema actual de la red Optimsoft Sucursal Guayaquil

Como se puede observar en la figura 3.5 (Red Optimsoft Matriz-Guayaquil) la empresa tiene 2 departamentos:

Departamento de Operaciones.- Se encargan de todo lo correspondiente a la parte de Comercio Exterior que tenga que ver con la Aduana de Guayaquil, es necesario verificar o incluso modificar documentos ingresados en Quito para lo cual se utiliza correos electrónicos.

Departamento de Recepción.- Se encarga de la atención al cliente y direccionarlo al departamento que corresponda en cualquier requerimiento.

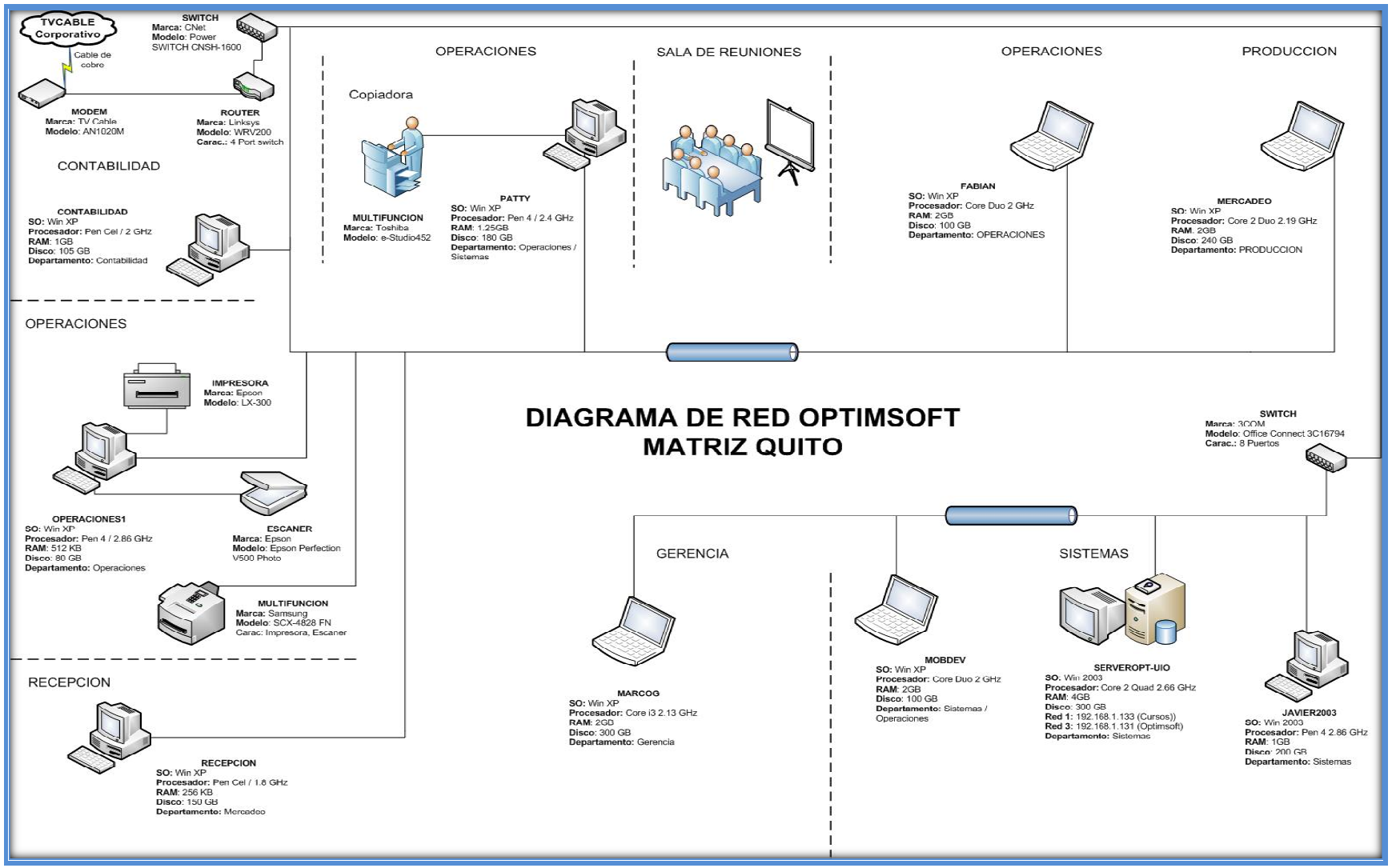


Figura 3.4 Diagrama red Optimsoft Quito

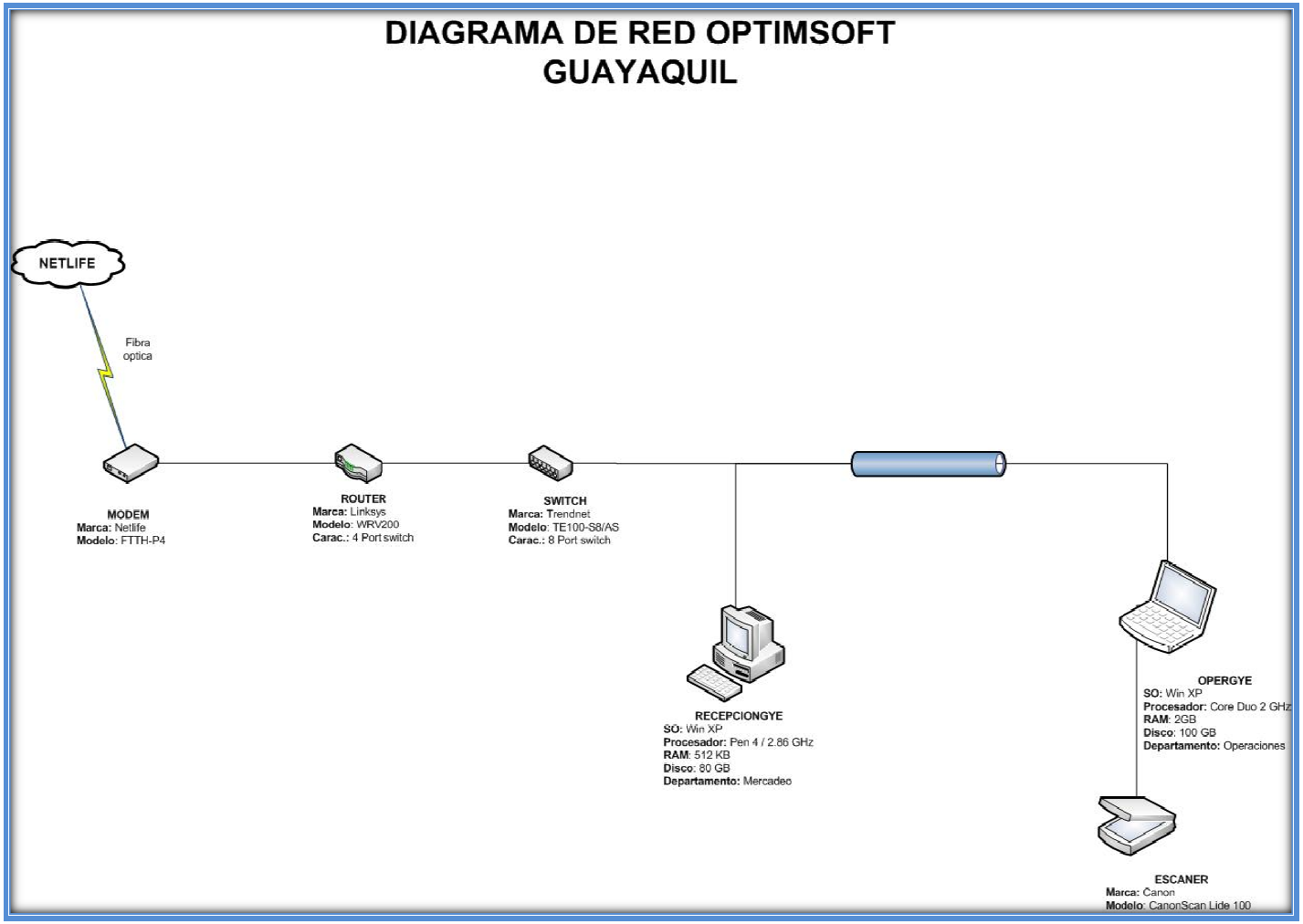


Figura 3.5 Diagrama red Optimsoft Guayaquil

3.1.2.9 Descripción de las Aplicaciones actuales que generan tráfico en la red Optimsoft Quito

Actualmente los empleados de la empresa Optimsoft utilizan múltiples aplicaciones que facilitan su desempeño laboral, las mismas que generan tráfico en la red.

A continuación se detallan brevemente las aplicaciones, para poder tener un mejor conocimiento del ancho de banda que necesita la empresa.

- Google Apps
    - Correo
    - Calendario
    - Documentos

- Redes Sociales
- Soporte Remoto
- Acceso a la Base de Datos db_impo
- Correo seguro

Google Apps

Es un conjunto de aplicaciones web que permite aumentar la productividad de pequeñas, medianas y grandes empresas, ayudándolas a que su trabajose realice de manera más eficiente, permitiendo comunicar, organizar y colaborar desde cualquier lugar.

En la tabla 3.1 se indica las características de Google Apps y Google Apps for Business

	Google Apps (Gratis)	Google Apps for Business
Máximo de usuarios Cuentas de usuario permitidas por organización	10*	Sin límites
Aplicaciones de mensajería: Gmail y Google Calendar	SI	SI
Aplicaciones de colaboración: Google Docs y Google Sites	SI	SI
Más aplicaciones de Google: Google Reader, Blogger, Álbumes Álbumes web de Picasa, AdWords y más.	SI	SI
Otras aplicaciones para empresas: Google Video para empresas y Google Groups for Business	NO	SI
Funciones para empresas: 25 GB de almacenamiento de correo electrónico por usuario, Interoperabilidad con BlackBerry y Microsoft Outlook, entre otros.	NO	SI
Herramientas de control para empresas: SSO, SSL forzado, requisitos de seguridad de contraseña personalizados y más	NO	SI
Asistencia y confiabilidad para empresas: SLA con garantía de tiempo de actividad del 99,9% y Asistencia las 24 horas, los 7 días de la semana.	NO	SI

Tabla 3.1 Comparación Google Apps con Google Appsfor Business[3]

*Las políticas del año 2007 cuando recién inició Google Apps eran entregar 100 usuarios, por lo que la Empresa Optimsoft posee Google Apps para 100 usuarios.

Google Apps permite modificar varias configuraciones para aplicar a la empresa.

- Permite subir el logotipo de la empresa para que aparezca en las páginas de acceso y en las propias aplicaciones.

- Permite configurar la dirección de la página de acceso de la empresa, como http://correo.dominio-empresa.com.
- Da la posibilidad de crear y publicar páginas web para el sitio.
- Se puede integrar Google Apps con la infraestructura de TI[40] actual de la empresa.

a. Correo Gmail

Logra una comunicación más fácil al utilizar: envío de correos electrónicos, mensajes, redacción de correos, llamadas por teléfono o video llamadas desde una sola interfaz.

b. *Gmail Offline*

Es una extensión para el navegador Google *Chrome*;se puede usar el correo electrónico cuando la conexión a Internet no está activa, permitiendo responder *emails*, organizarlos, leeros o archivarlos. El momento en que la conexión esté activa de nuevo, los datos se sincronizarán para no tener alguna pérdida.

c. *Google Calendar*

Permite organizar actividades de forma más eficiente, con la programación de reuniones y diseño de proyectos, mediante la visualización de calendariosde colegas y programación de eventos.

d. *Google Docs*

Logra una mejor colaboración mediante la compartición de ideas, trabajo en forma conjunta en tiempo real, haciendo el trabajo más rápido,permitiendo modificar de inmediatodocumentos compartidos.

---

[40]TI.- Tecnologías de la Información

Redes Sociales

La empresa utiliza las redes sociales: Facebook, twitter, y la comunidad de todo comercio exterior, mediante las cuales logra un contacto con todos sus clientes y futuros clientes; la comunidad se utiliza para poder ayudar a personas que necesiten información o asesoría en cualquier ámbito de Comercio Exterior.

Como se puede observar en la tabla 3.2, la empresa tiene un número considerable de miembros en estas redes, por lo que su uso se vuelve parte del día a día en el trabajo.

Canal	Usuarios Registrados	Visitas x mes
Todocomercioexterior	+ 2.000	+ 17.000
Blog Noticias	+ 1.280	+ 10.000
Comunidad	+ 1.450	+ 6.000
Redes Sociales	+ 6.150	+ 1.000
TOTAL TCE.EC	**> 10.880**	**> 34.000**

Tabla 3. 2 Estadísticas de visitas a las redes sociales [4]

Soporte Remoto

La empresa con el fin de ser mucho más eficiente, tiene implementado el acceso remoto mediante *LogmeIn free*, que permite solucionar muchos de los problemas que presenten los clientes en el Sistema SICEProfesional.

El software de LogmeIn permite controlar de forma rápida y sencilla uncomputador remoto a través de la web, similar a estar sentado frente a él. Cabe

resaltar que el momento de la conexión una sola persona puede acceder al uso de dicho computador.

Correo seguro

Es un requisito de la Aduana del Ecuador que todos los operadores de comercio exterior utilicen el correo seguro para la transmisión electrónica de las declaraciones de importación y exportación.

Ingreso a la Base de Datos db_impo

En la empresa las personas encargadas de operaciones, utilizan la base de datos db_impo, para poder realizar los trámites de aduana. El ingreso a la base de datos es de vital importancia ya que allí se encuentra almacenada toda la información que se enviará a la Aduana del Ecuador.

3.2 CÁLCULO DE LA CAPACIDAD NECESARIA DEL CANAL PARA INTERCONECTAR LA BASES DE DATOS DE IMPORTACIÓN DE LA EMPRESA OPTIMSOFT

Se llama capacidad de canal a la velocidadde transmisión a la que se pueden transferir los datos en un canal, normalmente se expresa en bits por segundo (bps). Comercialmente la capacidad del canal se la conoce con el nombre de ancho de banda, término que utilizaremos de ahora en adelante y que por siguiente también se expresa en bps.

El cálculo del ancho de banda que se necesita, se debe realizarlo a partir de ancho de banda que utilizan todas las aplicacionesde la empresa.

Google Apps

En la empresa Optimsoft se utilizan las tres aplicaciones web (gmail, google calendar, google docs); a continuación se analizará el ancho de banda que ocupa cada una de ellas.

a. Correo Gmail

Se considera que por día trabajan 6 personas[5] utilizando esta aplicación (cuentas activas / 8 horas laborables) con un tamaño de 673.7MBytes.

$$ABgmail = \frac{\text{Tamaño gmail(KB)}}{\text{Tiempo de carga(s)}}$$

$$AB\ gmail = \frac{673.7\text{MBytes}/6\ \text{cuentas activas}}{8\ \text{horas}} * \frac{8\text{bits}}{1\ \text{Byte}} * \frac{1\text{hora}}{3600\text{s}}$$

$$\boxed{ABgmail = 0.031189\ \text{Mbps}}$$

$$\boxed{ABgmail = 31.19\ \text{Kbps}}$$

b. Google Calendar

Se calcula la utilización del ancho de banda, en base al tamaño promedio de la página del calendario, que es de 15KBytes;se considera que un tiempo razonable para acceder a la misma es de 5 segundos (tiempo promedio que los empleados están dispuestos a esperar).

$$ABcalendar = \frac{\text{Tamaño calendar(KB)}}{\text{Tiempo de carga(s)}}$$

$$AB\ calendar = \frac{15\ \text{KBytes}}{5\ \text{segu}\square\text{dos}} * \frac{8\text{bits}}{1\ \text{Byte}}$$

$$ABcalendar = 24\ \text{Kbps}$$

c. Google Docs

Se calcula la utilización del ancho de banda, en base al tamaño promedio de los documentos que es de 121.21KBytes, considerando un tiempo razonable para acceder a él de 5 segundos (tiempo promedio que los empleados están dispuestos a esperar).

$$ABdocs = \frac{\text{Tamaño docs(KB)}}{\text{Tiempo de carga(s)}}$$

$$ABdocs = \frac{121.21\ \text{KBytes}}{5\text{(s)}} * \frac{8\text{bits}}{1\text{Byte}}$$

$$ABdocs = 193.94\ \text{Kbps}$$

Redes Sociales

En la empresa Optimsoft se utilizan tres redes sociales: facebook, twitter y la comunidad de todo comercio exterior; a continuación se considera el ancho de banda que ocupa cada una de ellas.

a. Facebook

Se calcula la utilización del ancho de banda, en base al tamaño de la página de facebook que es de 398 KBytes[6]y el tiempo considerado para acceder a ella, se toma como 10 segundos (tiempo promedio que los empleados están dispuestos a esperar).

$$ABfacebook = \frac{\text{Tamaño facebook(KB)}}{\text{Tiempo de carga(s)}}$$

$$ABfacebook = \frac{398\ \text{KBytes}}{10(\text{s})} * \frac{8\text{bits}}{1\text{Byte}}$$

$$\boxed{ABfacebook = 318.4\ \text{Kbps}}$$

b. Twitter

Se calcula la utilización del ancho de banda, en base al peso de la página de twitter que es 154KBytes[6] y el tiempo considerado para acceder a ella se toma como 8 segundos (tiempo promedio que los empleados están dispuestos a esperar).

$$ABtwitter = \frac{\text{Tamaño twitter(KB)}}{\text{Tiempo de carga(s)}}$$

$$ABtwitter = \frac{154\ \text{KBytes}}{8(\text{s})} * \frac{8\text{bits}}{1\text{Byte}}$$

$$\boxed{ABtwitter = 154\ \text{Kbps}}$$

c. Comunidad Todo Comercio Exterior

Se calcula la utilización del ancho de banda en base al peso de la página de la Comunidad de Todo Comercio Exteriorque es 180 Kbytes[7]y el tiempo considerado para acceder a ella que se toma como 12 segundos (tiempo promedio que los empleados están dispuestos a esperar)..

$$ABcomunidad = \frac{\text{Tamaño comu?idad(KB)}}{\text{Tiempo de carga(s)}}$$

$$ABcomunidad = \frac{180\ \text{KBytes}}{12(\text{s})} * \frac{8\text{bits}}{1\text{Byte}}$$

$$\boxed{ABcomunidad = 120\ \text{Kbps}}$$

$$\boxed{ABredes\ sociales = \text{AB facebook} + \text{AbB twitter} + \text{AB comu?idad}}$$

$$\boxed{ABredes\ sociales = 318.4\ \text{Kbps} + 154\ \text{Kbps} + 120\ \text{Kbps}}$$

$$\boxed{ABredes\ sociales = 592.4\ \text{Kbps}}$$

Soporte Remoto

El programa LogmeIn que se utiliza para el soporte remoto recomienda un mínimo de 10 KBps. Depende mucho también de la resolución de la pantalla y profundidad de color, pero 10-12KBps[8]se considera suficiente. Se toma el mayor valor es decir 12KBps.

$$ABsoporte\ remoto = \frac{12\text{KByte}}{1\text{s}} * \frac{8\text{bits}}{1\ \text{Byte}}$$

$$\boxed{ABsoporte\ remoto = 96\ \text{Kbps}}$$

Ingreso a la Base de Datos db_impo

Los trámites que son ingresados a la base de datos db_impo, mediante el Sistema SICE Profesional,tienen un tamaño promedio de 850 KBytes[9]. Se ingresa 1 trámite promedio por hora.

$$AB\ base\ datos = \frac{\text{Tamaño trámite}}{\text{tiempo de e vio}}$$

$$AB\ base\ datos = \frac{850\ \text{KBytes}}{1\text{hora}} * \frac{1\text{hora}}{3600\text{segu dos}} * \frac{8\text{bits}}{1\text{Byte}}$$

$$\boxed{AB\ base\ datos = 1.89\ \text{Kbps}}$$

Correo seguro

Según la información proporcionada por el departamento de sistemas, se tiene que se envía y recibe un máximo de 6 correos [9]en una hora, considerando que su tamaño promedio es de 7KBytes.

$$ABcorreo\ seguro = \frac{\#\text{de correos} * \text{Tamaño correo}}{\text{tiempo de e vio}}$$

$$ABcorreo\ seguro = \frac{6\ \text{correos}}{1\text{hora}} * \frac{7\text{KBytes}}{1\text{correo}} * \frac{1\text{hora}}{3600\text{segu dos}} * \frac{8\ \text{bits}}{1\text{Byte}}$$

$$\boxed{ABsoporte\ remoto = 0.0933\ \text{Kbps}}$$

Descarga de Archivos

Se descargan archivos de 1Mbyte en 1 minuto, que comprenden documentos de clientes.

$$ABdescarga = \frac{\text{Tamaño descarga(Kb)}}{\text{Tiempo de carga(s)}}$$

$$ABdescarga = \frac{1\ \text{MBytes}}{60(\text{s})} * \frac{8\text{bits}}{1\text{Byte}}$$

$$\boxed{ABtwitter = 0.1333\ \text{Mbps} = 133.3\ \text{Kbps}}$$

Para determinar el porcentaje de ancho de banda que estásiendo utilizado por las aplicaciones, se multiplica el ancho de banda utilizado de cada aplicación por el índice de simultaneidad[10].

En la tabla 3.3 se indica el ancho de banda utilizado de cada aplicación y su índice de simultaneidad que el departamento de sistemas de la empresa proporciona, obteniendo un valor total de acuerdo al uso total de la aplicación.

APLICACIÓN	AB Utilizado individual	Índice de simultaneidad	AB Utilizado por aplicación considerando la simultaneidad
Gmail	31.19Kbps	15%	4.67 Kbps
Google Calendar	24 Kbps	5%	1.20 Kbps
Google Docs	193.94Kbps	15%	29.09 Kbps
Redes Sociales	592.4 Kbps	10%	59.24 Kbps
Soporte Remoto	96Kbps	5%	4.8 Kbps
Base de datos	1.89 Kbps	40%	0.76 Kbps
Correo seguro	0.0933 Kbps	5%	0.05 Kbps
Descarga de archivos	133.3 Kbps	5%	6.66 Kbps

Tabla 3. 3 Cálculo del ancho de banda utilizado por cada aplicación

$$AB\ utilizado = (4.67 + 1.2 + 29.09 + 59.24 + 4.8 + 0.76 + 0.05 + 6.66)Kbps$$

$$AB\ utilizado = 106.47\ Kbps$$

Se puede comparar el valor de utilización del ancho de banda con el monitoreo que se ha realizado en la tarjeta de red en el servidor de base de datos en horario de trabajo (8:30 hasta 18:00). Como se puede apreciar, en la figura 3.7 el tráfico de entrada al servidor fluctúa entre 175 Kbps y 25 Kbps;se utilizará el valor de

175Kbps para calcular el porcentaje que está siendo utilizado del ancho de banda de entrada, lo cual corresponde a un 15.9% del ancho de banda de entrada, que es utilizado solamente en la base de datos.

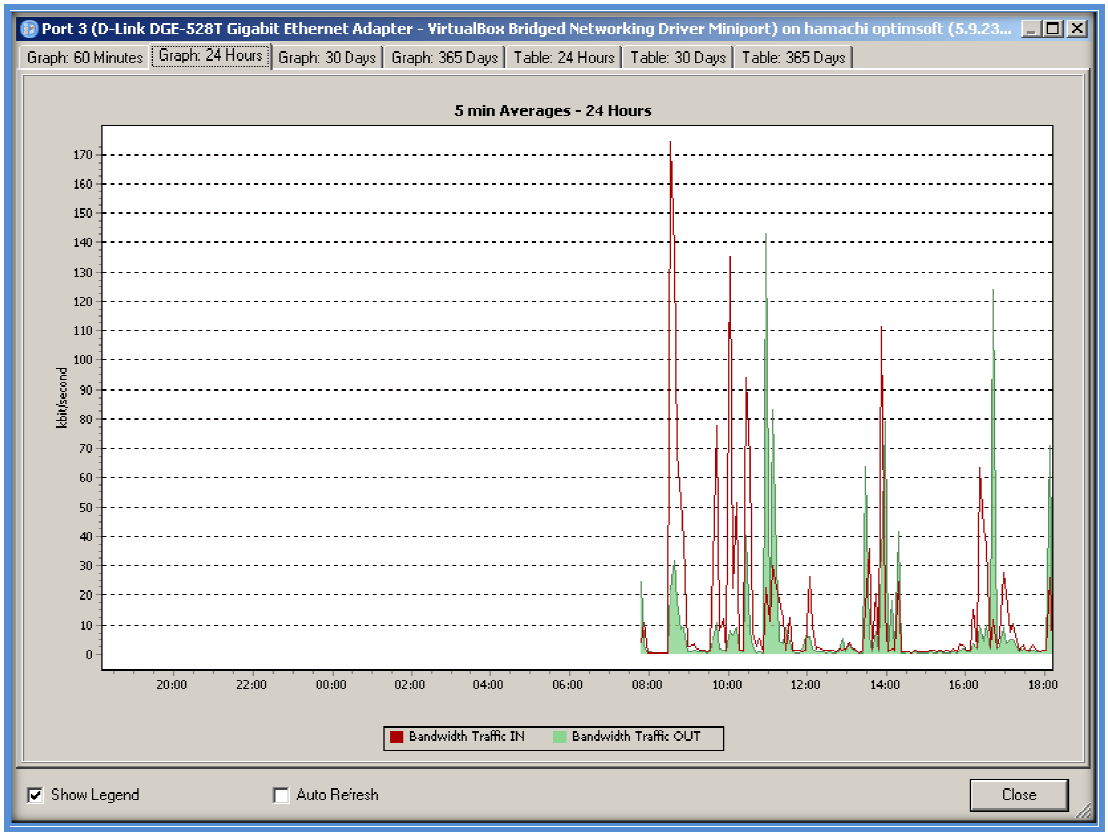


Figura 3.7 Tráfico generado en la base de datos db_impo

El porcentaje del ancho de banda de entrada utilizado se lo calcula: dividiendoel mayor valor de tráfico de entrada monitoreado en el servidor para el total del ancho de banda disponible (contratado).

En la figura 3.6 se muestra el porcentaje de ancho de banda que se ocupa para las aplicaciones existentes.

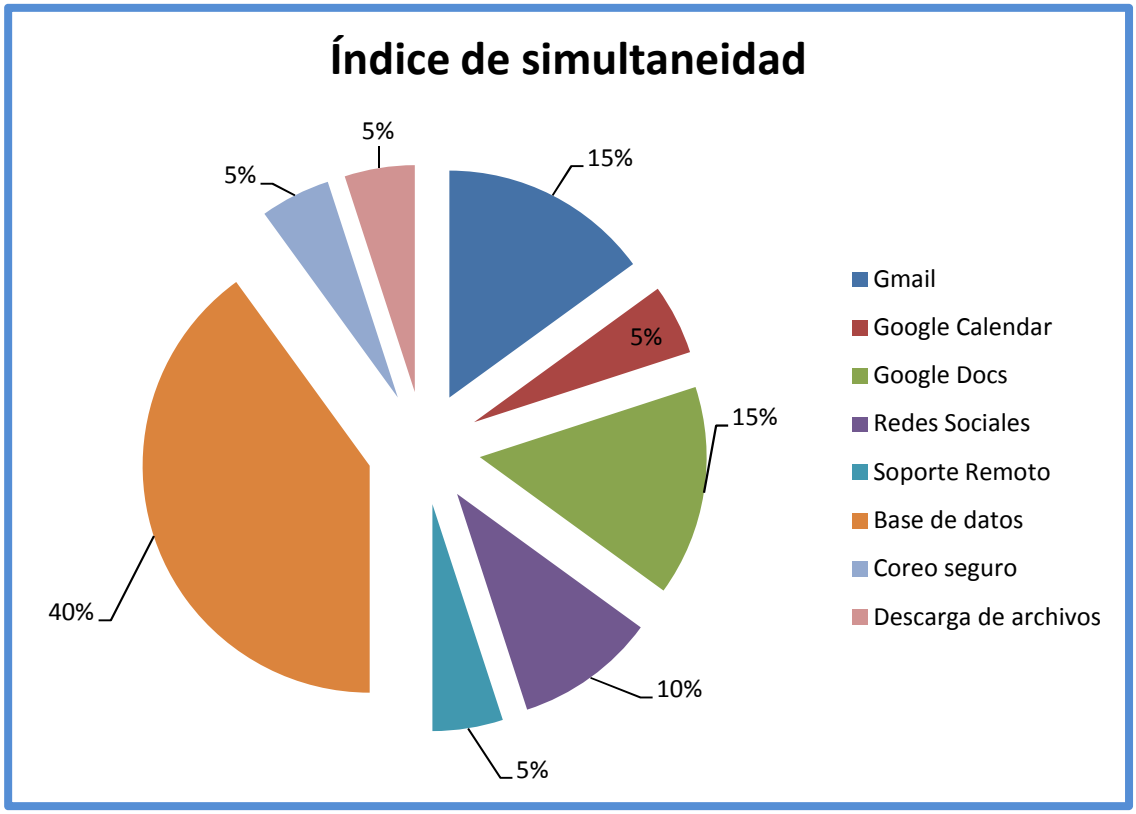


Figura 3.6 Porcentajes de ancho de banda utilizado por las aplicaciones de la empresa Optimsoft

Como se pudo observar en la figura 3.4 existen 9 usuarios de la red LAN, los cuales utilizan una conexión de 1.1 Mbps corporativo[41] provista por el Grupo TV Cable tal como se muestra en la figura 3.8.

El ancho de banda total utilizado por la empresa es igual al ancho de banda utilizado de las aplicaciones por el número de usuarios que las ocupan.

$$AB\ utilizado\ Total = 106.47\ Kbps * 9\ usuarios$$

$$\boxed{AB\ utilizado\ Total = 958.23\ Kbps}$$

[41]Conexión corporativa.-el proveedor realiza una división del canal de transmisión de 1 a 3

Figura 3.8 Velocidad de carga y descarga de Internet de la conexión en Quito

3.3 DISEÑO DE LA VPN

3.3.1 Antecedentes para realizar la VPN

La empresa Optimsoft en Quito accede mediante la red LAN, a la base de datos db_impo donde se almacena toda la información correspondiente a los trámites de aduanas. Mientras que los trámites desde las oficinas ubicadas en Guayaquil, acceden a la información almacenada en la base de datos db_impo, a través delenvío de información vía correo electrónico, lo cual es muy ineficiente, debido a que se necesita ingresar nuevamente los datos de cada formulario con el riesgo de ser modificado en la transmisión.

En la figura 3.9 se indica la manera actual como se accede a la información de la base de datos db_impo entre Quito y Guayaquil, utilizando envíos mediante correos electrónicos.

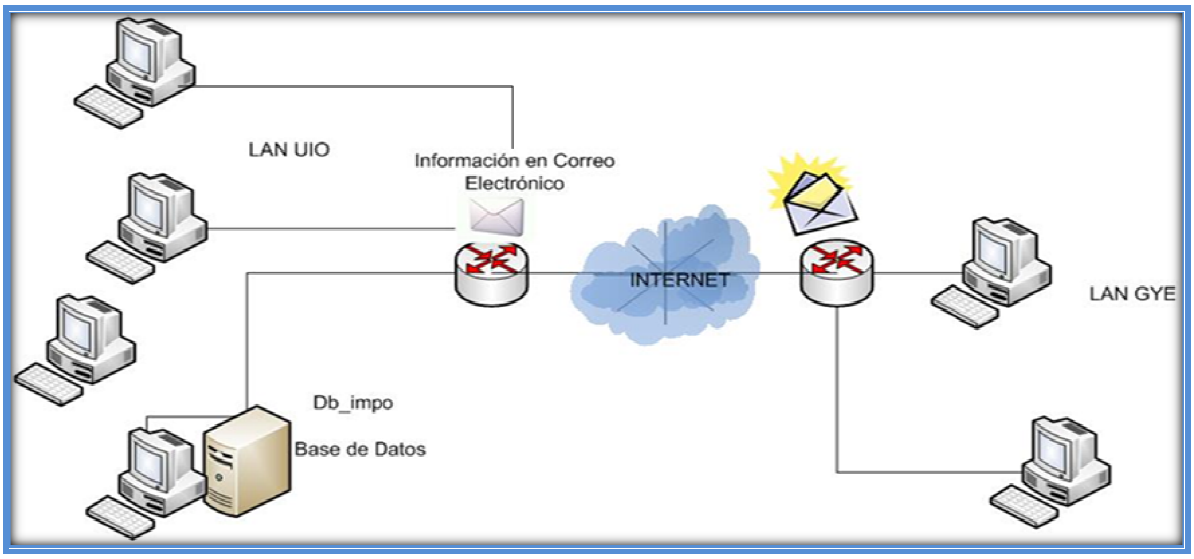


Figura 3.9 Envío de la información UIO- GYE (correo electrónico)

3.3.2 SELECCIÓN DE LA MEJOR ALTERNATIVA DE IMPLEMENTACIÓN

Para poder definir cuál es la alternativa óptima para la empresa Optimsoft, es necesario observar la tabla 2.2, en la cual se encuentran las 3 alternativas de implementación (*software, hardware y firewall*).

Se selecciona la VPN Punto a Punto, ya que es necesario proyectar que en unfuturo se requerirá la interconexión entre las redes LAN de la empresa.

Después de realizar el análisis técnico se ha seleccionado a la VPN *router a router* por ser la implementación que más cumple con los requerimientos de la empresa, tanto en seguridad como en rendimiento, debido a que posee hardware especializado.

Luego de revisar el análisis de costos de la sección 2.5 del Capítulo 2, se pudo establecer que la implementación utilizando hardware es la más económica.

Por lo antes expuesto la VPN a implementarse en las oficinas de Optimsoft, será la VPN de hardware para la cual se utilizarán dos*Routers Linksys* WRV- G 200.

3.3.3 CARACTERÍSTICAS DEL *ROUTER* LINKSYS WRV-G200

Wireless G con*RangeBooster* (WRV200), es parte de una solución empresarial,ya que proporciona a las pequeñas empresas acceso a la red inalámbrica con un modo de gestión fiable, inteligente y con SNMP (Protocolo Simple de Gestión de Redes).

RangeBooster, es una tecnología adicional compatible con la tecnología estándar *Wireless* G, para aumentar hasta el doble la cobertura de red inalámbrica y el rendimiento hasta un 35%. A diferencia de las tecnologías inalámbricas habituales, que pueden ser interferidas por reflejos de señales, *RangeBooster* utiliza dos receptores inteligentes en cada extremo para detectar y decodificar señales a unas distancias a las que no llegan las tecnologías normales. *RangeBooster* proporciona una mejora de la cobertura incluso cuando esté funcionando en una red mixta con dispositivos *RangeBooster* y los habituales Wireless G.[11]

Las características del Router Linksys WRV200*Wireless* G con *Rangebooster* son:

- Incluye una red privada virtual (VPN) que garantiza las conexiones de los trabajadores móviles, así como múltiples SSID (nombre de red) compatibles con QoS inalámbrico (WMM) y QoS con cable (priorización por puerto), que confieren una más uniforme y mayor calidad de voz y vídeo a toda la empresa.
- El protocolo SNMP permite gestionar y controlar a distancia el dispositivo.
- Cuenta con funciones de seguridad: autenticación, cifrado y cortafuegos; además activación/desactivación del SSID[42]*Broadcast*, Filtrado basado en MAC, Prevención por denegación de servicio (DoS).

[42]SSID(*Service Set IDentifier*).- es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de ella.

El objetivo del ataque de denegación del servicio es impedir la comunicación entre un terminal y un puerto de acceso; para esto se hace pasar por AP[43] utilizando su dirección MAC[44] y se niega la comunicación a los terminales elegidos usando continuas notificaciones de desasociación.

Otras características del WRV200

- *RangeBooster* utiliza tecnología MIMO[45] para aumentar la cobertura.
- Múltiples BSSID[46] y VLAN para permitir que haya redes seguras independientes.
- 10 túneles IPsec QuickVPN con un rendimiento de hasta 30 Mbps.
- Mejor calidad de servicio (QoS) tanto para la red por cable como para la inalámbrica, lo que mejora visiblemente la calidad de voz y de vídeo.
- 4 puertos LAN y 4 SSID que pueden asignarse hasta a 5 VLAN.
- Seguridad: *Firewall* SPI, WPA2, 3DES, AES y 802.1x .

3.4 IMPLANTACIÓN Y PRUEBAS DE LA VPN

La implementación de la VPN que permite interactuar con la base de datos db_impo por medio del Sistema SICE Profesional desde la ciudad de Guayaquil, se la realiza en base a la alternativa seleccionada en la sección 3.3.2, del Capítulo 3.

---

[43] AP.- *Access Point*

[44] Dirección MAC (siglas en inglés de *media access control*; en español "control de acceso al medio") es un identificador de 48 bits (3 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red.

[45] Tecnología MIMO (*Multiple-input Multiple-output*),Múltiples entradas múltiples salidas

[46] BSSID (*Basic Service Set Identifier*) es la dirección MAC(física) del AP al que nos conectamos.

3.4.1 CONFIGURACIÓN DE LA VPN DEL ROUTER DE GUAYAQUIL

Es necesario primero configurar la IP local de cada *router* para no tener conflicto al crear la VPN.Como se muestra en la figura 3.10,se selecciona la IP Address 192.168.2.1 para Guayaquil y para el caso de Quito se asigna la IP address 192.168.1.1.

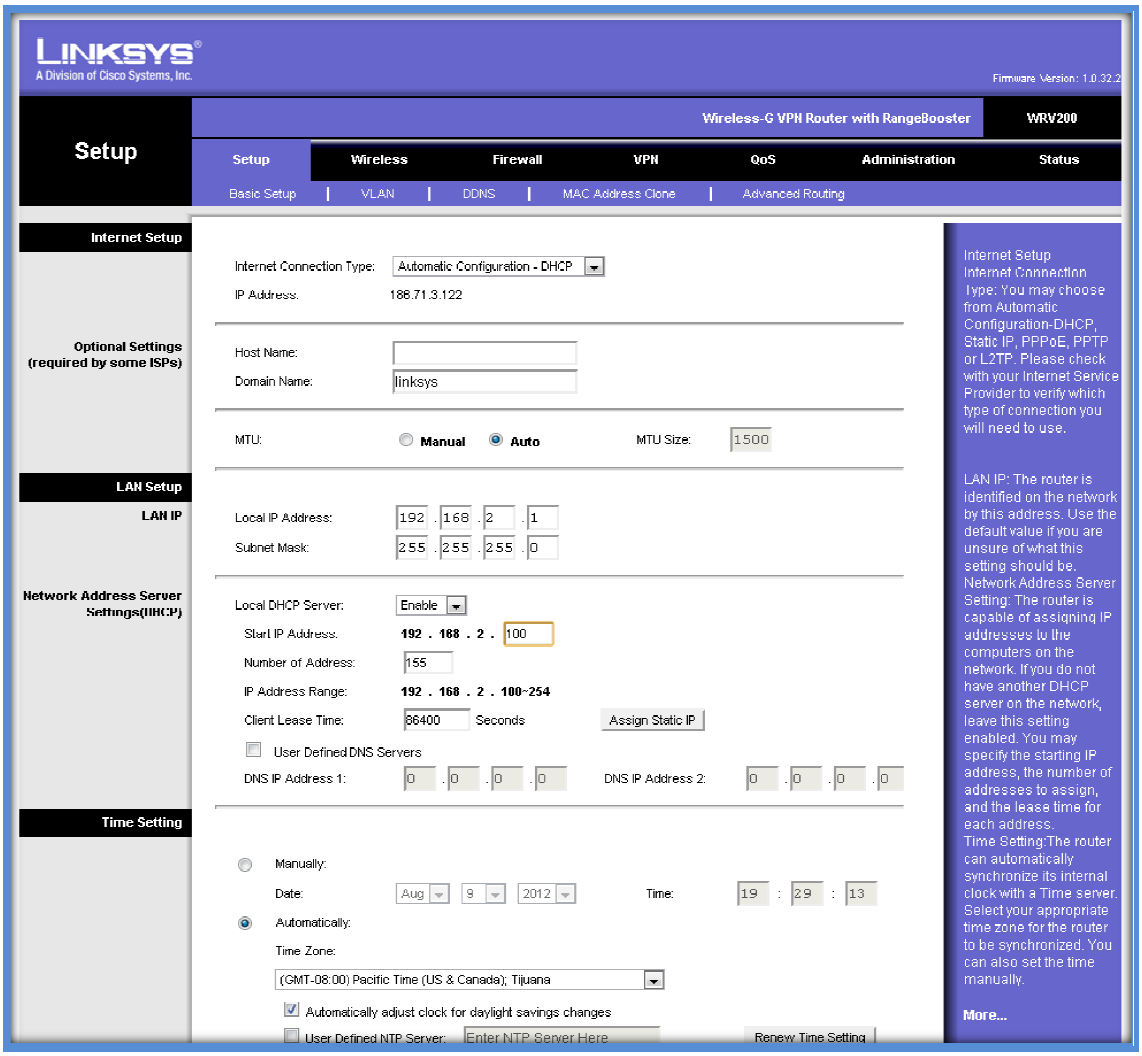


Figura 3.10 Configuración de la IP del Router de Guayaquil

Se verifica la dirección IP de Internet del *router* de Guayaquil, la misma que será el puente de acceso remoto seguro del *router* de Quito. En este caso es 186.71.3.122. (Ver figura 3.11)

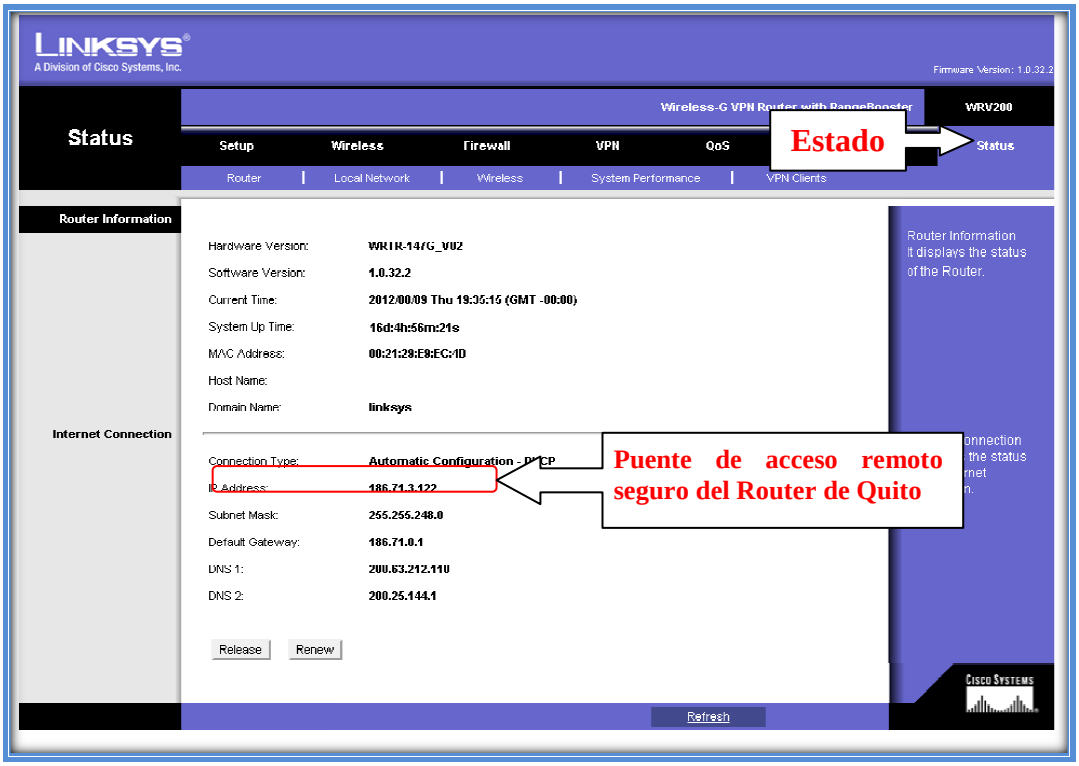


Figura 3.11 Configuración actual del router de Guayaquil

Dentro de la opción Estado, se selecciona Local Network, para verificar la dirección IP local del *router* de Guayaquil en este caso 192.168.2.1, ésta será el Grupo Local Seguro del *Router* de Guayaquil y a la vez será el Puente de Acceso Remoto Seguro del *router* de Quito. (Ver figura 3.12)

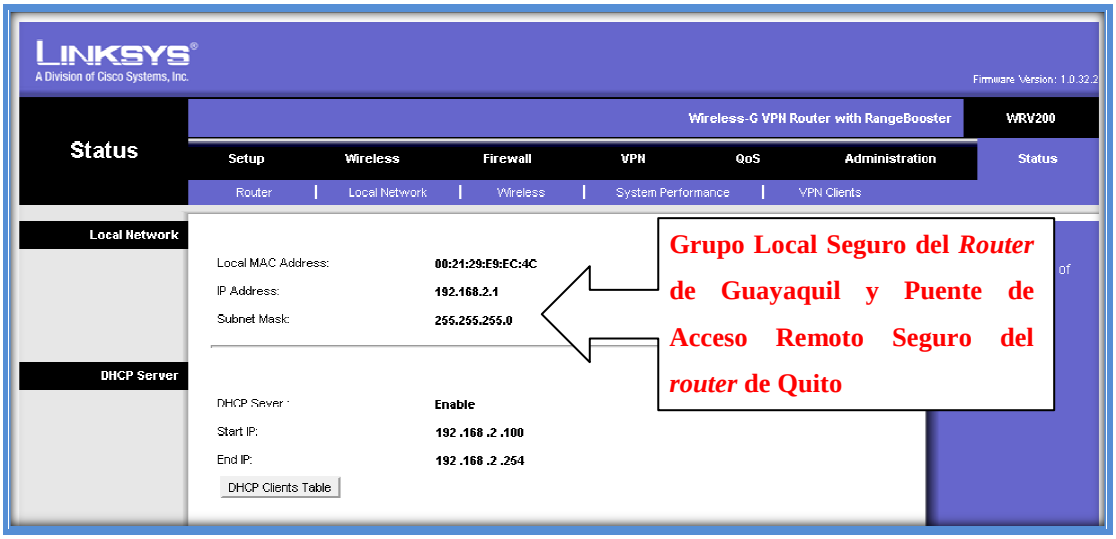


Figura 3.12 Resumen de los datos de configuración actualdel*router* de Guayaquil

Pasos para Configurar el Túnel VPN en el *Router* de Guayaquil

Es necesario crear un túnel y habilitarlo, teniendo bien en claro los datos de la red local desde la que se va a conectar, así como los datos de la red remota a la que se quiere conectar; para ello es indispensable definir el *Gateway*con el que se creará la VPN como se observa en la figura 3.13. A continuación se detallan los pasos para su configuración:

1. Acceder a la **opción VPN** y hacer clic en la opción **IPSEC VPN**.
   En la sección **VPN *Tunnel***
2. Seleccionar la entrada del túnel a utilizar en este caso **Tunnel A**.
3. Seleccionar la opción Enabled para habilitar el túnel.
4. En***Tunnel Name***escribir un nombre para el túnel, en este caso será **Tunel Opt**.
   En la sección ***Local Secure Group***
5. Seleccionar***Subnet***y en IP Address escribir el Rango IP 192.168.2.0 ya que éste es el segmento LAN del *router* local y “255.255.255.0” para la Máscara.
   En la sección ***Remote Secure Group***
6. Seleccionar***Subnet***y en IP Address escribir el Rango IP 192.168.1.0 (estos valores serán del *router*de Quito) y “255.255.255.0” para la Máscara.
   En la sección ***Remote Secure Gateway***
7. Seleccionar ***IP Address***, y luego ingresar la dirección IP de WAN/Internet del *router*de Quito,en este caso es “186.69.37.75”.
   En la sección ***Key Management***
8. En ***Key Exchange Method*** (Método de Intercambio de Clave), seleccionar Auto (IKE).
9. En ***IPSec Encriptation Method***, se dispone de varias técnicas de encriptación: 3DES, AES 192, AES 256, AES 128; en este caso se seleccionarála técnica**AES128** debido la seguridad que presta y realmente en la implementación no representa una demora significativa en su

aplicación. (Debe asegurarse que el nivel de Encripción sea el mismo en ambos*routers* para establecer un túnel VPN).

10. En ***IPSec Authentication Method***los protocolos de autenticación con los que se cuenta son: MD5 y SHA1, se seleccionará MD5 debido a que el sistema que accederá a la base db_impo por medio de la VPN (SICE Profesional) está desarrollado en Visual Basic. (Asegurarse que el método de Autenticación sea el mismo que en el *router*de Quito para establecer el túnel VPN).
11. Asegurarse que **PFS** (Confidencialidad Directa Secreta) esté seleccionada. Esto asegurará que el intercambio inicial de clave y las propuestas IKE sean seguras.
12. En ***Pre-Sharede Key*** (Clave Pre-Compartida), ingresar la clave que se quiere habilitar en el túnel. En este caso se usará “VpnOptimsoft@”.
13. En ***IPSec Key Lifetime***(s) (Clave De Por Vida IPSec), ingresar el período en el que desea que la clave caduque en el túnel. En este caso se usará “3600”. (Asegúrese que las Clave Pre-Compartida y Clave De Por Vida IPSec ingresadas sean las mismas que las del router de Quito)
14. Hacer clic en ***Save Settings***(Guardar Configuraciones).

En la figura 3.13 se observa la habilitación de la VPN en el *router* de Guayaquil, siguiendo los pasos anteriormente explicados.

En la figura 3.14 consta la configuración de protocolos de encriptación y autentificación que se usa para la creación de la VPN.

Se debe considerar que tal como se indica en la figura 3.15 se deben habilitar todos los protocolos de túnel debido a que de esta manera se accede a soluciones VPNs de capa 3 del modelo OSI.

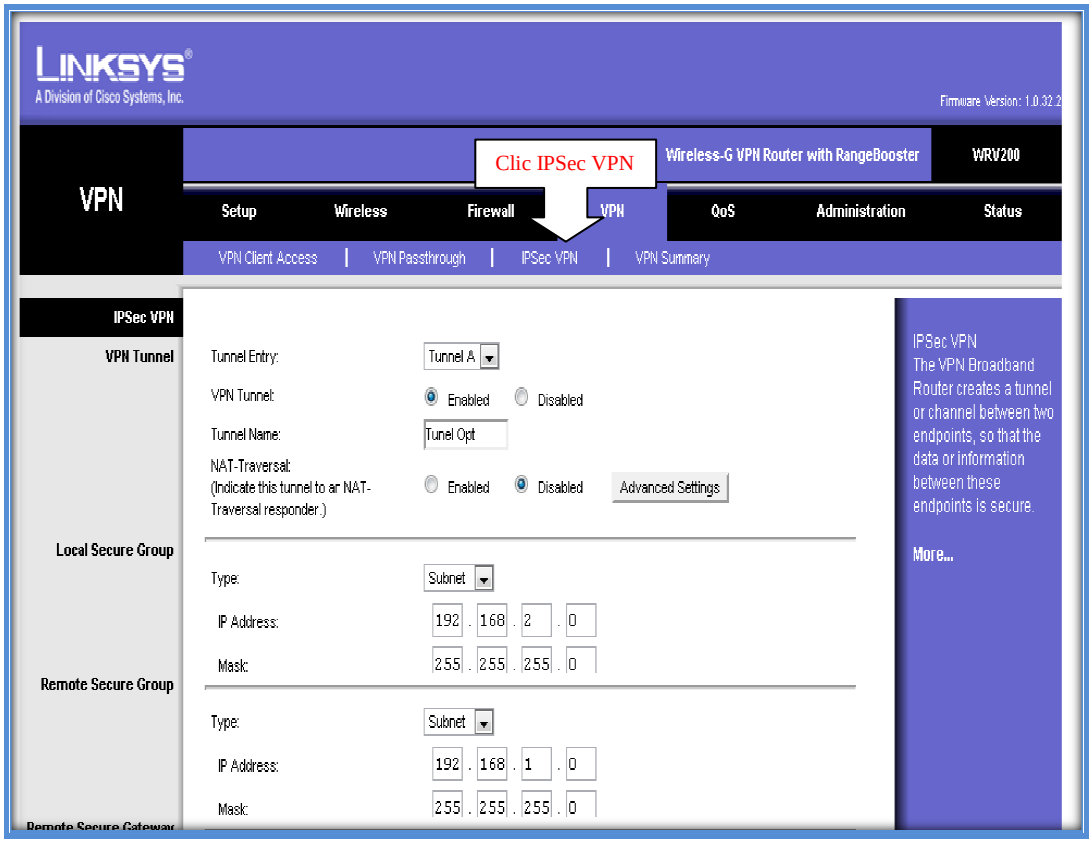


Figura 3.13 Habilitación de la VPN

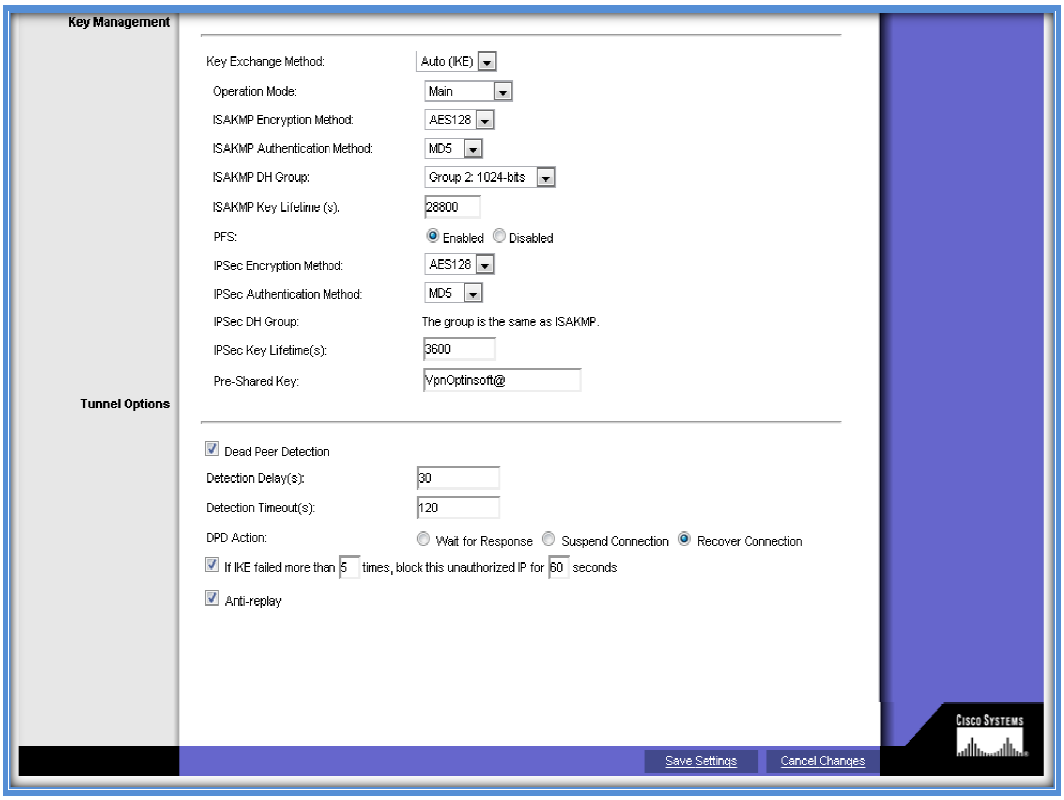


Figura 3.14 Configuración de protocolos de encriptación y autentificación

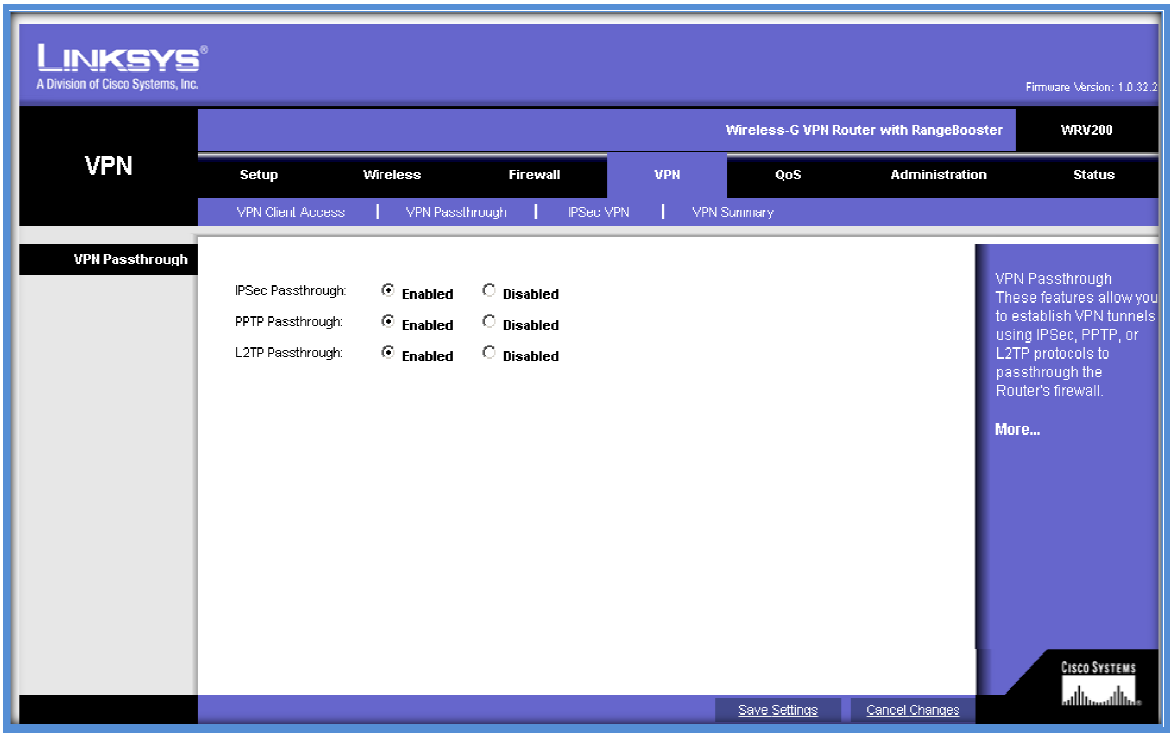


Figura 3.15 Habilitación Protocolos de Túnel

3.4.2 CONFIGURACIÓN DEL *ROUTER* DE QUITO

Es necesario primero configurar la IP local del*router* para no tener conflicto al crear la VPN. Como se muestra en la figura 3.16,la IP del servidor es una IP estática porque se tiene contratado un Plan corporativo de Internet el cual incluye 5 IP's estáticas con la empresa TVCable.

La figura 3.17 muestra en resumen la configuración actual del *router* que está conectado con el Servidor de base de datos ubicado en la ciudad de Quito

Al configurar el *router*de Quito se debe tener mucho cuidado con poner las mismas especificaciones en cuanto a: nombre de la VPN, protocolos deencriptación y autentificación para lograr que la VPN se comunique.

Si un dato varía con respecto al *router* de Guayaquil no se logrará establecer el túnel VPN; para esto se puede ver que las características sean las mismas en ambos*routers* que se van a conectar la VPN.

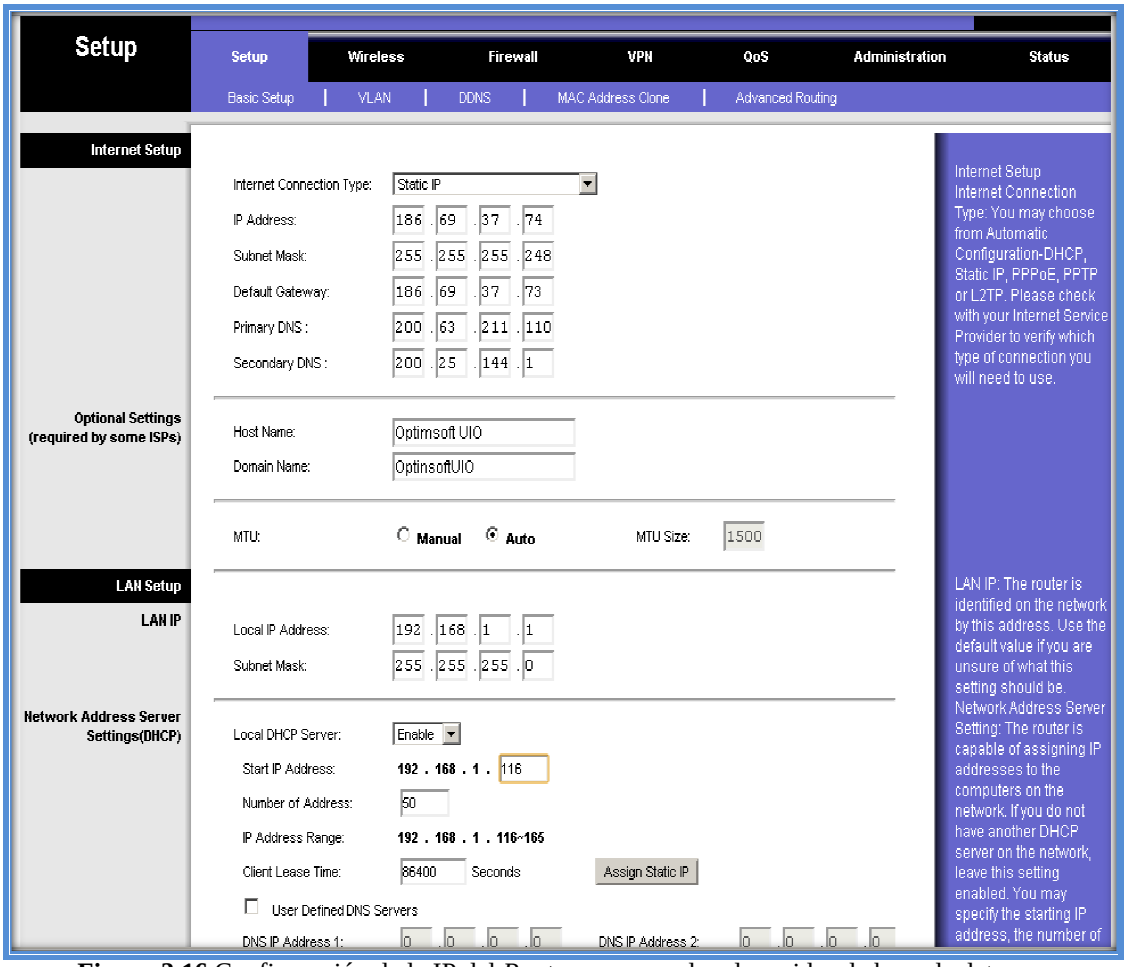


Figura 3.16 Configuración de la IP del *Router* para acceder al servidor de base de datos

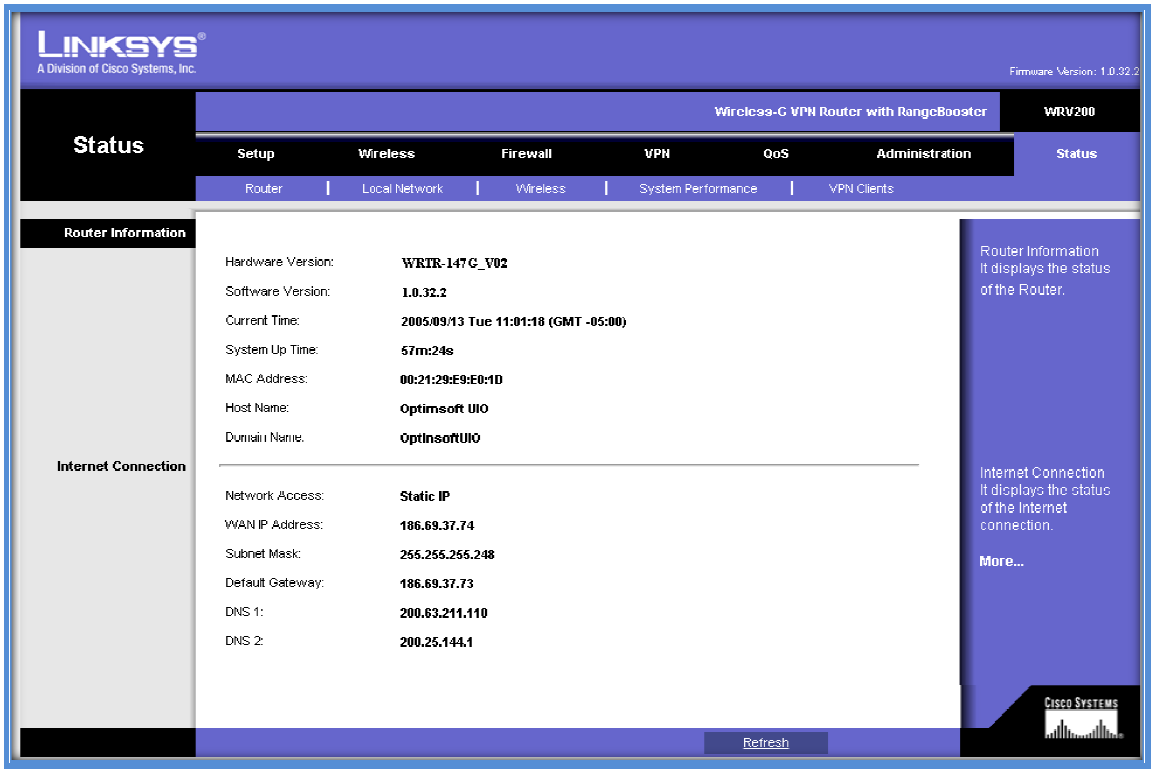


Figura 3.17 Resumen de la configuración del *Router* de Optimsoft en la ciudad de Quito

Pasos para Configurar el Túnel VPN en el *Router* de Quito

1. Acceder a la**opción VPN** y hacer clic en la opción **IPSEC VPN**.
   En la sección **VPN *Tunnel***
2. Seleccionar la entrada del túnel a utilizar en este caso **Tunnel A**.
3. Seleccionar la opción Enabled para habilitar el túnel.
4. En***Tunnel Name*** escribir un nombre para el túnel, en este caso será ***Tunel Opt***.
   En la sección ***Local Secure Group***
5. Seleccionar***Subnet***y en IP Address escribir el Rango IP 192.168.1.0 ya que éste es el segmento LAN del *router* local y “255.255.255.0” para la Máscara.
   En la sección ***Remote Secure Group***
6. Seleccionar***Subnet***y en IP Address escribir el Rango IP 192.168.2.0 (estos valores serán del *router*de Quito) y “255.255.255.0” para la Máscara.
   En la sección ***Remote Secure Gateway***
7. Seleccionar ***IP Address***, y luego ingresar la dirección IP de WAN/Internet del *router* de Quito, en este caso es “186.71.3.122”.
   En la sección ***Key Management***
8. En ***Key Exchange Method*** (Método de Intercambio de Clave), seleccionar Auto (IKE).
9. En ***IPSec Encriptation Method***, se dispone de varias técnicas de encriptación: 3DES, AES 192, AES 256, AES 128; en este caso se seleccionarála técnica**AES 128** debido la seguridad que presta y realmente en la implementación no representa una demora significativa en su aplicación. (Debe asegurarse que el nivel de Encripción sea el mismo en ambos*routers* para establecer un túnel VPN).
10. En **IPSec Authentication Method** los protocolos de autenticación con los que se cuenta son: MD5 y SHA1, se seleccionará **MD5** debido a que el sistema que accederá a la base db_impo por medio de la VPN (SICE Profesional) está desarrollado en Visual Basic. (Asegurarse que el método

de Autenticación sea el mismo que en el *router*de Quito para establecer el túnel VPN).

11. Asegurarse que **PFS** (Confidencialidad Directa Secreta) esté seleccionada. Esto asegurará que el intercambio inicial de clave y las propuestas IKE sean seguras.
12. En ***Pre-Sharede Key*** (Clave Pre-Compartida), ingresar la clave que se quiere habilitar en el túnel. En este caso se usará “VpnOptimsoft@”.
13. En ***IPSec Key Lifetime****(s)* (Clave De Por Vida IPSec), ingresar el período en el que desea que la clave caduque en el túnel. En este caso se usará “3600”. (Asegúrese que las Clave Pre-Compartida y Clave De Por Vida IPSec ingresadas sean las mismas que las del router de Quito)
14. Hacer clic en ***Save Settings*** (Guardar Configuraciones)

Una vez configurados ambos *routers* hay que ubicarse en la sección VPN *Summary* para verificar el estado del túnel VPN. En la figura 3.19 se puede verificar que todavía se está intentado conectar al *router* de UIO con el *router* remoto de GYE.

Para poder conectar la VPN luego de configurar los parámetros se debe reiniciar el túnel por el cual se desea establecer la comunicación. Una vez reiniciado el túnel se puede comprobar en la figura 3.20 que ya se encuentra conectado el túnel VPN entre Quito y Guayaquil.

En la Figura 3.22 se observa información avanzada y las características de la conexión del túnel VPN entre Quito y Guayaquil.

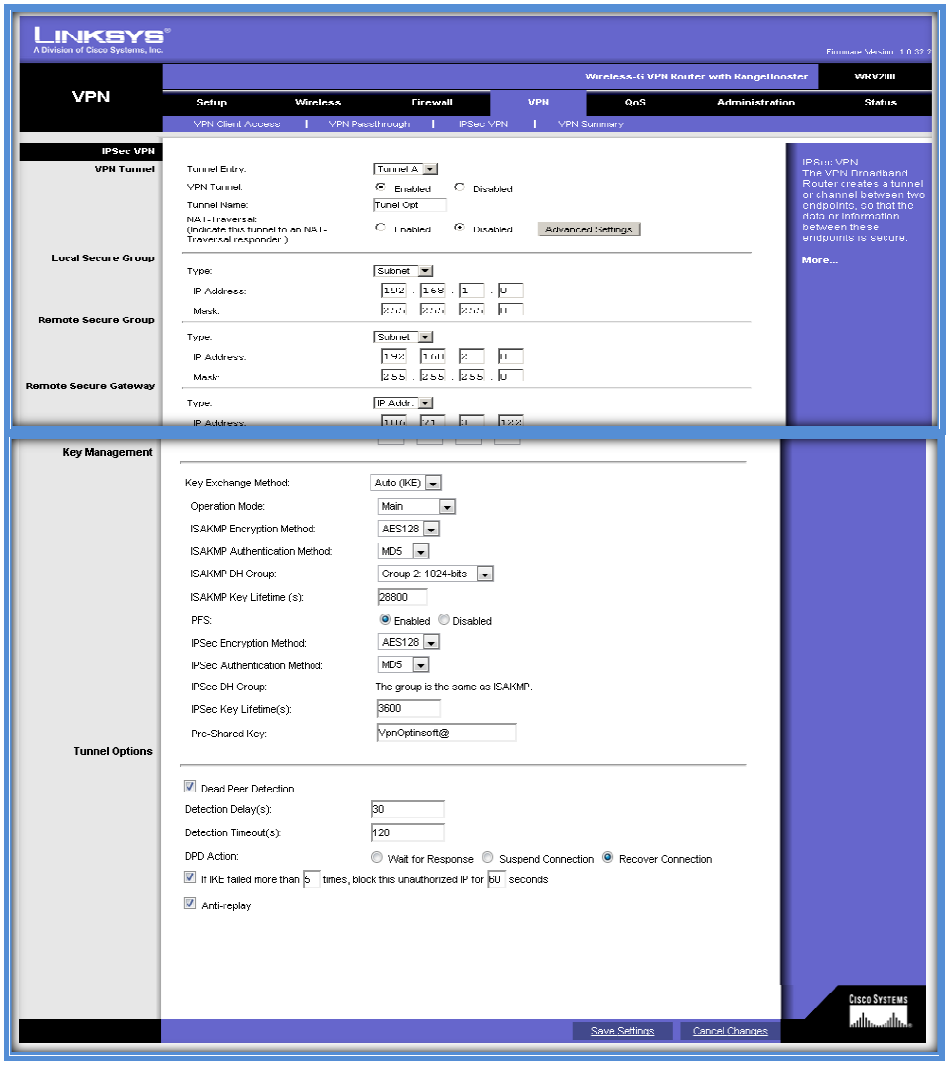


Figura 3.18 Configuración de la VPN para el *Router* de Quito

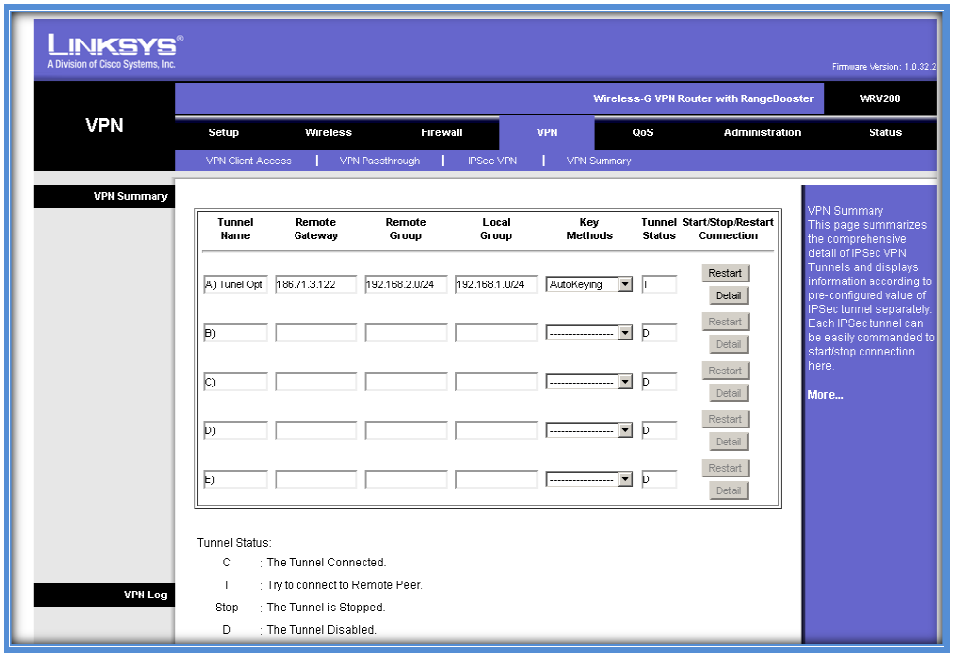


Figura 3.19 Estado del Túnel de la VPN creada visto desde UIO

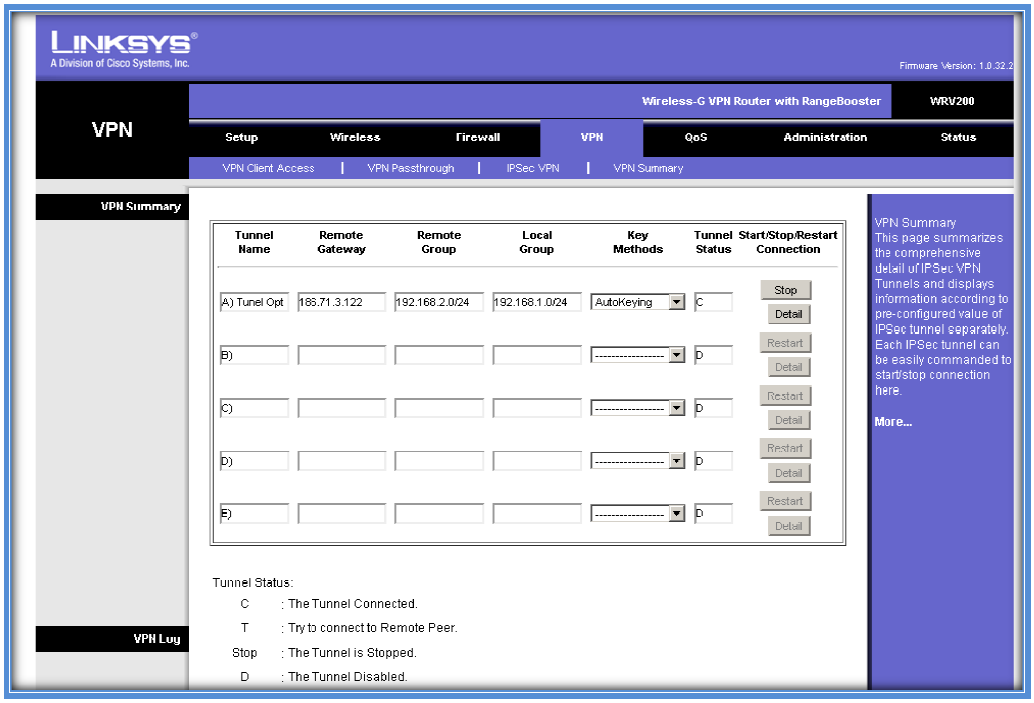


Figura 3.20 Túnel Conectado de la VPN (UIO-GYE) (Tunel Opt)

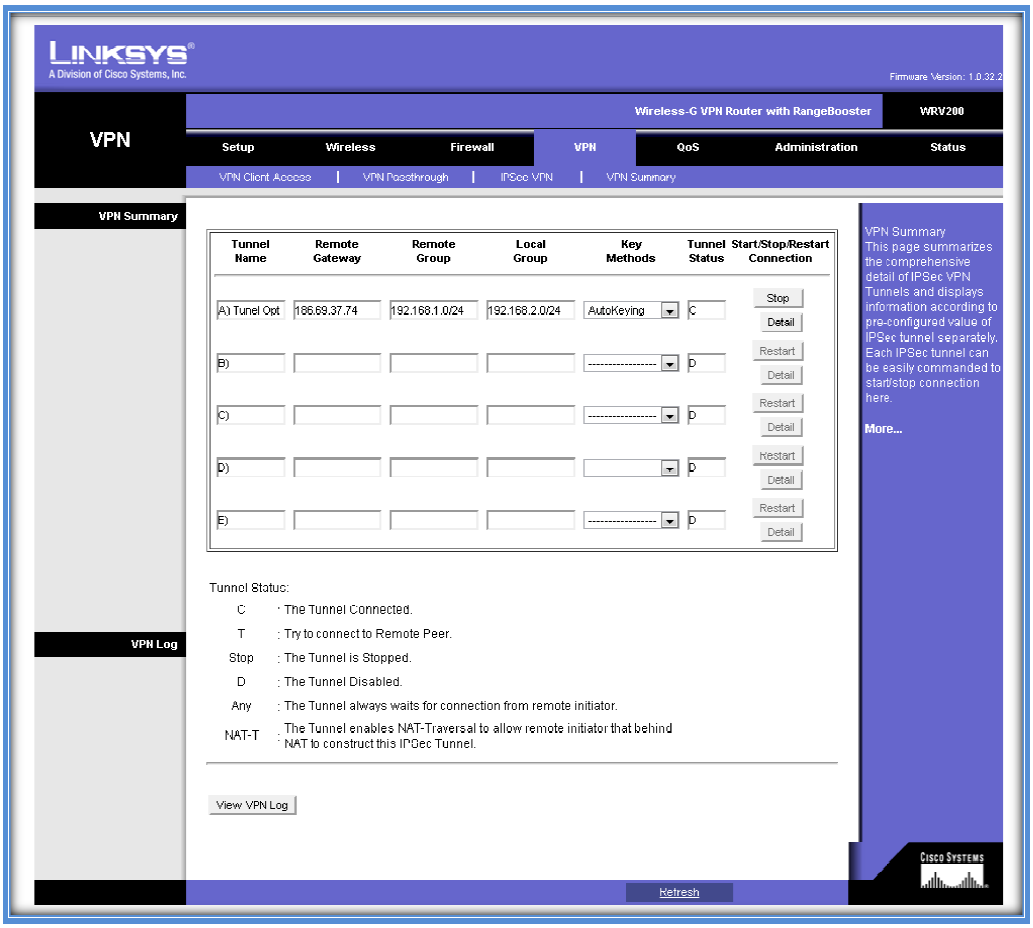


Figura 3.21Túnel Conectado de la VPN (GYE- UIO) (Tunel Opt)

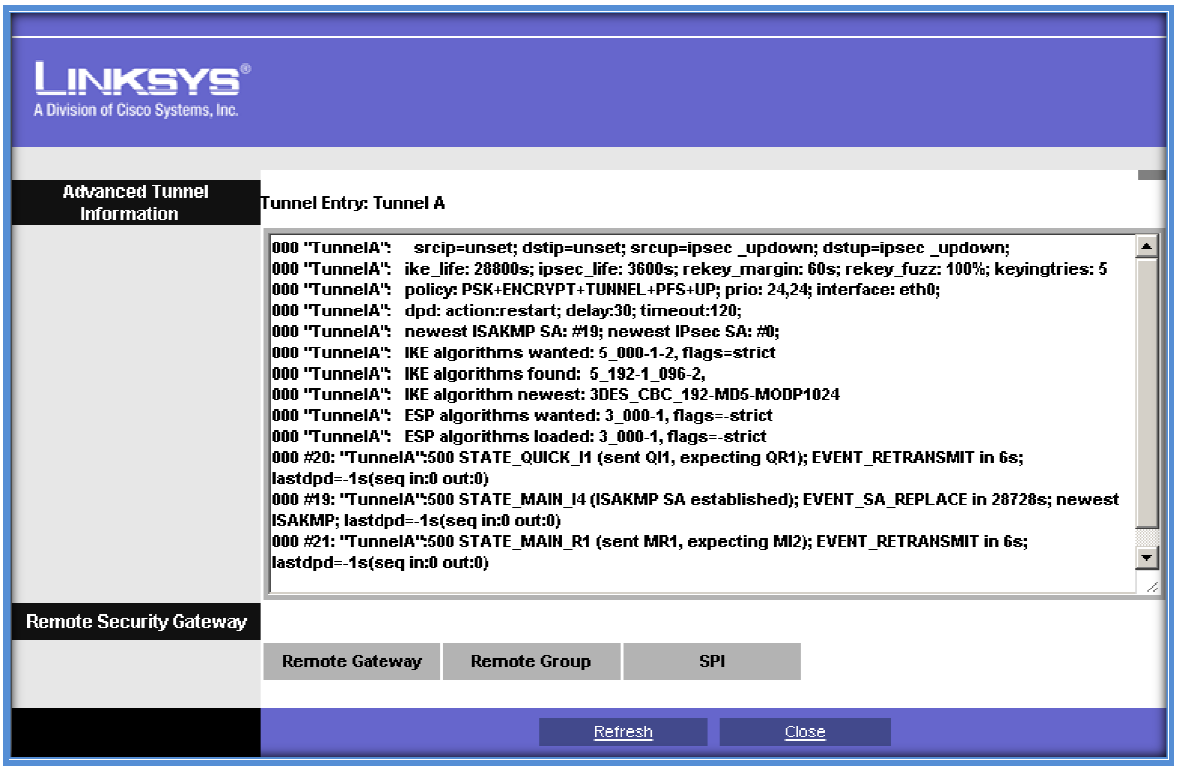


Figura 3.22 Información Avanzada de la conexión del Túnel Quito Guayaquil

3.4.3 PRUEBAS DE LA VPN

Al establecer la VPN entre Quito y Guayaquil, el cliente de Guayaquil es un miembro másde la red de Quito y puede acceder a: directorios compartidos,servidor, correo electrónico, impresoras de red, etc.

Con el fin de verificar el enlace del túnel VPN se ejecuta el comando PING desde el usuario remoto en Guayaquil hacia un usuario remoto seguro en Quito que corresponde al servidor de base de datos. Como se puede observar en la figura 3.23 se tiene levantada la VPN y el tiempo de respuesta es considerablemente bajo.

Otra prueba de conexión de la VPN, se la puede realizar accediendo desde un computador de Guayaquil (red local) a los recursos compartidos del servidor de Quito (red remota) escribiendo en *Ejecutar*el IP del computador de la red remota 192.168.1.131 como se ve en las figuras 3.24a y 3.24b.

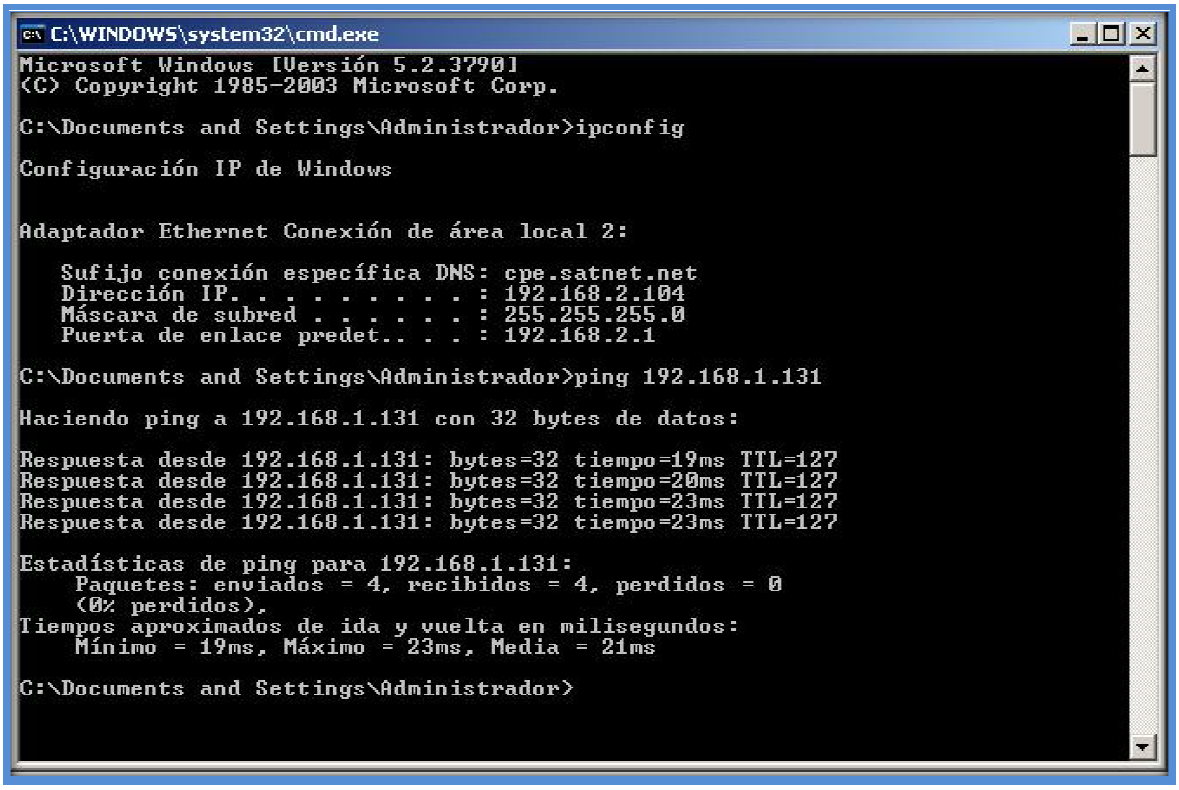


Figura 3.23 Ping a un usuario del Grupo remoto Seguro de la VPN

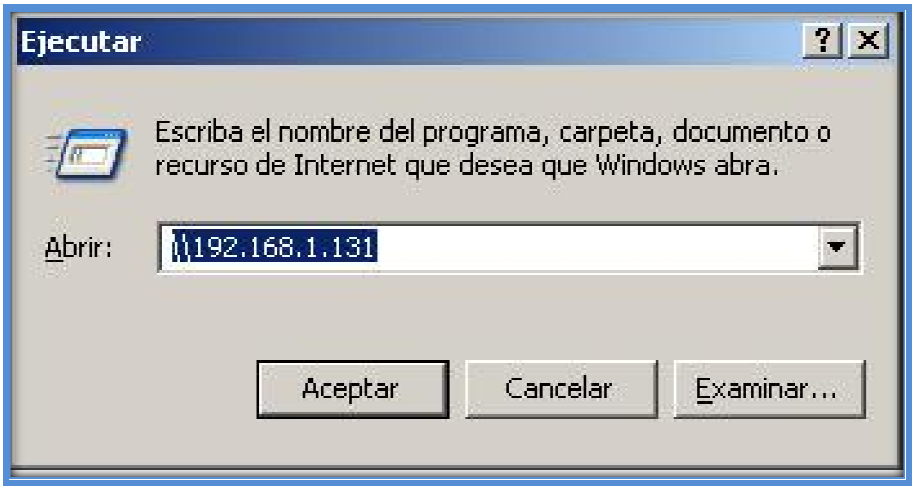


Figura 3.24a Prueba de Acceso a recursos compartidos a través del IP del computador de la red remota

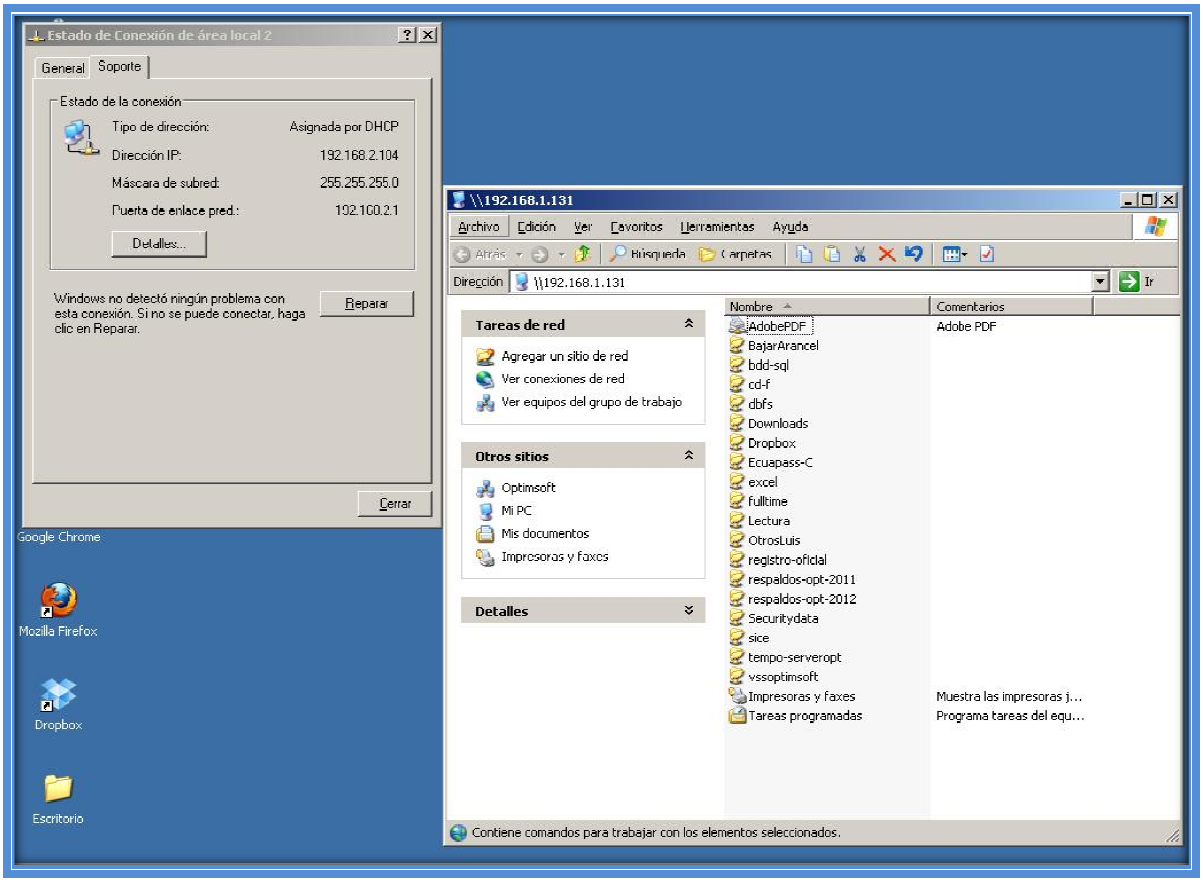


Figura 3.24b Prueba de Acceso a recursos compartidos a través del IP del computador de la red remota

Se puede comprobar que es un acceso remoto desde Guayaquil observando en la figura 3.25 que la IP 192.168.2.104 pertenece al grupo local seguro 192.168.2.0 de la Red Optimsoft Guayaquil y la IP 192.168.1.131con la que se accede a la base de datos db_impo utilizando la aplicación SICE Profesional, pertenece al grupo remoto seguro 192.168.1.0 de la Red Optimsoft Quito.

Se puede ver en la figura 3.26 el acceso a la base de datos db_impo en Quito desde un usuario remoto seguroen la ciudad de Guayaquil.

Al acceder a la base de datos centralizada por medio del sistema SICE Profesional desde un usuario remoto se puede ingresar a los siguientes módulos:

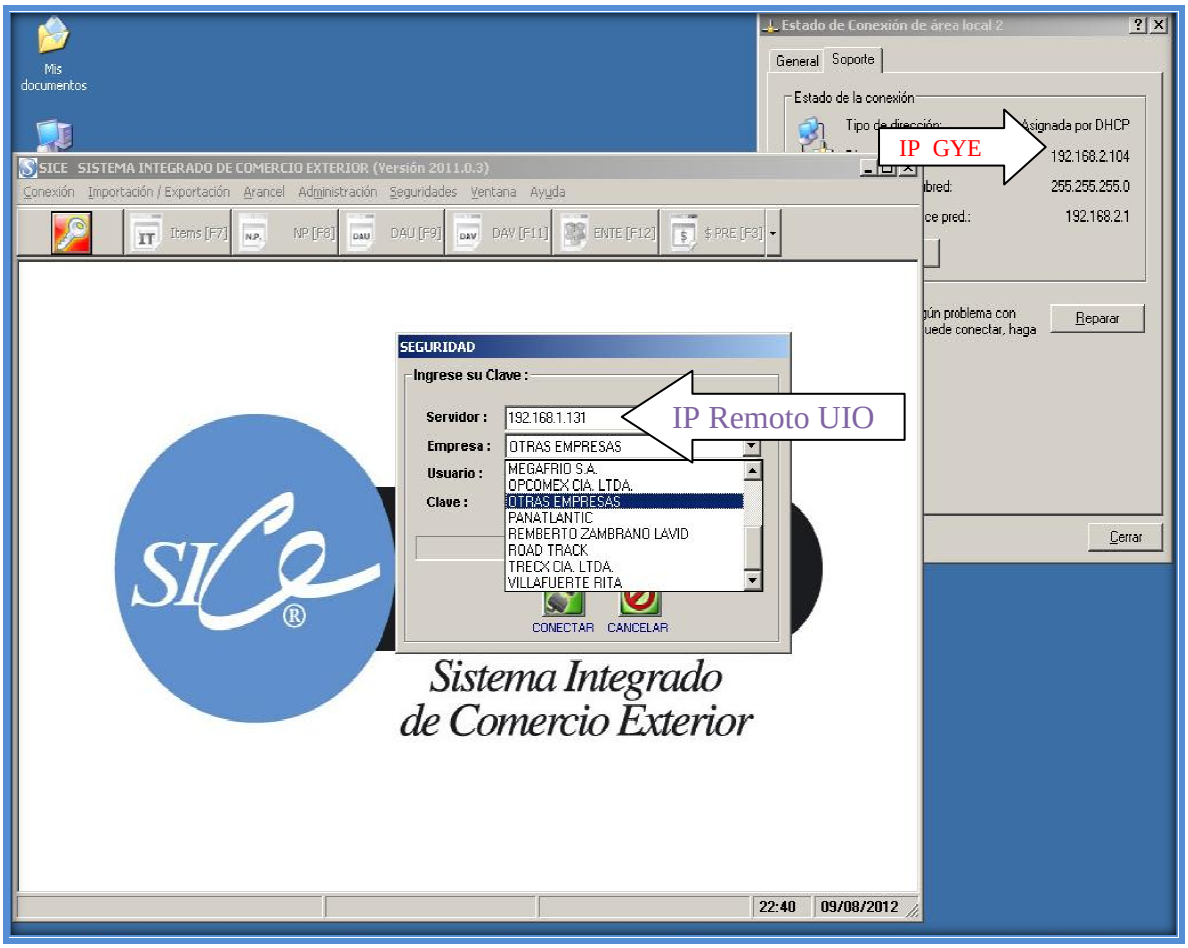


Figura 3.25 Verificación Acceso remoto desde la aplicación GYE a db_impo UIO

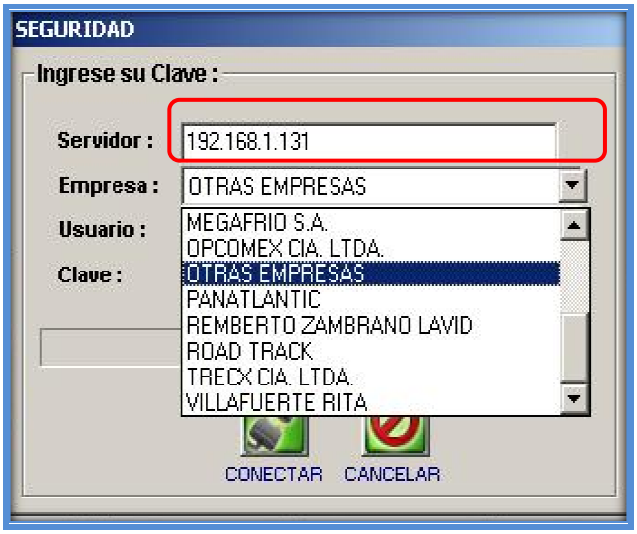


Figura 3.26 Acceso al sistema SICE Profesional

DAU, DAV, Ítems, NP[47], ENTE[48], PRE[49], lo cual anteriormente se los realizaba por medio del envío de correo electrónico para cada DAU que se necesitaba realizar.

En la Figura 3.27 se observa la pantallacon información del DAU desdeun cliente remoto seguro en Guayaquil. Cabe señalar que si se necesita acceder a la base db_impo desdeotro usuario del grupo remoto seguro, simplemente se debe conectar dicho usuario a la red de Guayaquil para que acceda mediante el *router* que tiene configurado el Túnel VPN.

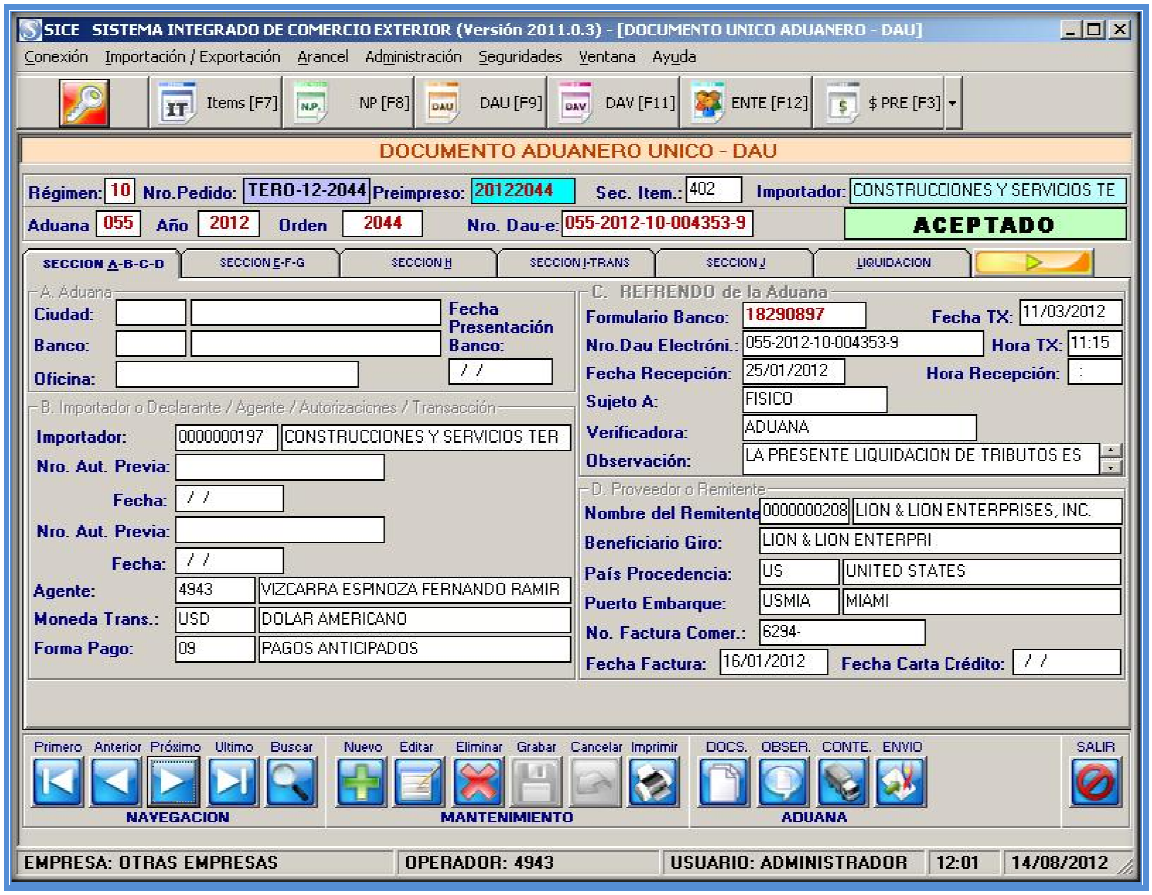


Figura 3.27 Accesoal SICE Profesional desde un usuario remoto seguro en Guayaquil

[47]NP.- Nota de Pedido

[48]ENTE.- Entidades que intervienen en el trámite

[49]PRE.- Pre liquidación de tributos

Otra forma de comprobar que la VPN entre la ciudad de Quito y Guayaquil está funcionando es utilizando el programa VPN Link Test, como se observa en la figura 3.28

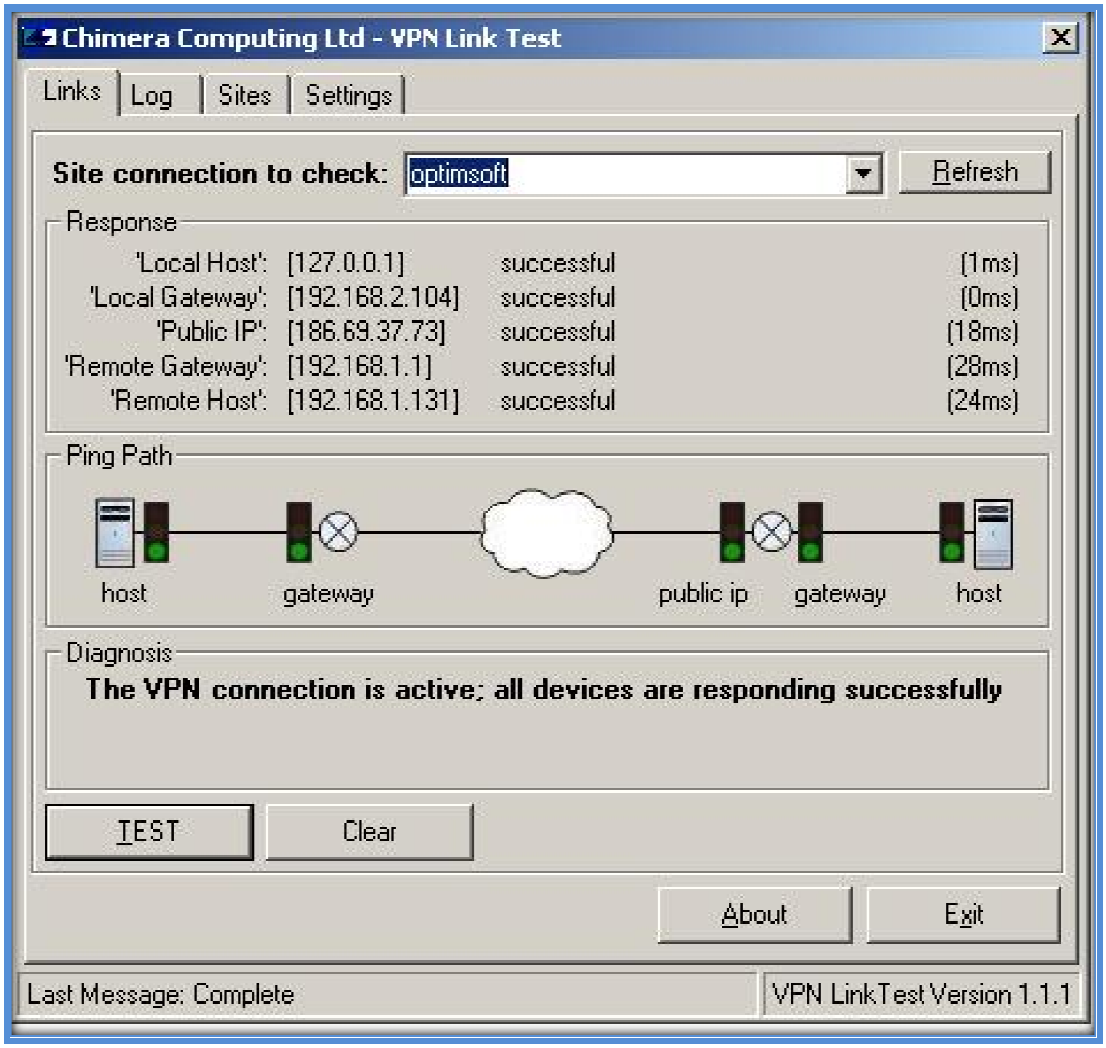


Figura 3.28 Prueba de Conexión de la VPNcon programa VPN Link Test

Mediante la opción VPN Summary que está dentro del menú VPN en la configuración del*router*, se puede comprobar que la VPN está funcionando correctamente ya que se puede apreciar que el estatus del Túnel indica como conectado (ver figura 3.29)

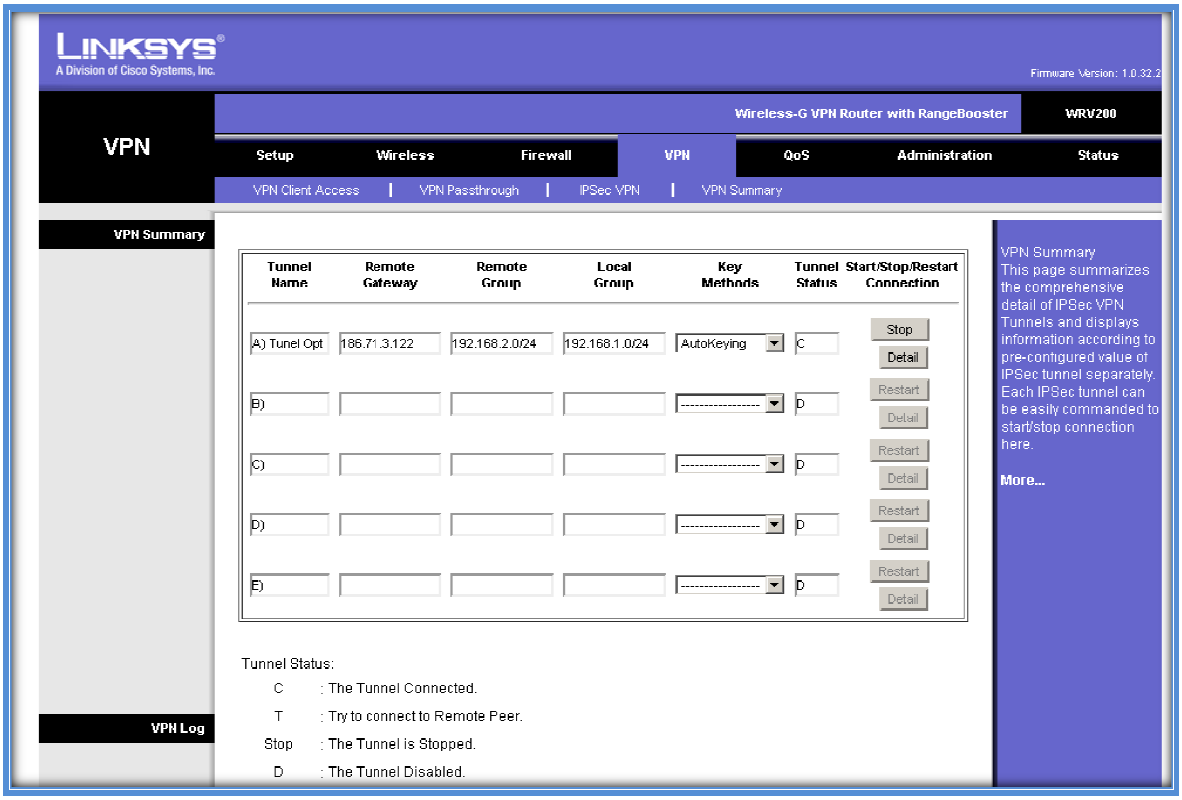


Figura 3.29 Prueba de Conexión de la VPN

CAPÍTULO 4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Uno de los problemas comunes de las empresas que trabajan con la Aduana Ecuatoriana es la necesidad de tener centralizada la información de las sucursales en la oficina matriz, debido a que toda la documentación debe tenerla el agente de aduana.Actualmente se deben enviar los cambios mediante un correo al agente y luego a la Aduana. Siendo ésta la manera tradicional que utiliza la mayoría, es una forma que involucra pérdida de tiempo en envíos y que expone a ser atacada la información (no existe información en tiempo real).

- Las VPNs son una alternativa económica, con ellas las empresas se mantienen interconectadas con seguridad, utilizando un medio público de bajo costo como el Internet.

- Las VPNs mediante *firewall*, a pesar de ser seguras, su principal inconveniente es que a todos los clientes de la VPN los envía primero a cuarentena, volviéndola un poco más lenta por su comprobación, lo cual dependiendo del sistema operativo que se posea puede crear conflicto.

- En el presente trabajo se ha cumplido con el objetivo de proveer a la empresa Optimsof de una VPN, con la cual se elimina el envío de correos electrónicos para mantener la base de datos db_impo actualizada e interconectada.

- Como resultado del análisis de mejor alternativa de VPNs se ha determinado que el diseño mediante hardware es la mejor opción no solo desde el punto de vista económico, sino porque además permite tener

seguridad en la transmisión de datos sin necesidad de cambiar la estructura que posee.

- En el momento de implementar la VPN, es muy importante no tener errores tanto en las direcciones locales como remotas, ya que de haberlos en el momento de configurar los *routers* no se logrará la creación de la VPN.

- Es necesario mantener los mismos protocolos tanto en el *router* local como en el remoto parar crear la VPN.

- Actualmente la empresa posee más sucursales con las cuales se podría crear VPN`s con el fin de mantenerse interconectadas y actualizar la base de datos db_impo sin inconvenientes.

- La empresa puede comercializar la creación de VPN´s para sus clientes de SICE Profesional, dándoles un valor agregado al facilitar a sus clientes que poseen múltiples oficinas a nivel nacional una interconexión e interacción segura con su base de datos.

- El costo invertido en los equipos para proveer la VPN tiene un valor realmente insignificante frente a las ventajas, que ésta brinda.

- La VPN implementada produce una disminución de tiempo en cada trámite debido a que ya no se necesita esperar que la persona que está en Quito reciba un correo y lo conteste, simplemente se pueden conectar directamente y actualizar la base de datos.

- Debido a que en la actualidad hay muchos ataques informáticos es necesario tener seguridad para transmitir la información, y con la VPN es posible mantener un canal privado sin ataques.

- Todo trámite que debe ser enviado a la Aduana del Ecuador posee documentos anexos; con la creación de la VPN se elimina los envíos y duplicidad de dichos documentos tanto en Quit como en Guayaquil.

4.2 RECOMENDACIONES

- En el futuro se debe incrementar el ancho de banda a 2 Mbps para poder cumplir con lo solicitado por la Aduana del Ecuador y ayudar a que cada aplicación tenga una mayor capacidad debido a que con el tiempo todas las redes tienden a crecer y aumentar el número de usuarios.

- Incluir en la empresa Optimsoft la creación y comercialización de VPN como un servicio adicional del sistema SICEProfesional, así los usuarios podrán acceder a sus bases de datos sin necesidad de envío de datos vía correo electrónico desde otras ciudades, añadiendo de esta manera seguridad a la transmisión de datos, lacentralización de la información en tiempo real.

- Capacitar al personal para poder utilizar la base de datos db_impo, para mantenerla siempre actualizada y disponible en caso de una revisión por parte de la Aduana Ecuatoriana.

- Aprovechar las características propias de la VPN, como el compartir documentos, con el fin de acceder a la información cuando se requiera sin necesidad que existan tiempos de espera y dependencia de otra persona. O a su vez se podría implementar una VPN para acceder a la base de datos que corresponde al SICE Proscan, evitando así duplicidad de información, ahorro de tiempo y agilidad.

- Actualmente la Aduana del Ecuador exige que todo trámite esté firmado con el token(firma electrónica); la empresa podrá utilizar la VPN creada para firmar los documentos de otras ciudades de forma segura.

- Se debe a futuro administrar el nivel de acceso de los usuarios a la red conforme ésta vaya creciendo, debido a que en el servidor se encuentra la información de clientes de la empresa y muchos datos importantes que podrían ser alterados por personal mal intencionado.

- Ser cuidadoso en contratar un proveedor de Internet, ya que lacalidad del servicio es fundamental en el rendimiento de lasRedes Privadas Virtuales, se deberá tomar en cuenta la tecnología deconexión, la disponibilidad del servicio, nivel de compartición y soportetécnico todos los días del año.

REFERENCIAS BIBLIOGRÁFICAS

CAPÍTULO 1

[1] Blog de redes de información, disponible en línea: Noviembre 2012 http://emsambleyredes.blogspot.com/p/comunicacion-atravez-de-la-red.html

[2] Ibañez Meca Antonio, *Support Specialist* , disponible en línea: Noviembre 2012 http://download.microsoft.com/download/f/3/0/f305b708-87b5-4780-bd2a-f2c7b8039353/VPN.ppt

[3] Soporte Linksys, disponible en línea: Noviembre 2012 http://linksys-de.custhelp.com

[4] Ect Telecom, disponible en línea: Noviembre 2012 www.ecttelecom.com/services/data-internet/mpls-vpn/

[5] Espiñeira Sheldon y Asociados, (2003), VPN o Redes Privadas Virtuales (Parte I)

[6] Enciclopedia en línea Wikipedia 2012, disponible en línea: Noviembre 2012 www.wikipedia.com

[7] Ing. Gómez Valdivia Javier Rafael, Revista Telem@tica 2004

[8] Microsoft, Curso Redes Privadas Virtuales ,2001

[9] Nader Carrión Roberto, monografias.com, disponible en línea: Noviembre 2012 http://www.monografias.com/trabajos11/repri/repri.shtml

[10] Cline communications, disponible en línea: Noviembre 2012 http://clinecommunications.net/?ID=37

[11] VPN - Tunneling, disponible en línea: Noviembre 2012 http://techtipsbysatish.blogspot.com/2010/09/vpn-tunneling.html

[12] VPN - Tunneling, disponible en línea: Noviembre 2012 http://techtipsbysatish.blogspot.com/2010/09/vpn-tunneling.html

[13] Ing. Gómez Valdivia Javier Rafael, Revista Telem@tica 2004

[14] Instituto de Ingeniería Eléctrica, Universidad de La República

[15] Instituto de Ingeniería Eléctrica, Universidad de La República

[16] Instituto de Ingeniería Eléctrica, Universidad de La República

[17] Valera Pintor Francisco,Redes y Servicios Internet de nueva Generación Curso 2004-2005
http://www.it.uc3m.es/dlarra/rsing/traspas/3-%20trabajos_fvalera.pdf

[18] Ibañez Meca Antonio, *Support Specialist* , disponible en línea: Noviembre 2012
http://download.microsoft.com/download/f/3/0/f305b708-87b5-4780-bd2a-f2c7b8039353/VPN.ppt

[19] CANO SEPULVEDA SERGIO ALEXIS, Administración de Redes de Computadoras , disponible en línea: Noviembre 2012
www.scribd.com/doc/11562560/Criptografia

[20] Daccach José Camilo, 2007, disponible en línea: Noviembre 2012
http://www.gestiopolis.com/delta/term/TER289.html

[21] Diccionario de Informática, disponible en línea: Noviembre 2012
http://www.alegsa.com.ar/Dic/encriptacion.php

[22] Concepto basado en:FIPS PUB 198-1, *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION*

[23] Network Land, disponible en línea: Noviembre 2012
http://network-land.awardspace.com/vpn/requerimientos.php

CAPÍTULO 2

[1] Manual Windows Server 2003

[2] Microsoft Tech Net, Guía detallada de creación de una conexión de red privada virtual de sitio a sitio.

[3] LogMeIn, disponible en línea: Noviembre 2012
https://secure.logmein.com/

[4] LogMeIn, disponible en línea: Noviembre 2012
https://secure.logmein.com/

[5] LogMeIn, disponible en línea: Noviembre 2012

https://secure.logmein.com/

[6] cisco, disponible en línea: Noviembre 2012
www.cisco.com

[7] Red Infinita, disponible en línea: Noviembre 2012
http://www.redinfinita.com/gateway.html

[8] Microsoft TechNet, disponible en línea: Noviembre 2012
http://technet.microsoft.com

CAPÍTULO 3

[1] Información entregada por la Empresa OPTIMSOFT Cia. Ltda.

[2] Información entregada por la Empresa OPTIMSOFT Cia. Ltda.

[3] Google, 2011, disponible en línea: Noviembre 2012
http://www.google.com/apps/intl/es/index.html

[4] Valores proporcionados por el Departamento de Sistemas de la Empresa Optimsoft

[5] Valores proporcionados por el Departamento de Sistemas de la Empresa Optimsoft

[6] Valores proporcionados por el Departamento de Sistemas de la Empresa Optimsoft

[7] Valores proporcionados por el Departamento de Sistemas de la Empresa Optimsoft

[8] LogmeIn, disponible en línea: Noviembre 2012
www.logmein.com

[9] Valores proporcionados por el Departamento de Sistemas de la Empresa Optimsoft

[10] Valores proporcionados por el Departamento de Sistemas de la Empresa Optimsoft

[11] Manual *Router* Linksys WRV200

ANEXOS

ANEXO A

Tabla comparativa de la versiones LogMeIn Hamachi: Premium y Básica

	Básica	Premium	
Precio			
Mensual	Gratis	$4.95	
Anual	Gratis	$39.95	
Límites de red			
Redes	64	256	El número de redes que puede crear un usuario.
Unión	64	256	El número de redes a las que puede unirse un usuario y que dependen de la capacidad.
Capacidad	16	256	Una red puede tener hasta 16 clientes con la versión gratuita y hasta 256 clientes con la premium.
Chat			
Entre iguales - En línea	Sí	Sí	Intercambio de mensajes instantáneos con interlocutores de Hamachi en línea.
Entre iguales - Fuera de línea	-	Sí	Intercambio de mensajes instantáneos con clientes de Hamachi fuera de línea.
Chat en grupo – Ver	Sí	Sí	La mensajería de red, más conocida como "chat en grupo" es una opción que permite chatear a la vez y en una misma ventana con todos los miembros de la red que estén
Chat en grupo – Enviar	-	Sí	

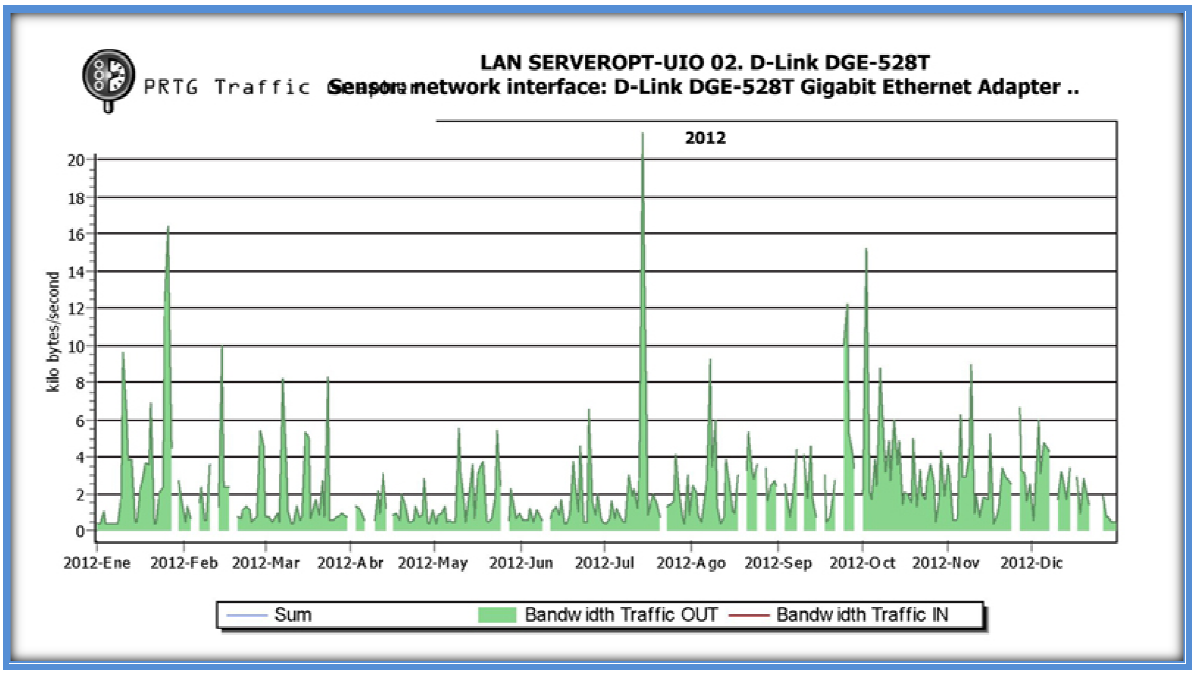
			conectados.
Protección de red			
Protección de contraseña	Sí	Sí	A cualquiera que intente unirse a la red, se le pedirá que presente una contraseña de red válida.
Bloqueo de red	-	Sí	La red puede bloquearse para evitar que los miembros nuevos se unan a ella. De esta forma, se conserva el resto de ajustes de control de acceso.
Aprobación de miembros	-	Sí	Ningún miembro nuevo tendrá acceso total a la red hasta que haya sido aprobado manualmente por el propietario o por el administrador.
Redes sin contraseña	-	Sí	
Administración de red			
Expulsión de miembros	Sí	Sí	Los propietarios y los administradores pueden expulsar a los miembros de la red. Si esto ocurre, las personas expulsadas perderán su condición de miembros, pero podrán unirse a la red en cualquier momento.
Prohibición de miembros	-	Sí	Los administradores o propietarios de la red pueden elaborar una lista de los clientes Hamachi que no podrán unirse a ella bajo ninguna condición.
Crear administradores	-	Sí	Los propietarios de la red pueden nombrar administradores de red a uno o a varios miembros de la misma red y asignarles derechos.

Mensajes de red	-	Sí	Los propietarios y los administradores de la red pueden establecer mensajes de bienvenida y de anuncios para cada red.
Conectividad ampliada			
Retransmisiones de ancho de banda bajo	Sí	Sí	Las retransmisiones sirven para conectar a los clientes de Hamachi que no pueden establecer un canal de comunicación directo por alguna razón. Las probabilidades estadísticas de necesitar una retransmisión cuando se utiliza Hamachi es del 5 % aproximadamente.
Retransmisiones de ancho de banda alto	-	Sí	
Funciones avanzadas			
Tunelización enrutada	Sí	Sí	Además de dirigir el tráfico entre sus clientes, Hamachi puede configurarse para permitirle acceder de forma remota a los ordenadores LAN que no puedan ejecutar el cliente de Hamachi.
Proxy web integrado	-	Sí	Sus interlocutores de Hamachi pueden configurar sus navegadores web para acceder a Internet a través del ordenador que tenga usted y proteger así su tráfico web. Esta función suele utilizarse para proteger la navegación web de locales poco fiables, como cibercafés, cafés, hoteles, etc.

Ejecutar como servicio del sistema de Windows	-	Sí	Una opción para ejecutar el cliente Hamachi como un servicio del sistema. Normalmente se necesita cuando se ejecuta Hamachi en servidores o en instalaciones que requieren la autenticación de dominio de Windows.

ANEXO B

Monitoreo con el programa PRTG *Traffic Grapher*



	net total per sec
Fecha	kilo bytes/second
31/12/2012	0.446
30/12/2012	0.459
29/12/2012	0.464
28/12/2012	0.79
27/12/2012	0.709
26/12/2012	1.858
21/12/2012	1.436
20/12/2012	2.358
19/12/2012	2.816
18/12/2012	0.975
17/12/2012	2.904
14/12/2012	3.329
13/12/2012	1.685
12/12/2012	2.794
11/12/2012	3.176
10/12/2012	1.645
07/12/2012	4.258
05/12/2012	4.71
04/12/2012	3.059
03/12/2012	5.926
01/12/2012	0.529
TOTAL	46.33

	net total per sec
Fecha	kilo bytes/second
30/11/2012	2.51
29/11/2012	1.548
28/11/2012	3.062
27/11/2012	3.28
26/11/2012	6.58
23/11/2012	2.557
22/11/2012	2.782
21/11/2012	2.864
20/11/2012	3.37
19/11/2012	1.278
18/11/2012	0.837
17/11/2012	0.413
16/11/2012	5.212
15/11/2012	1.649
14/11/2012	1.769
13/11/2012	1.735
12/11/2012	0.751
11/11/2012	1.839
10/11/2012	0.957
09/11/2012	8.908
08/11/2012	4.003
07/11/2012	2.87
06/11/2012	2.918
05/11/2012	6.207
04/11/2012	0.642
03/11/2012	0.521
02/11/2012	0.553
01/11/2012	3.088
TOTAL	74.70

	net total per sec
Fecha	kilo bytes/second
31/10/2012	3.496
30/10/2012	1.883
29/10/2012	4.239
28/10/2012	1.687
27/10/2012	0.477
26/10/2012	2.589
25/10/2012	3.564
24/10/2012	2.734
23/10/2012	1.714
22/10/2012	1.994
21/10/2012	3.229
20/10/2012	1.336
19/10/2012	4.946
18/10/2012	1.505
17/10/2012	1.981
16/10/2012	2.092
15/10/2012	1.398
14/10/2012	4.873
13/10/2012	3.497
12/10/2012	5.918
11/10/2012	2.655
10/10/2012	4.866
09/10/2012	3.197
08/10/2012	4.907
07/10/2012	8.757
06/10/2012	2.416
05/10/2012	3.858
04/10/2012	1.646
03/10/2012	2.04
02/10/2012	15.155
01/10/2012	2.073
TOTAL	106.72

	net total per sec
Fecha	kilo bytes/second
28/09/2012	3.311
27/09/2012	4.184
26/09/2012	5.223
25/09/2012	12.211
24/09/2012	10.087
21/09/2012	2.724
20/09/2012	1.931
19/09/2012	0.771
18/09/2012	0.478
17/09/2012	2.949
14/09/2012	0.745
13/09/2012	1.649
12/09/2012	4.542
11/09/2012	1.786
10/09/2012	4.115
07/09/2012	4.378
06/09/2012	2.256
05/09/2012	0.767
04/09/2012	1.299
03/09/2012	2.554
TOTAL	67.96

	net total per sec
Fecha	kilo bytes/second
31/08/2012	2.392
30/08/2012	2.682
29/08/2012	2.437
28/08/2012	1.614
27/08/2012	3.347
24/08/2012	3.576
23/08/2012	2.803
22/08/2012	3.298
21/08/2012	5.35
20/08/2012	3.269
17/08/2012	2.965
16/08/2012	0.927
15/08/2012	1.05
14/08/2012	2.636
13/08/2012	3.817
12/08/2012	0.773
11/08/2012	0.409
10/08/2012	1.263
09/08/2012	5.976
08/08/2012	3.416
07/08/2012	9.192
06/08/2012	2.669
04/08/2012	0.432
03/08/2012	0.867
02/08/2012	2.062
01/08/2012	2.435
TOTAL	71.66

	net total per sec
Fecha	kilo bytes/second
31/07/2012	0.864
30/07/2012	2.952
29/07/2012	0.359
28/07/2012	0.79
27/07/2012	2.051
26/07/2012	4.13
25/07/2012	1.584
24/07/2012	1.429
23/07/2012	1.308
20/07/2012	0.744
19/07/2012	1.519
18/07/2012	1.958
17/07/2012	1.588
16/07/2012	0.818
14/07/2012	21.424
13/07/2012	2.903
12/07/2012	1.223
11/07/2012	2.265
10/07/2012	1.818
09/07/2012	2.987
08/07/2012	0.42
07/07/2012	0.463
06/07/2012	0.781
05/07/2012	1.251
04/07/2012	0.655
03/07/2012	1.583
02/07/2012	0.632
01/07/2012	0.415
TOTAL	60.91

	net total per sec
Fecha	kilo bytes/second
30/06/2012	0.422
29/06/2012	0.681
28/06/2012	1.97
27/06/2012	0.862
26/06/2012	1.553
25/06/2012	6.541
24/06/2012	0.47
23/06/2012	0.472
22/06/2012	4.56
21/06/2012	1.058
20/06/2012	2.621
19/06/2012	3.761
18/06/2012	0.802
17/06/2012	0.364
16/06/2012	0.358
15/06/2012	1.716
14/06/2012	0.813
13/06/2012	1.327
12/06/2012	1.025
11/06/2012	0.63
08/06/2012	0.549
07/06/2012	0.893
06/06/2012	1.141
05/06/2012	0.442
04/06/2012	1.234
03/06/2012	0.526
02/06/2012	0.516
01/06/2012	0.594
TOTAL	37.90

	net total per sec
Fecha	kilo bytes/second
31/05/2012	0.906
30/05/2012	0.629
29/05/2012	1.245
28/05/2012	2.26
27/05/2012	0.595
24/05/2012	2.423
23/05/2012	5.441
22/05/2012	1.764
21/05/2012	0.612
20/05/2012	0.432
19/05/2012	0.556
18/05/2012	3.695
17/05/2012	3.323
16/05/2012	3.079
15/05/2012	0.653
14/05/2012	3.586
12/05/2012	0.43
11/05/2012	1.612
10/05/2012	3.201
09/05/2012	5.508
08/05/2012	0.502
07/05/2012	0.476
06/05/2012	0.558
05/05/2012	0.484
04/05/2012	1.33
03/05/2012	0.975
02/05/2012	0.85
01/05/2012	0.349
TOTAL	47.47

	net total per sec
Fecha	kilo bytes/second
30/04/2012	1.094
29/04/2012	0.403
28/04/2012	0.468
27/04/2012	2.787
26/04/2012	0.88
25/04/2012	0.735
24/04/2012	1.27
23/04/2012	0.556
22/04/2012	0.48
21/04/2012	0.495
20/04/2012	1.428
19/04/2012	1.934
18/04/2012	0.531
17/04/2012	0.945
16/04/2012	0.828
13/04/2012	1.198
12/04/2012	3.092
11/04/2012	0.902
10/04/2012	2.146
09/04/2012	0.576
05/04/2012	0.589
04/04/2012	1.002
03/04/2012	1.212
02/04/2012	1.302
TOTAL	26.85

	net total per sec
Fecha	kilo bytes/second
30/03/2012	0.703
29/03/2012	0.819
28/03/2012	0.948
27/03/2012	0.721
26/03/2012	0.757
25/03/2012	0.596
24/03/2012	0.6
23/03/2012	8.26
22/03/2012	0.725
21/03/2012	2.66
20/03/2012	0.884
19/03/2012	1.661
17/03/2012	0.606
16/03/2012	5.017
15/03/2012	5.306
14/03/2012	0.746
13/03/2012	0.574
12/03/2012	1.311
11/03/2012	0.371
10/03/2012	0.363
09/03/2012	0.989
08/03/2012	3.753
07/03/2012	8.2
06/03/2012	0.472
05/03/2012	0.922
03/03/2012	0.494
02/03/2012	0.706
01/03/2012	0.772
TOTAL	49.94

	net total per sec
Fecha	kilo bytes/second
29/02/2012	4.589
28/02/2012	5.4
27/02/2012	0.754
25/02/2012	0.468
24/02/2012	1.093
23/02/2012	1.319
22/02/2012	1.094
21/02/2012	0.673
20/02/2012	0.787
17/02/2012	2.302
16/02/2012	2.322
15/02/2012	2.359
14/02/2012	9.958
13/02/2012	1.304
10/02/2012	3.55
09/02/2012	0.587
08/02/2012	0.571
07/02/2012	2.338
06/02/2012	1.484
03/02/2012	0.613
02/02/2012	1.308
01/02/2012	0.472
TOTAL	45.35

	net total per sec
Fecha	kilo bytes/second
31/01/2012	1.454
30/01/2012	2.677
27/01/2012	4.457
26/01/2012	16.383
25/01/2012	12.406
24/01/2012	2.363
23/01/2012	2.071
22/01/2012	0.356
21/01/2012	0.358
20/01/2012	6.856
19/01/2012	3.505
18/01/2012	3.636
17/01/2012	2.595
16/01/2012	2.258
15/01/2012	0.457
14/01/2012	0.446
13/01/2012	3.852
12/01/2012	3.781
11/01/2012	6.339
10/01/2012	9.627
09/01/2012	1.786
08/01/2012	0.352
07/01/2012	0.344
06/01/2012	0.418
05/01/2012	0.385
04/01/2012	0.378
03/01/2012	1.051
02/01/2012	0.379
01/01/2012	0.407
TOTAL	91.38