

**UNIVERSIDAD CENTRAL DE VENEZUELA**  
**FACULTAD DE INGENIERÍA**  
**ESCUELA DE INGENIERÍA ELÉCTRICA**

**ACTUALIZACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DEL  
SIGECOF A ENLACES FRAME RELAY E IMPLEMENTACIÓN DEL  
ESQUEMA DE SEGURIDAD**

Trabajo de Grado presentado a la ilustre Universidad Central de Venezuela para optar al  
título de Especialista en Comunicaciones y Redes de Comunicación de Datos

Caracas, Octubre de 2005

**UNIVERSIDAD CENTRAL DE VENEZUELA**  
**FACULTAD DE INGENIERÍA**  
**ESCUELA DE INGENIERÍA ELÉCTRICA**

**ACTUALIZACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DEL  
SIGECOF A ENLACES FRAME RELAY E IMPLEMENTACIÓN DEL  
ESQUEMA DE SEGURIDAD**

Trabajo de Grado presentado a la ilustre Universidad Central de Venezuela para optar al  
título de Especialista en Comunicaciones y Redes de Comunicación de Datos

Presentado por:

**Ing. Fernando Y. Zerpa D.**

Tutor Académico:

**Prof. Vincenzo Mendillo**

Caracas, Octubre de 2005

---

## **DEDICATORIA**

A mi madre, pilar fundamental en el éxito de mis proyectos.

A mis hermanos, por su apoyo incondicional.

A mis amigos y compañeros.

---

## AGRADECIMIENTOS

- A Dios Todopoderoso y a la Santísima Virgen, por haberme dado la oportunidad de vivir, por guiarme y acompañarme siempre.
- A mi querida madre, por haber guiado mis pasos y por su apoyo incondicional.
- A mis compañeros y amigos de estudios con quien compartí momentos gratos y difíciles en esta nueva meta.
- A todos quienes de una u otra forma contribuyeron a la culminación e implantación de este proyecto.

---

**UNIVERSIDAD CENTRAL DE VENEZUELA**  
**FACULTAD DE INGENIERIA**  
**ESCUELA DE INGENIERÍA ELÉCTRICA**

**TRABAJO ESPECIAL DE GRADO**

Especialización: Comunicaciones y Redes de Comunicación de Datos

Tema: Actualización de la Infraestructura Tecnológica del Sigecof a Enlaces Frame Relay e Implementación del Esquema de Seguridad

Ponente: Fernando Y. Zerpa D.

**Resumen**

El presente Trabajo Especial de Grado tiene como objetivo actualizar la infraestructura tecnológica del Sistema Integrado de Gestión y Control de las Finanzas Públicas (SIGECOF) el cual es Administrado por La **Oficina Nacional de Contabilidad Pública (ONCOP)**, ente rector de las Finanzas Públicas del Estado adscrito al Ministerio de Finanzas, con la finalidad de garantizar la integridad y confidencialidad de la información, así como la disponibilidad de los recursos y servicios de la red, permitiendo aumentar la calidad de los procedimientos relacionados con el área de negocios.

La **Oficina Nacional de Contabilidad Pública (ONCOP)**, es el Organismo administrador del SIGECOF, para ello, formuló en 1997, su primer Plan Estratégico orientado a modernizar la plataforma informática. El cual fue aprobado por la Oficina Central de Estadística e Informática de la Presidencia de la República. El referido Plan, fue ejecutado en un alto porcentaje en el año 1998. Sin embargo, los nuevos requerimientos de los usuarios, nuevos sistemas y el advenimiento del nuevo siglo, obliga a formular un nuevo Plan Estratégico, que permita actualizar y resguardar las bases de la información y la inversión efectuada por la Oficina en el área de informática.

Este nuevo Plan Estratégico, está orientado a la actualización de la infraestructura actual de conexión y a la implementación de un esquema de seguridad entre la Administración Central y los Organismos Ordenadores de Compromisos y Pagos (OOCOP), en único protocolo de comunicación de alta velocidad a través de una

---

Red Digital, capaz de transmitir datos a grandes velocidades con una tasa mínima de retardo y errores.

En palabras más simples, migración de la infraestructura actual de conexión a enlaces **Frame Relay**, servicio rápido, seguro y estable de conmutación de paquetes de longitudes variables para transportar datos sobre áreas extensas e implementación de túneles VPN la cual representa una gran solución en cuanto a seguridad, confidencialidad e integridad de los datos.

En la implementación de esta nueva infraestructura se propone utilizar como plataforma de transporte la Red Conmutada de CANTV, consolidando la comunicación de datos solicitados sobre enlaces Frame Relay.

---

## INDICE

|                                                                                       |            |
|---------------------------------------------------------------------------------------|------------|
| <b>AGRADECIMIENTO.....</b>                                                            | <b>iii</b> |
| <b>RESUMEN.....</b>                                                                   | <b>v</b>   |
| <b>INTRODUCCIÓN.....</b>                                                              | <b>1</b>   |
| <b>Capítulo 1: Justificación y Objetivos del Proyecto.....</b>                        | <b>2</b>   |
| Planteamiento del Problema.....                                                       | 2          |
| Justificación del Proyecto.....                                                       | 3          |
| Objetivos.....                                                                        | 4          |
| General.....                                                                          | 4          |
| Específicos.....                                                                      | 4          |
| Limitaciones.....                                                                     | 5          |
| <b>Capítulo 2: Tecnología Frame Relay.....</b>                                        | <b>6</b>   |
| Introducción.....                                                                     | 6          |
| Antecedentes.....                                                                     | 6          |
| Estándares asociados a Frame Relay.....                                               | 8          |
| Estructura de una Red Frame Relay.....                                                | 12         |
| Teoría de Operación.....                                                              | 14         |
| Estructura del Protocolo.....                                                         | 16         |
| Formato de la Trama Frame Relay.....                                                  | 17         |
| Estructura del Campo de Dirección.....                                                | 18         |
| Direccionamiento en Frame Relay.....                                                  | 20         |
| Parámetros asociados a la tecnología Frame Relay.....                                 | 21         |
| Control de Flujo y Manejo de la Congestión.....                                       | 23         |
| Notificación de Congestión Explícita.....                                             | 25         |
| Control del cumplimiento del CIR.....                                                 | 26         |
| Adaptación de la Velocidad.....                                                       | 26         |
| Implementaciones de Frame Relay usando Circuitos Virtuales<br>Permanentes (PVCs)..... | 26         |
| Gestión de los PVCs.....                                                              | 28         |
| Descripción de los Elementos de Información.....                                      | 30         |
| Descripción de los Procedimientos.....                                                | 32         |

---

|                                                                                      |           |
|--------------------------------------------------------------------------------------|-----------|
| Verificación de la Integridad del Enlace.....                                        | 33        |
| Incorporación de nuevos PVCs.....                                                    | 35        |
| Disponibilidad de los PVCs.....                                                      | 35        |
| Manejo de las Condiciones de Error.....                                              | 36        |
| Implementaciones de Frame Relay usando Circuitos Virtuales<br>Conmutados (SVCs)..... | 36        |
| Gestión de los SVCs.....                                                             | 37        |
| Descripción de los Elementos de Información.....                                     | 43        |
| Procedimientos de Establecimiento.....                                               | 48        |
| Procedimientos de Liberación.....                                                    | 49        |
| Manejo de las Condiciones de Error.....                                              | 50        |
| <b>Capítulo 3: Redes Privadas Virtuales (VPN) y Firewall.....</b>                    | <b>52</b> |
| Introducción.....                                                                    | 52        |
| ¿Qué es una Red Privada Virtual (VPN)?.....                                          | 52        |
| Tecnología de túnel.....                                                             | 54        |
| Protocolos utilizados en las VPNs.....                                               | 55        |
| Categorías de VPN.....                                                               | 61        |
| Requerimientos básicos de una VPN.....                                               | 61        |
| Controles y riesgos asociados a la tecnología VPN.....                               | 62        |
| Ventajas de una VPN.....                                                             | 63        |
| Protegiendo la red: VPN y Firewall.....                                              | 63        |
| El Firewall ó Cortafuego.....                                                        | 64        |
| Funciones Básicas de un Firewall.....                                                | 65        |
| Niveles de Filtrado de un Firewall.....                                              | 65        |
| Tipos de Firewall.....                                                               | 66        |
| Ventajas de un Firewall.....                                                         | 67        |
| Limitaciones de un Firewall.....                                                     | 68        |
| <b>Capítulo 4: Infraestructura Actual.....</b>                                       | <b>69</b> |
| Situación Actual.....                                                                | 69        |
| Plataforma Tecnológica Actual.....                                                   | 70        |
| Sistema de Acceso al Sigecof.....                                                    | 71        |
| Sistema de Seguridad del Sigecof.....                                                | 73        |
| Limitaciones en la Plataforma Actual.....                                            | 73        |

---

---

|                                                                                               |            |
|-----------------------------------------------------------------------------------------------|------------|
| Requerimientos de la Plataforma Tecnológica Actual.....                                       | 74         |
| <b>Capítulo 5: Desarrollo del Proyecto.....</b>                                               | <b>76</b>  |
| Descripción de la Solución.....                                                               | 76         |
| Localidades y Requerimientos.....                                                             | 76         |
| Interconexión Sede Principal – Sedes Remotas.....                                             | 77         |
| Configuración de los Equipos Router Cisco 3660 y 1720.....                                    | 80         |
| Implantación del Esquema de Seguridad Firewall.....                                           | 82         |
| Sistema de Seguridad WatchGuard.....                                                          | 82         |
| Características de Seguridad más destacadas del Sistema Firebox.....                          | 82         |
| Características de gestión destacadas.....                                                    | 85         |
| Especificaciones Técnicas.....                                                                | 87         |
| Estrategia e Implantación de la Solución.....                                                 | 91         |
| Diseño e implementación de la arquitectura de red a montar.....                               | 92         |
| Instalación y configuración de equipos Router.....                                            | 94         |
| Configuración del Firewall III WatchGuard 4500 (Sede Principal)<br>y 700 (Sedes Remotas)..... | 102        |
| Configuración de las Redes Privadas Virtuales – VPN.....                                      | 109        |
| Pruebas de Servicios.....                                                                     | 115        |
| <b>CONCLUSIONES.....</b>                                                                      | <b>117</b> |
| <b>RECOMENDACIONES.....</b>                                                                   | <b>119</b> |
| <b>GLOSARIO DE TERMINOS Y ABREVIATURAS.....</b>                                               | <b>120</b> |
| <b>BIBLIOGRAFIA.....</b>                                                                      | <b>126</b> |
| <b>FUENTES ELECTRONICAS.....</b>                                                              | <b>127</b> |
| <b>ANEXOS.....</b>                                                                            | <b>128</b> |

---

## INDICE DE FIGURAS

### Capítulo 2: Tecnología Frame Relay

|                                                                                                          |    |
|----------------------------------------------------------------------------------------------------------|----|
| Figura 2.1. Red Frame Relay.....                                                                         | 12 |
| Figura 2.2. Interfaces UNI y NNI dentro de una conexión Frame Relay.....                                 | 13 |
| Figura 2.3. Asignación del ancho de banda en Frame Relay.....                                            | 15 |
| Figura 2.4. Modo de operación del protocolo Frame Relay.....                                             | 15 |
| Figura 2.5. Estructura del protocolo Frame Relay.....                                                    | 17 |
| Figura 2.6. Transporte de tramas en Frame Relay.....                                                     | 17 |
| Figura 2.7. Estructura de la trama Frame Relay.....                                                      | 18 |
| Figura 2.8. Estructura del campo de dirección de la trama Frame Relay.....                               | 18 |
| Figura 2.9. Operación de direccionamiento en Frame Relay.....                                            | 21 |
| Figura 2.10. Operación para controlar el CIR.....                                                        | 23 |
| Figura 2.11. Envío de tramas de acuerdo a la calidad de servicio.....                                    | 24 |
| Figura 2.12. Tipos de congestión que se presentan en redes Frame Relay.....                              | 25 |
| Figura 2.13. Formato general de las tramas que transportan los mensajes de<br>señalización.....          | 29 |
| Figura 2.14. Estructura del elemento de información verificación de integridad<br>del enlace.....        | 31 |
| Figura 2.15. Estructura del elemento de información situación del PVC.....                               | 32 |
| Figura 2.16. Procedimientos de interrogación y respuesta en la señalización de<br>PVCs.....              | 33 |
| Figura 2.17. Procedimiento de verificación de secuencias numéricas.....                                  | 35 |
| Figura 2.18 Estructura del elemento de información referencia de llamada.....                            | 44 |
| Figura 2.19. Estructura del elemento de información tipo de mensaje.....                                 | 44 |
| Figura 2.20. Estructura del elemento de información número de usuario<br>llamado.....                    | 45 |
| Figura 2.21. Formato del elemento de información causa.....                                              | 46 |
| Figura 2.22. Estructura del elemento de información identificador de conexión<br>de enlace de datos..... | 46 |
| Figura 2.23. Elemento de información parámetros de núcleo de enlace de<br>datos.....                     | 47 |

---

|                                                                               |     |
|-------------------------------------------------------------------------------|-----|
| Figura 2.24. Proceso de establecimiento del circuito virtual.....             | 48  |
| Figura 2.25. Proceso de liberación del SVC.....                               | 50  |
| <b>Capítulo 3: Redes Privadas Virtuales (VPN) y Firewalls</b>                 |     |
| Figura 3.1. Red Privada Virtual (VPN).....                                    | 53  |
| Figura 3.2. Funcionamiento de una VPN.....                                    | 53  |
| Figura 3.3. Protocolos utilizados.....                                        | 54  |
| Figura 3.4. Tecnología de túnel.....                                          | 55  |
| Figura 3.5. Capas del encapsulamiento PPTP.....                               | 56  |
| Figura 3.6. Escenario típico L2TP.....                                        | 59  |
| Figura 3.7. Relación entre los marcos PPP y los mensajes de control.....      | 60  |
| Figura 3.8. Firewall y servidor VPN en dispositivos separados.....            | 64  |
| Figura 3.9. Firewall y servidor VPN incorporados en un mismo dispositivo..... | 64  |
| Figura 3.10. Firewall: Bloqueo de ataques externos.....                       | 65  |
| <b>Capítulo 4: Infraestructura Actual</b>                                     |     |
| Figura 4.1. Esquema red actual.....                                           | 70  |
| Figura 4.2. Sistema de acceso actual.....                                     | 72  |
| <b>Capítulo 5: Desarrollo del Proyecto</b>                                    |     |
| Figura 5.1. Esquema simplificado red a implementar.....                       | 79  |
| Figura 5.2. Conexión a través de Túneles VPN IPSec.....                       | 80  |
| Figura 5.3. Vista física del Firebox® 4500 Firewall.....                      | 87  |
| Figura 5.4. Vista física del Firebox® 700 Firewall.....                       | 89  |
| Figura 5.5. Arquitectura de red a montar.....                                 | 92  |
| Figura 5.6. Arquitectura de red sede principal.....                           | 93  |
| Figura 5.7. Arquitectura de red sedes remotas.....                            | 93  |
| Figura 5.8. Conexión Firewall sede principal.....                             | 103 |
| Figura 5.9. Configuración final Firewall 4500.....                            | 106 |
| Figura 5.10. Configuración final Firewall 700.....                            | 106 |
| Figura 5.11. Conexiones en tiempo real sede principal sedes remotas.....      | 107 |
| Figura 5.12. Uso del enlace en tiempo real.....                               | 107 |
| Figura 5.13. Esquema VPN general.....                                         | 110 |
| Figura 5.14. Túnel VPN.....                                                   | 111 |
| Figura 5.15. Configuración VPN.....                                           | 112 |
| Figura 5.16. Configuración VPN Security.....                                  | 112 |

---

---

|                                           |     |
|-------------------------------------------|-----|
| Figura 5.17. Configuración VPN final..... | 113 |
| Figura 5.18. VPN Manager.....             | 113 |
| Figura 5.19. VPN creadas.....             | 114 |

---

## INDICE DE TABLAS

### Capítulo 2: Tecnología Frame Relay

|                                                                                         |    |
|-----------------------------------------------------------------------------------------|----|
| Tabla 2.1. Estándares asociados a la tecnología Frame Relay.....                        | 9  |
| Tabla 2.2. Asignación de los DLCIs para los posibles campos de información.....         | 19 |
| Tabla 2.3. Especificaciones asociadas a la gestión de los PVCs.....                     | 27 |
| Tabla 2.4. Elementos de información que constituyen al mensaje ESTADO.....              | 29 |
| Tabla 2.5. Elementos de información que componen al mensaje CONSULTA DE ESTADO.....     | 30 |
| Tabla 2.6. Valores posibles para el elemento de información tipo de informe.....        | 31 |
| Tabla 2.7. Mensajes involucrados en la gestión de los SVCs.....                         | 38 |
| Tabla 2.8. Elementos de información que componen al mensaje ESTABLECIMIENTO.....        | 39 |
| Tabla 2.9. Elementos de información que componen el mensaje de LLAMADA en CURSO.....    | 40 |
| Tabla 2.10. Elementos de información presentes en el mensaje CONEXIÓN.....              | 40 |
| Tabla 2.11. Elementos de información presentes en el mensaje DESCONEXIÓN.....           | 41 |
| Tabla 2.12. Elementos de información que componen el mensaje de LIBERACIÓN.....         | 41 |
| Tabla 2.13. Elementos de información que componen al mensaje de CONSULTA de ESTADO..... | 42 |
| Tabla 2.14. Elementos de información que componen el mensaje de ESTADO...               | 43 |
| Tabla 2.15. Codificaciones posibles del elemento de información tipo de mensaje.        | 44 |

### Capítulo 4: Desarrollo del Proyecto

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| Tabla 4.1. Distribución de enlaces Sigecof conectados por la red de Finanzas..... | 71 |
| Tabla 4.2. Distribución de enlaces Sigecof Conectados por la red de Platino.....  | 71 |

### Capítulo 5: Desarrollo del Proyecto

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| Tabla 5.1. Localidades del proyecto.....                                          | 77 |
| Tabla 5.2. Configuración Frame Relay para transporte de tráfico de voz y datos... | 78 |
| Tabla 5.3. Disponibilidad de datos en los Routers por localidad.....              | 78 |
| Tabla 5.4. Configuración Router para la sede principal.....                       | 81 |
| Tabla 5.5. Configuración Router para las 26 localidades remotas.....              | 82 |

---

|                                                                      |     |
|----------------------------------------------------------------------|-----|
| Tabla 5.6. Funciones de seguridad Firebox® III.....                  | 85  |
| Tabla 5.7. Características de gestión Firebox® III.....              | 86  |
| Tabla 5.8. Especificaciones técnicas modelo Firebox® III 4500.....   | 88  |
| Tabla 5.9. Especificaciones de funcionamiento Firebox® III 4500..... | 88  |
| Tabla 5.10. Especificaciones técnicas modelo Firebox® III 700.....   | 89  |
| Tabla 5.11. Especificaciones de funcionamiento Firebox® III 700..... | 90  |
| Tabla 5.12. Direccionamiento IP Routers.....                         | 94  |
| Tabla 5.13. Lista de interfaces configuradas Firewall principal..... | 104 |
| Tabla 5.14. Rutas adicionales configuradas en la sede principal..... | 105 |
| Tabla 5.15. Túneles VPN.....                                         | 110 |
| Tabla 5.16. Pruebas de conectividad método Ping.....                 | 115 |

---

## INTRODUCCIÓN

Los avances en la tecnología, Internet y la necesidad de mantener un flujo de información permanente en nuestra organización son factores principales que impulsan la creación y fortalecimiento de una infraestructura de comunicaciones que permita a nuestra organización integrar los servicios de información y ofrecer a nuestros usuarios una atención oportuna, confiable y ajustada a sus necesidades.

El volumen de información generada internamente para la operación y la integración de las aplicaciones actuales, así como el soporte a dichas aplicaciones han orientado a las organizaciones a mejorar e incrementar el uso del ancho de banda tanto en sus redes privadas como entre sus localidades remotas.

La integración en la mayoría de los casos de estas redes locales, dispersas geográficamente, utilizaban líneas alquiladas o canales fijos, lo que no era una solución económicamente conveniente, si se trataba de una red con gran cantidad de localidades. Frame Relay conservando la misma filosofía de su predecesora X.25, suprime gran cantidad de funciones que traen "overhead" (sobrecarga) a la red, y entrega la responsabilidad de varias acciones, entre ellas la detección y corrección de errores a los terminales inteligentes conectados a la red. La consecuencia inmediata de esta decisión es un incremento notable en la velocidad de transmisión y en la eficiencia de la red, proporcionando un ahorro en los costos e implementando una mejor calidad del servicio con la reducción del número de saltos entre nodos intermedios y mejorando con esto su tiempo de respuesta.

Otra de las ventajas de Frame Relay es el manejo del flujo variable o "avalanchas" de información, ya que debido a que no posee un control de flujo, los usuarios pueden enviar tantos datos como necesiten en un momento dado. De este modo es posible que todos los usuarios envíen grandes cantidades de datos en ráfagas por la red ya que el uso del protocolo Frame Relay no forzará al usuario a cesar la transmisión, aunque si existen mecanismos que le recomendaran detener por un momento su envío. Teniendo en cuenta lo antes expuesto y la necesidad que tiene la "Oficina Nacional de Contabilidad Pública - ONCOP" de mejorar la comunicación entre la Administración Central y cada uno de los Organismos Ordenadores de Compromisos y Pagos, evidencia la necesidad de implementar esta nueva tecnología, trayendo como consecuencia una mejora en el control y manejo de la red.

### ***Justificación y Objetivos del Proyecto***

#### **Planteamiento del Problema**

Actualmente la Oficina Nacional de Contabilidad Pública (ONCOP), administra 26 localidades remotas, cada una de ellas cuenta con un Servidor de Base de Datos y Aplicaciones donde reside el Sistema Integrado de Gestión y Control de las Finanzas Públicas (SIGECOF), los enlaces desde la ONCOP a cada una de estas localidades se realiza a través de líneas dedicadas y conexiones por Antenas Inalámbricas provistas por diferentes empresas de Telecomunicaciones, específicamente CANTV, a través de la Red WAN del Ministerio de Finanzas y la Red PLATINO.

Esta infraestructura de conexión data en el caso de la más antigua, desde el año 1998, sobre estos enlaces circula toda la data referente al Sistema SIGECOF, el cual es un Sistema crítico para la Administración Central.

Todo esto afecta directamente la forma como se realizan las actividades dentro de la ONCOP, haciendo difícil la conexión con algunos Organismo e imposibilitando el proceso de automatización en muchas actividades inherentes a esta institución, generando retrasos en los tiempos de atención de las solicitudes de los usuarios del sistema las cuales son atendidas por el Centro de Atención del Usuario Sigecof (CAUS), ubicados físicamente en las instalaciones del Ministerio de Finanzas en la ONCOP, y quienes utilizan la infraestructura actual para conectarse a las diferentes localidades remotas.

Además de los Analistas del CAUS, a estas localidades remotas se conecta también los Organismo Rectores la Tesorería Nacional y la Oficina Nacional de Presupuesto (ONAPRE).

Todo esto ha llevado al Ministerio de Finanzas en conjunto con la ONCOP ha implementar un Plan Estratégico para actualizar la infraestructura tecnológica actual e implementar un esquema de Seguridad para resguardar la Base de Datos de la información de forma que se pueda sacar provecho de la tecnología disponible hoy en día y se puedan implementar en un futuro mecanismos de automatización que hagan de la ONCOP un organismo más eficiente y con tecnología de punta.

---

Sobre la base de estos inconvenientes, se estableció como criterio general del proyecto la actualización de la infraestructura actual de conexión, de forma transparente a los usuarios, mediante la implementación de la tecnología Frame Relay y de un esquema de seguridad a través de Túneles VPN.

Se requiere la interconexión de 27 localidades con la sede principal Ministerio de Finanzas, consolidando el tráfico de datos e implementando un red de seguridad entre todas las localidades del proyecto, así como los usuarios del sistema SIGECOF.

### **Justificación del Proyecto**

Tomando en cuenta que las telecomunicaciones son fundamentales en el proceso productivo de la ONCOP, se hace necesario la actualización de la infraestructura existente y los procesos utilizados para llevar a cabo la misma, obteniendo así una mejor comunicación y un mejor control en todas las actividades realizadas por la oficina.

Partiendo de la problemática planteada, la actualización de la infraestructura tecnológica del Sigecof representaría un gran avance para la ONCOP. Con la actualización de la infraestructura actual, estaríamos consolidando el tráfico de Dato en una sola Red administrada directamente por la oficina, mejorando el tiempo de respuesta de las aplicaciones y de las solicitudes de los usuarios e implementando un esquema de seguridad para resguardar las Base de Datos de la información.

---

## **Objetivo General**

Actualización de la infraestructura tecnológica del SIGECOF e implementación de un esquema de seguridad, mediante la implementación de enlaces Frame Relay, que permita mejorar la prestación de los servicios de red, garantizar su disponibilidad y satisfacer la creciente demanda de servicios y recursos, mejorando la seguridad de la información y los tiempos de respuesta de las aplicaciones que apoyan los procesos del negocio de las distintas unidades y direcciones del Ministerio.

## **Objetivos Específicos**

1. Estudiar la estructura de la Red WAN del SIGECOF, para definir las Redes, Subredes a interconectar, equipos de Internetworking (switch y routers) y Servidores de Base de Datos y Aplicación del Sistema.
2. Estudiar los equipos Ciscos a instalar, esquema de rutas a configurar.
3. Estudiar los Firewall WachtGuard a instalar, definición de políticas de seguridad e instalación del Software de Administración de los Firewall.
4. Coordinación técnica y logística con el personal de CANTV que va a instalar y configurar cada uno de los circuitos Frame Relay en cada una de las localidades remotas y en la sede principal, así como la configuración de los equipos de comunicaciones necesarios.
5. Realizar Pruebas Piloto con el nuevo esquema de conexión para solventar problemas técnicos antes de migrar las localidades restantes al nuevo esquema. Elaborar configuración modelo para la migración del resto de las localidades.
6. Implementar el Esquema de Seguridad, creación de Túneles VPN, sobre enlaces Frame Relay a cada uno de las localidades remotas desde la sede principal que forman parte de la nueva plataforma tecnológica del SIGECOF.
7. Elaborar un cronograma de actividades definiendo inicio de la instalación, recursos humanos, alcance de las pruebas, entonación y culminación.
8. Etapa de mantenimiento, administración diaria, monitoreo del performance de los circuitos y de los equipos.
9. Documentar el proyecto.

---

## **Limitaciones**

No se prevé ningún tipo de limitación para cumplir con los objetivos establecidos. Sin embargo, existen ciertas etapas del trabajo que son consideradas difíciles, tales como: la interrupción de servicios durante la instalación de los nuevos equipos debido a lo delicado de los procesos que se ejecutan actualmente a diario.

### **Tecnología Frame Relay**

#### **Introducción**

Frame Relay es una tecnología de conmutación rápida de paquetes que permite la transferencia de información a grandes velocidades sobre redes de área amplia (WAN). Ha sido desarrollada en base a la calidad de las líneas de transmisión disponibles actualmente y a la gran capacidad de procesamiento que tienen las estaciones terminales. Es así como no se ocupa de retransmisiones ni chequeo de errores, sino que releva estas funciones en los protocolos de capas superiores que residen en los equipos extremos, como por ejemplo TCP (*Transmission Control Protocol*).

Redes de conmutación de paquetes como X.25, redes privadas empleando técnicas de multiplexación en el tiempo (TDM) y antiguas redes usando SDLC, dominaron el mercado de la comunicación de datos en las WAN desde los años 80's hasta principios de los 90's. Pero, con la creciente demanda de ancho de banda, se hizo necesario el desarrollo de una tecnología que permitiera transportar datos a grandes velocidades. De esta manera surgió Frame Relay. Este protocolo tuvo sus orígenes en las recomendaciones de la ISDN (*Integrated Service Digital Network*). Sin embargo, ha sido visto como la tecnología de relevo de X.25 y fue propuesto como estándar al Comité Consultivo Internacional de Telegrafía y Telefonía o CCITT en 1984.

En este capítulo se pretenden describir con cierto detalle todos los aspectos relacionados con esta tecnología de conmutación rápida de paquetes. Esta sección corresponde a la base teórica de la presente investigación y es fundamental para el entendimiento de los capítulos posteriores.

#### **Antecedentes**

La conmutación de paquetes como tal, fue introducida en el mundo de las comunicaciones hace aproximadamente 25 años. La forma de conmutar paquetes denominada Frame Relay surgió gracias a la convergencia de varios factores: necesidad de alta velocidad, estructura de transmisión sencilla y una buena relación costo - beneficio.

---

A medida que los requerimientos de las redes fueron cambiando, los procesadores también lo hicieron. La evolución vino acompañada de un decremento en los costos de éstos dispositivos y trajo como consecuencia la proliferación de terminales inteligentes, PCs, estaciones de trabajo poderosas y servidores conectados a las LAN (*Local Area Network*). Estos equipos terminales ofrecen la posibilidad de ejecutar en los protocolos de capas superiores labores como el chequeo de errores y la retransmisión de la información. Sin la sobrecarga asociada a la detección y corrección de errores, se podía desarrollar una técnica que transportara mayor cantidad de información en menor cantidad de tiempo.

Las soluciones que se planteaban antiguamente para la interconexión de LAN eran a través de líneas dedicadas. Esta alternativa presenta la característica de que a medida que se incrementa la necesidad de ancho de banda, la distancia y el número de lugares enlazados, los costos se elevan significativamente. La tecnología Frame Relay ofrece características que lo hacen ideal para la interconexión de redes de área local sobre redes públicas o privadas, pues es un protocolo diseñado para transportar tráfico de datos tipo ráfaga que no requiere de una velocidad de transmisión constante, sino de grandes anchos de banda por períodos cortos de tiempo. Además, en los casos en los que se desea interconectar varios puntos, Frame Relay brinda soluciones a costos mucho más reducidos que las líneas muertas o dedicadas gracias al establecimiento de conexiones lógicas.

Frame Relay como técnica, tiene sus raíces en los estándares desarrollados para X.25 y la ISDN. El protocolo usado en el canal D de la ISDN conocido como LAPD (*Link Access Protocol for D channel*), basado en el LAPB (*Link Access Protocol Balanced*) para X.25, proporciona los lineamientos para la definición de Frame Relay. El LAPB es un protocolo de capa de enlace o de capa 2, según el famoso modelo de referencia OSI (*Open System Interconnect*). La capa 2 es responsable de establecer y mantener una conexión confiable sobre el enlace, garantizando que las tramas de información sean transferidas sin la presencia de errores. Frame Relay puede ser más eficiente que otros protocolos de capa 2 en términos de velocidad de operación y facilidad de implementación.

---

## **Estándares asociados a Frame Relay**

A lo largo de los años muchos protocolos de comunicación han sido desarrollados e implementados, algunos con más éxito que otros. En la década de los 60 y parte de los 70, fue común que los fabricantes desarrollaran un conjunto de protocolos de carácter propietario, que sólo funcionaban en sus productos, mas no en otros.

En la década del 70, IBM publicó su primera especificación para una nueva arquitectura de comunicación, SNA (*Systems Networks Architecture*). Dado que los productos IBM eran los más populares alrededor del mundo, dispositivos compatibles con SNA comenzaron a aparecer rápidamente. El mundo de clientes atados a productos propietarios comenzó a desaparecer, y el organismo de estandarización conocido como CCITT publicó sus recomendaciones relativas a X.25. Con la finalidad de garantizar la interoperatividad entre los dispositivos que conforman las redes de comunicaciones, los fabricantes deben apegarse a las recomendaciones de los cuerpos de estándares internacionales.

Las dos organizaciones que más han tenido participación en el desarrollo de estándares para Frame Relay son: el antiguo CCITT ahora conocido como UIT-T (Unión Internacional de Telecomunicaciones – Sector Telecomunicacines) y ANSI (*American National Standard Institute*).

Frame Relay no surgió por sí sólo como un protocolo de comunicación. El protocolo original fue definido dentro de un conjunto de recomendaciones del CCITT como un protocolo para la ISDN. Éste debía prestar el servicio de transporte de datos eficientemente, con bajo retardo y sin recuperación de errores. Se le conoce con el nombre de LAPD (*Link Access Protocol - D Channel*). Los miembros pertenecientes a los cuerpos de estándares reconocieron que el LAPD tenía características que podían ser muy útiles en otras aplicaciones. Una de ellas es que provee la capacidad para multiplexar varios circuitos virtuales en la misma conexión física a nivel de capa 2 o nivel de trama.

La industria de las telecomunicaciones se ha estado moviendo rápidamente. Los usuarios demandan cada vez mayor velocidad. Hay dos maneras de satisfacer éstos requerimientos: aumentar la capacidad de procesamiento de los conmutadores o disminuir el *overhead* del protocolo. El incremento del poder de procesamiento está sujeto a la disponibilidad de los componentes procesadores disponibles en el mercado.

Los organismos de estándares antes mencionados, elaboran normas lentamente en comparación con los requerimientos del mercado. En consecuencia, los fabricantes decidieron trabajar juntos para definir sus propios estándares y garantizar la interoperatividad. El resultado fue el llamado “grupo de los cuatro”, formado inicialmente por *Digital Equipment Corporation (DEC)*, *Northern Telecom*, *Cisco* y *Stratacom*. Hoy varias compañías se han sumado al grupo y se le conoce con el nombre de *Frame Relay Forum (FRF)*. Estos publican periódicamente acuerdos de implementación o IA (*Implementation Agreement*) en los que se especifican los lineamientos a seguir en la fabricación de los equipos. La siguiente tabla resume los estándares asociados a la tecnología:

*Tabla 2.1 Estándares asociados a la tecnología Frame Relay*

| Organización | Estándar                    | Breve Descripción                                                                                                          |
|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| ITU-T        | I.222.                      | Descripción de los servicios portadores en modo paquete.                                                                   |
| ITU-T        | I.233                       | Descripción de los servicios portadores Frame Relay.                                                                       |
| ITU-T        | I.370                       | Manejo de la congestión para servicios portadores en modo trama.                                                           |
| ITU-T        | I.555                       | Interoperatividad entre servicios portadores en modo trama y otros servicios                                               |
| ITU-T        | E.164                       | Plan de numeración para la ISDN.                                                                                           |
| ITU-T        | Q.922 (Anexo A)             | Descripción de los servicios portadores en modo trama para el del núcleo de capa de enlace de datos.                       |
| ITU-T        | Q.933 (Anexo A)             | Procedimientos de señalización de los servicios portadores en modo trama para control y monitoreo de los PVCs              |
| ITU-T        | Q.933                       | Procedimientos de señalización de los servicios portadores en modo trama para el control de la llamada en la interfaz UNI. |
| ITU-T        | X.76 (Revisado) Sección 10. | Procedimientos de señalización en redes públicas de datos para el control de la llamada en la intrefaz NNI.                |
| ITU-T        | X.76 (Anexo A)              | Procedimientos para el establecimiento de PVCs conmutados (SPVCs).                                                         |
| ITU-T        | X.121                       | Plan de numeración para redes públicas de datos.                                                                           |
| ANSI         | T1.606                      | Descripción de los servicios portadores Frame Relay.                                                                       |
| ANSI         | T1.617                      | Procedimientos de señalización para los servicios portadores Frame Relay.                                                  |
| ANSI         | T1.618                      | Descripción de los métodos de formato y transmisión para Frame Relay.                                                      |
| FRF          | FRF 1.1                     | Descripción de la interfaz UNI para PVCs en Frame Relay.                                                                   |
| FRF          | FRF 2.1                     | Descripción de la interfaz NNI para PVCs en Frame Relay.                                                                   |

---

|     |         |                                                        |
|-----|---------|--------------------------------------------------------|
| FRF | FRF 3.1 | Descripción del encapsulamiento multiprotocolo         |
| FRF | FRF 4.1 | Señalización en la interfaz UNI para SVCs.             |
| FRF | FRF 5   | Interoperatividad de red entre Frame Relay y ATM.      |
| FRF | FRF 8.  | Interoperatividad de servicio entre Frame Relay y ATM. |
| FRF | FRF 10. | Señalización en la interfaz NNI para SVCs.             |
| FRF | FRF 11  | Descripción del transporte de voz sobre Frame Relay.   |

El desarrollo de estándares en organismos como ANSI y la UIT-T ha ido en paralelo. Es por ello que la gran mayoría de las especificaciones emitidas por un cuerpo y otro coinciden en los aspectos más importantes. De manera similar, los acuerdos de implementación emitidos por el FRF son de carácter más comercial y por lo general hacen referencia a una u otra recomendación de ANSI o la UIT-T según sea el caso.

- **Recomendaciones T1.606 (ANSI) e I.233 (UIT-T)**

Estas recomendaciones son equivalentes y describen el servicio de transporte de datos en modo trama. Entre otras cosas, se especifica que la transferencia de información debe ser bidireccional, manteniendo el orden de las tramas. Adicionalmente, éstas deben ir acompañadas de una etiqueta que sirve como identificador lógico de carácter local y durante el transporte, la red sólo puede modificar la etiqueta o la secuencia de verificación de integridad de la trama. Por lo demás, la transferencia se efectúa transparentemente.

- **Recomendación T1.618 (ANSI) y Anexo A de Q.922 (UIT-T)**

El protocolo LAP-F es el que utiliza Frame Relay a nivel de la capa 2, según el modelo referencial de OSI, para el transporte de las tramas. LAP-F corresponde sólo al núcleo de ésta capa y se define en detalle en estas recomendaciones.

Se describen los procedimientos por medio de los cuales se lleva a cabo la comunicación entre dos entidades de capa de enlace de datos y, entre éstas y las capas adyacentes. La comunicación entre dos entidades se efectúa por medio del transporte de tramas y, entre capas por el intercambio de primitivas.

- **Recomendaciones T1.617 (ANSI) y Q.933 (UIT-T)**

En los anexos A y D correspondientes, se definen los procedimientos por medio de los cuales se establece y monitorea el estado de un PVC. Todo esto gracias a mensajes de

---

señalización que se intercambian entre el equipo de acceso del usuario y el equipo de acceso de la red. Aquí se definen los tipos de mensajes así como también su formato.

La recomendación Q.933 establece cuales son los mensajes de señalización que se intercambian entre dos entidades de comunicación para establecer, mantener y liberar un circuito virtual conmutado o SVC. A esta recomendación se hace referencia en los acuerdos de implementación del FRF para definir la señalización de SVCs en la interfaz Usuario - Red.

- **Recomendación X.76, Sección 10 (UIT-T)**

X.76 es un protocolo de capa 3. Pero, los mensajes definidos para la interfaz Red - Red en esta recomendación han sido adoptados por el FRF para implementar los circuitos virtuales conmutados en la interfaz NNI.

- **Recomendación I.555 (UIT-T)**

Aquí se definen los procesos que se llevan a cabo para que la interoperatividad de Frame Relay con otros protocolos sea posible. De manera similar, en los acuerdos FRF 5 y FRF 8, se definen los dos modos en los que pueden coexistir Frame Relay y ATM.

- **Recomendaciones E.164 y X.121 (UIT-T)**

Estas dos recomendaciones emitidas por la UIT-T, corresponden a los planes de numeración que pueden adoptarse en el caso de que se preste el servicio Frame Relay con circuitos virtuales conmutados o SVCs. X.121 fue en principio, definido para el protocolo X.25, al igual que E.164 para la ISDN. De manera muy general, ambas recomendaciones especifican un código de longitud variable que sirve como identificador internacional. Dentro de dicho código, además del país, se lleva información acerca de una red específica y del respectivo abonado. Se especifican códigos particulares para cada país según la ubicación física. La distribución nacional de los números se deja a cargo de los organismos locales. El FRF, en los acuerdos de implementación asociados a SVCs, recomienda el uso del plan E.164.

- **Acuerdo de Implementación FRF 11**

Dado que en los últimos años ha sido posible el transporte de voz sobre redes Frame Relay, el FRF decidió elaborar este documento. Allí se especifica la manera por medio de la cual los paquetes de voz digitalizada se encapsulan dentro de una trama Frame Relay y como pueden coexistir los servicios de voz y datos en un mismo acceso.

---

## Estructura de una Red Frame Relay

Existen dos maneras de implementar el servicio Frame Relay en redes públicas o privadas según las definiciones de los cuerpos de estándares. Los bloques principales que componen una red Frame Relay son (Ver figura 2.1):

- Los equipos terminales, que pueden ser PCs, servidores o *hosts*.
- El equipo de acceso a la red, entre los que se encuentran los *routers* y los FRADs (*Frame Relay Access Devices*).
- El puerto de acceso a la red Frame Relay.
- Los equipos de red conocidos como FRND (*Frame Relay Network Device*). En esta categoría entran los conmutadores (o *switches*) y los multiplexores.

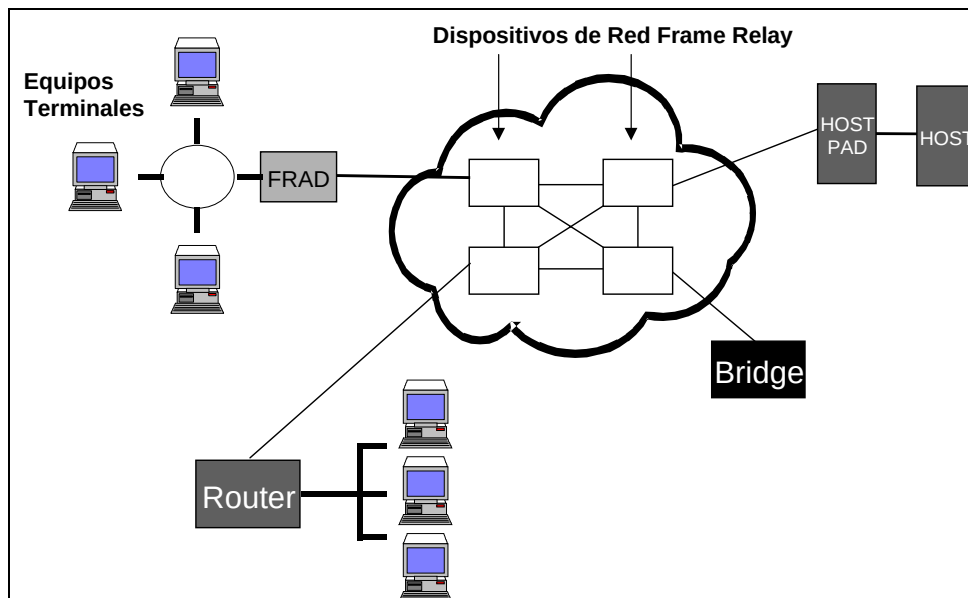


Figura 2.1. Red Frame Relay

Normalmente, existe una diversidad de aplicaciones con sus respectivos protocolos asociados que pueden ser transportados por una red Frame Relay. Para que esto sea posible, un dispositivo debe insertar en tramas Frame Relay la información proporcionada por estos protocolos. Esta tarea es efectuada por el FRAD. A los dispositivos que no están contruidos especialmente para estos fines, se les adiciona una tarjeta y un software especial para que puedan efectuar las labores de segmentación y formateo de las tramas. Tal es el caso de los *routers*.

---

El puerto de acceso para el usuario es un puerto físico en el equipo del cliente, como por ejemplo en un *router*. Este puerto es entonces conectado al puerto de acceso a la red Frame Relay, el cual es un puerto físico en un conmutador por lo general ubicado en los predios del proveedor de servicios. El conmutador o el FRND es el que se encarga de conmutar y encaminar las tramas a través de la red, para hacerlas llegar hasta su destino.

A la conexión que existe entre el equipo de acceso del cliente y el equipo de acceso a la red se le conoce como Interfaz Usuario - Red o UNI (*User to Network Interface*). De manera similar, a la conexión que existe entre dos redes Frame Relay se le llama Interfaz Red - Red o NNI (*Network to Network Interface*).

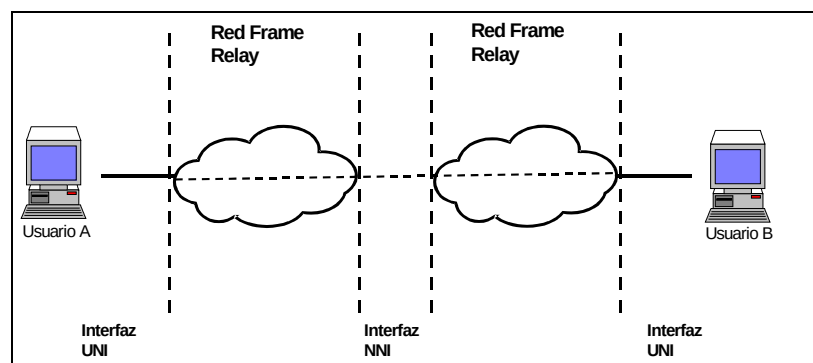


*Figura 2.2. Interfaces UNI y NNI dentro de una conexión Frame Relay.*

Cada UNI soporta uno o varios circuitos virtuales. Aunque cada circuito virtual termina en el puerto del conmutador Frame Relay, desde el punto de vista del usuario es como si llegara hasta sus predios. Este camino virtual es similar a una línea dedicada, aunque las características de tráfico, conmutación y ancho de banda pueden ser muy diferentes. Además, pueden ser configurados por el administrador de la red (caso de circuitos virtuales permanentes o PVC), o establecidos en el momento en que el usuario lo requiera (caso de circuitos virtuales conmutados o SVC). La interfaz UNI puede ser vista como una autopista y los circuitos virtuales como los canales por los que los autos (en este caso tramas) circulan.

Existen varias maneras de ingresar a una red Frame Relay: por medio de una línea dedicada o empleando una red conmutada como la ISDN. En el primer caso se instala un circuito físico desde el equipo del cliente hasta la sede del proveedor de servicios. En el segundo caso se tiene un acceso conmutado a la red que presta el servicio Frame

---

Relay. Originalmente, esta tecnología se diseñó para ser utilizada a través de la ISDN exclusivamente. Este caso no aplica en Venezuela, ya que no se cuenta con una ISDN pública.

### **Teoría de Operación**

La característica fundamental que le permite a Frame Relay manejar gran cantidad de información en períodos cortos de tiempo, es que no contempla la detección ni corrección de errores. Las tramas no válidas son simplemente descartadas. Esto equivale a remover la capa 3, según el modelo referencial OSI, del protocolo X.25.

Para que Frame Relay preste un buen servicio, es esencial que el medio de transmisión esté, en la medida de lo posible, libre de errores de transmisión. Todo lo concerniente a la corrección de errores y el control de flujo es manejado por los equipos en los predios del cliente o CPE (*Customer Premises Equipment*), que normalmente cuentan con una gran capacidad de procesamiento.

Frame Relay es un protocolo que trabaja bajo los conceptos de multiplexación estadística, asignando el ancho de banda sólo cuando el usuario lo necesita. Es por ello que opera muy bien en la interconexión entre LANs, donde el tráfico es esporádico y tipo ráfaga.

En Frame Relay a cada usuario se le asigna un canal virtual por el que éste enviará la información. Dentro de un enlace físico pueden existir múltiples canales virtuales. Con la asignación dinámica del ancho de banda, si hay tres canales asignados a tres usuarios respectivamente y sólo un usuario necesita transmitir en un período determinado de tiempo, entonces este usuario puede tomar todo el ancho de banda disponible. Diferente a TDM, no se desperdicia el ancho de banda cuando alguno de los usuarios no transmite información. Esta situación se ilustra en la figura 2.3 en la que se tiene un canal físico con tres circuitos lógicos programados. En el instante  $t=1$  un usuario ocupa todo el ancho de banda disponible en los circuitos virtuales. De manera similar, para el segundo período de tiempo, dos usuarios comparten la capacidad del canal. En el instante  $t=3$ , los tres usuarios están transmitiendo información y comparten el ancho de banda disponible en el circuito físico.

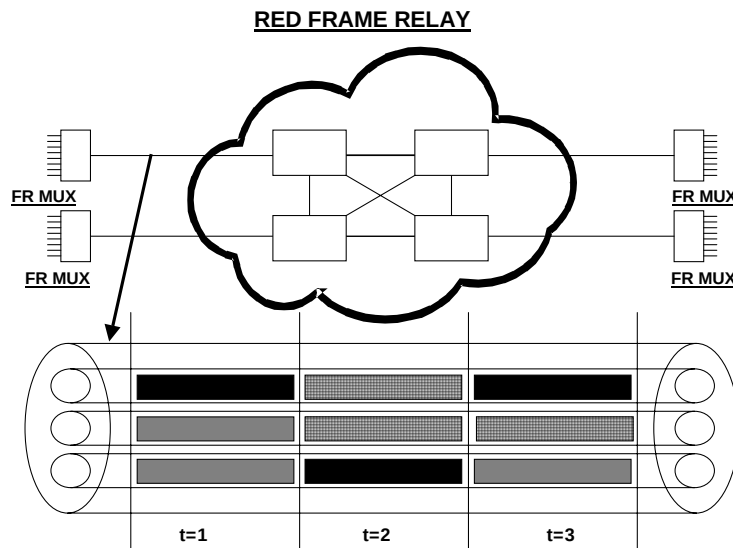


Figura 2.3. Asignación del Ancho de Banda en Frame Relay.

Frame Relay es un protocolo muy sencillo. En la figura 2.4 se muestra un aspecto clave de su simplicidad. El nodo A transmite información hacia su destino y ésta pasa a través del nodo B. No existen números de secuencia en la trama. Por esta razón, el nodo B sólo las releva hacia el enlace de salida que corresponda con el destino correcto. Si la trama es recibida con error, como muestra la cuarta trama del ejemplo, el nodo B simplemente no efectúa la entrega y la descarta.

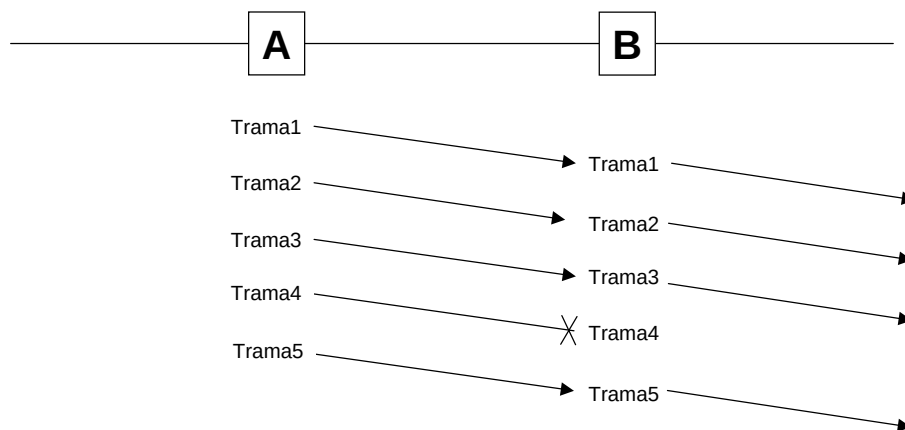


Figura 2.4. Modo de Operación del Protocolo Frame Relay.

En el camino de transmisión, la trama pasa por un número determinado de nodos intermedios antes de llegar a su destino. Cada uno de los enlaces entre éstos nodos corresponde a un segmento del circuito virtual y tienen un número asociado que los identifica. A éste se le conoce con el nombre de Identificador de Conexión de Enlace de Datos o DLCI (*Data Link Connection Identifier*). Este es el equivalente a una dirección,

---

pero sólo tiene carácter local. Es decir, una vez que la trama sale de un nodo cambia su identificador de enlace de datos.

#### ▪ **Estructura del Protocolo**

Para entender el modo en que Frame Relay trabaja, es necesario visualizar la estructura del protocolo sobre la cual este servicio se basa. Las interfaces y servicios que involucra el Protocolo Frame Relay se extienden desde la capa 1 (o física) hasta la capa 3 (o de red) del modelo de referencia OSI. Frame Relay elimina y/o combina ciertas operaciones de cada una de éstas capas para ofrecer un servicio orientado a conexión, con bajo retardo, altas velocidades de transmisión, sin corrección de errores ni retransmisión de tramas.

Frame Relay opera bajo el principio de enlaces lógicos, que son establecidos, según el modelo de capas OSI, en la capa de enlace de datos. Es así como las principales funciones del protocolo se ubican dentro de la capa 2 y, como es tan simple, el transporte sólo emplea el núcleo de ésta.

Como el servicio Frame Relay proviene de los servicios portadores de la ISDN, involucra dos subniveles lógicos en la capa de enlace de datos. Están definidos como el plano de control o plano C y el plano de usuario o plano U. El modelo estructural de éstos planos en comparación con el modelo OSI se muestra en la figura 2.5. Cada uno de ellos proporciona distintos servicios. El plano U efectúa el transporte de información por el acceso físico a través de conexiones lógicas. Para Frame Relay, las funciones del plano U están definidas en el anexo A de la recomendación Q.922 de la UIT-T y sólo involucra la capa 2 del modelo de referencia. El plano de control es el que se encarga del reporte de estados de los PVCs o del establecimiento y liberación de los SVCs (*Switched Virtual Circuits*) por medio de mensajes de señalización. Es también función de este plano la negociación de las clases de servicio en el caso de los circuitos conmutados, ya que para los permanentes la *QoS (Quality of Service)* está predefinida. Los mensajes de señalización, definidos en la capa 3, son encapsulados en tramas de capa 2 para ser transmitidos. La supervisión del transporte de tramas de capa 2 es efectuada también por el plano C. A nivel de capa 2, las funciones de éste plano están definidas en la recomendación Q.922 de la UIT-T. Para la capa 3, los procedimientos del plano C están descritos en la recomendación Q.933 del mismo organismo.

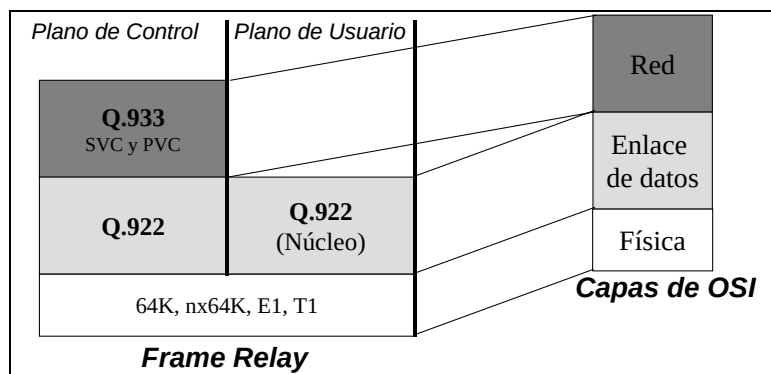


Figura 2.5. Estructura del protocolo Frame Relay.

El transporte Frame Relay sólo involucra las capas 1 y el núcleo de la capa 2. Dentro de la red, las tramas son relevadas entre nodos como muestra la figura 2.6. Los conmutadores Frame Relay operan en la capa 2, mientras que el transporte de datos en las interfaces UNI o NNI opera en la capa 1. La capa física de Frame Relay puede operar a velocidades que van desde 64Kbps o nx64Kbps hasta E1 (2048Kbps) o T1 (1544Kbps). Existen normas de estandarización para llegar hasta velocidades de 34Mbps (nivel jerárquico E3), pero ésta implementación es todavía poco común. Los detalles de la capa 1 se encuentran en la recomendación T1.601 de ANSI.

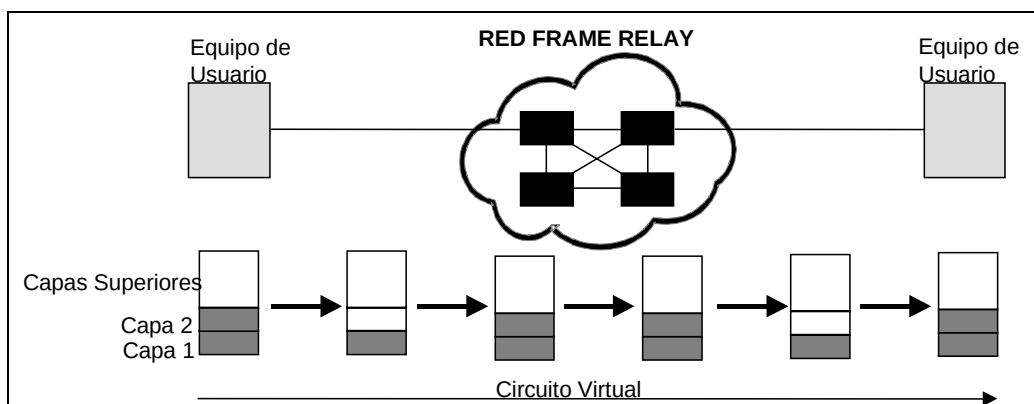


Figura 2.6. Transporte de tramas en Frame Relay

#### ▪ Formato de la Trama Frame Relay

Como ya se ha dicho antes, la trama utilizada en el protocolo Frame Relay deriva del protocolo LAP-D para la ISDN. Su estructura se muestra en la figura 2.7 y coincide con la definida en el anexo A de la recomendación Q.922 de la UIT-T. En una trama Frame Relay los datos de los usuarios son encapsulados de manera transparente. Frame Relay simplemente adiciona 2 bytes a la información que le proporcionan las capas superiores para conformar la unidad llamada “trama”.

|          |                    |                      |           |          |
|----------|--------------------|----------------------|-----------|----------|
| 1 Octeto | 2 Octetos          | Longitud Variable    | 2 Octetos | 1 Octeto |
| Bandera  | Campo de Dirección | Campo de Información | FCS       | Bandera  |

Figura 2.7. Estructura de la trama Frame Relay

Todas las tramas deben comenzar y terminar con una bandera de un octeto cuya secuencia numérica corresponde con seis unos delimitados por dos ceros. En la figura, éstas corresponden con el primer y último campo. El segundo campo es el de dirección y ocupa 2 octetos. Este puede ser extendido a tres o cuatro *bytes* según los requerimientos de la red. En algunas referencias, al campo de dirección se le llama encabezado o *header* de la trama. El siguiente campo está identificado en la figura como campo de información y es allí donde se ubican los datos del usuario y los mensajes de señalización. Se recomienda que todas las redes admitan como mínimo 1600 octetos para el campo de información. Los proveedores de servicio normalmente utilizan un campo de información de 4096 octetos de longitud. El FCS (*Frame Check Sequence*) es el mismo que se emplea en otros protocolos de la capa de enlace de datos y ocupa dos octetos. Éste chequea la integridad de toda la trama y es calculado de acuerdo al algoritmo CRC-16 (*16-bit Cyclic Redundancy Check*) definido en la especificación T1.618 de ANSI.

#### ▪ Estructura del Campo de Dirección

El formato que posee el campo de dirección se muestra en la figura 2.8.

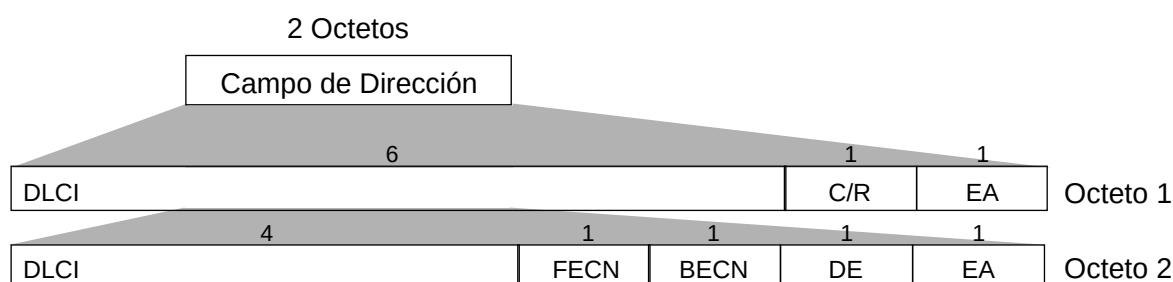


Figura 2.8. Estructura del campo de dirección de la trama Frame Relay.

El identificador de conexión de enlace de datos, mejor conocido como DLCI, ocupa 10 bits del campo de dirección ubicados en los bits más significativos de cada octeto. En teoría, este parámetro sirve para reconocer 1024 circuitos virtuales posibles en cada interfaz (aunque no todos pueden ser utilizados por los usuarios) y es empleado con estos fines tanto en la interfaz UNI como NNI. El DLCI tiene significado local dentro de una red Frame Relay. Esto quiere decir que un circuito virtual punto a punto puede tener diferentes DLCI para los circuitos de acceso en cada extremo. El campo de

dirección puede ser extendido a 3 o 4 octetos para aumentar la capacidad de DLCI por interfaz. En el primer caso, el DLCI tiene una extensión de 16 bit y en el segundo, de 22. En la tabla 2.2 se muestra la asignación de los DLCI según la longitud del campo de dirección.

*Tabla 2.2 Asignación de los DLCIs para los posibles campos de información*

| DLCI (10bits) | DLCI (16bits) | DLCI (22bits)   | Función                                                                                    |
|---------------|---------------|-----------------|--------------------------------------------------------------------------------------------|
| 0             | 0             | 0               | Señalización o Gestión definida para las especificaciones ANSI (anexo D) y UIT-T (anexo A) |
| 1-15          | 1-1023        | 1-131071        | Reservados                                                                                 |
| 16-1007       | 1024-64511    | 131072-8257535  | Asignados para el uso en procedimientos Frame Relay                                        |
| 1008-1022     | 64512-65534   | 8257536-8388606 | Reservados                                                                                 |
| 1023          | 65535         | 8388607         | Para usos del LMI (Local Management Interface) definido por el FRF.                        |

El bit C/R (*Command/Response*) no ha sido usado hasta el momento en las redes Frame Relay, previendo posibles usos futuros. La codificación es específica de la aplicación y es transportado transparentemente por el protocolo del núcleo de la capa de enlace de datos. Los bits EA (*Extended Address*) son los que se emplean para indicar el fin del campo de dirección. El último octeto del campo de dirección debe tener el bit EA colocado a uno, en los demás debe estar en cero.

Los bits FECN y BECN son los bits de notificación explícita de congestión. El FECN es colocado en uno en la dirección origen – destino y sirve para alertar al usuario remoto de que se ha presentado una condición de congestión en el camino de transmisión. El BECN es colocado a uno en la dirección contraria y trabaja de la misma forma que el anterior. Pero en éste caso, la notificación es hacia la fuente de información para que tome medidas preventivas.

El bit DE (*Discard Eligibility*), si se utiliza, es el que indica las primeras tramas en ser descartadas cuando se presenta una condición de congestión. Este puede ser puesto a uno por el equipo de usuario para diferenciar tráfico de alta y baja prioridad, o bien por la red cuando se ha violado el contrato de tráfico establecido. Ninguna red liberará (pondrá a cero) este bit.

---

### ▪ **Direccionamiento en Frame Relay**

La tecnología Frame Relay está basada en el uso de circuitos virtuales. Las conexiones pueden ser establecidas de dos maneras distintas: a través de circuitos virtuales conmutados o SVCs y de circuitos virtuales permanentes o PVCs. Éstos últimos son configurados por el operador de la red, mientras que los SVCs se establecen en el momento en que el usuario demanda la comunicación.

Cada circuito virtual corresponde a una conexión lógica entre dos usuarios. El tráfico que éstos generan pasa a través de la red por varios conmutadores hasta llegar a su destino. Los DLCI proporcionan el esquema para enrutar la información. En los *switches* es donde se efectúa la operación de direccionamiento de las tramas. Consiste en sustituir la dirección proveniente de la línea de entrada en una dirección equivalente de salida. Esta tarea se realiza de la siguiente manera:

1. Se chequea la integridad de toda la trama haciendo uso del *Frame Check Sequence* (FCS). Si se detecta algún error, la trama es descartada.
2. Se extrae el DLCI de la trama y se revisa en las tablas de enrutamiento. Si el DLCI no está definido, se descarta la trama.
3. Se releva la trama hacia su destino, haciéndola salir por el puerto o troncal que corresponde según la tabla de enrutamiento, adicionándole antes el nuevo DLCI.

En la figura 2.9 se muestra un ejemplo de la operación que se lleva a cabo cuando dos usuarios se comunican a través de una red Frame Relay. En el primer *router* se aceptan tramas de entrada con los DLCI 70 y 45. Esto equivale a dos conexiones lógicas de la LAN hacia la red que están contenidas en un mismo enlace físico. El conmutador, después de verificar el FCS, consulta la tabla de enrutamiento y encuentra que las tramas conteniendo el DLCI 70 provenientes del primer *router* (quien debe tener un puerto físico asignado en el conmutador), deben ser conmutadas al puerto del *host* con el DLCI 60. En cada nodo se efectuará un proceso similar hasta que la información llegue a su destino.

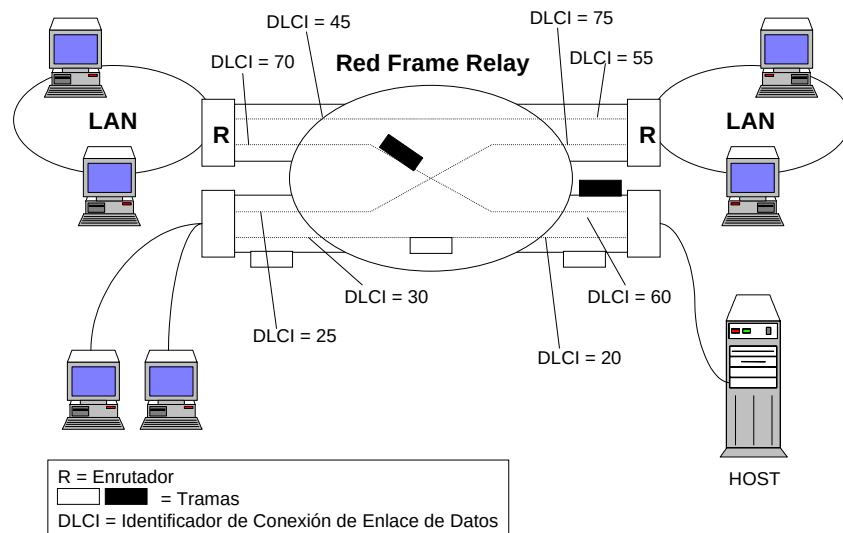


Figura 2.9. Operación de direccionamiento en Frame Relay.

La operación descrita anteriormente muestra que los DLCI pueden ser reusados por los conmutadores. La red Frame Relay puede ser configurada para que los DLCI tengan significado global. Esto simplificaría el esquema de direccionamiento, pero restringiría enormemente el número de conexiones lógicas posibles dentro de la red.

### Parámetros asociados a la tecnología Frame Relay

Existen ciertos parámetros que permiten manejar el tráfico y definir la calidad de servicio en redes Frame Relay. Estos especifican la cantidad de información que un usuario puede transmitir en un período de tiempo, bien sea contratada o en exceso. A continuación se definen los más importantes:

- Velocidad de Acceso, **AR (Access Rate)**. Es la máxima velocidad a la cual pueden ser enviados los datos hacia la red y, está determinada por la velocidad en que opera el circuito físico que conecta al usuario con la red.
- Tamaño de Ráfaga Contratado o Comprometido, **Bc (committed Burst size)**. Corresponde al número máximo de datos en bits que la red se compromete a transmitir, sin descartar, durante un intervalo de tiempo Tc.
- Intervalo de Medida, **Tc (Measurement Interval)**. Es el período de tiempo sobre el cual se miden las velocidades de transmisión y la cantidad de datos transmitidos.
- Tamaño de Ráfaga en Exceso, **Be (excess Burst size)**. Es la cantidad de información (en bits) en exceso sobre el Bc que la red intentará transmitir en el mismo intervalo

---

de tiempo  $T_c$ . Las tramas así transmitidas se marcan con el bit DE indicando que son elegibles para el descarte en caso de que la red así lo requiera.

- Velocidad de Información Contratada, **CIR (*Committed Information Rate*)**. Indica la velocidad a la cual la red se compromete a transmitir los datos bajo condiciones normales de operación. El CIR debe ser siempre menor o igual que AR y por definición corresponde a la relación entre el Bc y el período de tiempo  $T_c$  en el cual las mediciones son efectuadas. Esto es,  $CIR = Bc / T_c$  (bit/s). Normalmente, este es el principal criterio de facturación y medida de calidad de servicio en las redes Frame Relay.
- Velocidad de información en exceso, **EIR (*Excess Information Rate*)**. Está definido como la velocidad de transmisión por encima del CIR con la cual la red intentará transmitir la información si tuviese capacidad. El EIR es la relación que existe entre el Be y el intervalo de medición  $T_c$ . Esto es,  $EIR = Be / T_c$ . Con el EIR el usuario dispone de una cantidad adicional de ancho de banda por circuito virtual, que se toma prestado del resto de los circuitos virtuales existentes en la interfaz que no estén en uso.

Un puerto físico Frame Relay puede tener múltiples circuitos virtuales (VC). En cada VC pueden ser asignados dos valores independientes del CIR (uno en cada dirección). En estos caso se tienen VC asimétricos.

Existen dos maneras de asignar el CIR en un canal de acceso. La diferencia radica en si la suma de los CIR asociados sobrepasa o no la capacidad de la línea. El primer caso se conoce como sobre-suscripción y se configura con el supuesto de que todos los usuarios no transmiten al mismo tiempo, en base a estudios de tráfico efectuados previamente.

El valor correspondiente al intervalo de medición  $T_c$ , se escoge convenientemente de modo que sea superior al tiempo que tarda una trama en ser transmitida. Tampoco se coloca muy grande pues, en ese caso, todas las tramas deberían ser transportadas por la red. Normalmente, se eligen el Bc y el CIR que permiten caracterizar mejor el tráfico en la red y de ésta manera el  $T_c$  queda automáticamente determinado. Por sencillez, normalmente el  $T_c$  toma el valor de 1 segundo.

---

## Control de Flujo y Manejo de la Congestión

Para controlar el flujo de información que un usuario envía a una red Frame Relay, existen mecanismos instalados en los conmutadores para garantizar que el usuario no viole el contrato de tráfico.

El algoritmo que permite controlar el CIR es similar a un sistema de crédito basado en un depósito de fichas como muestra la figura 2.10. El depósito esta representado por un contador que refleja la cantidad de crédito disponible para el usuario, en base a la cantidad de ancho de banda que ha sido utilizado. Inicialmente, este depósito tiene una cantidad de fichas equivalentes al número de bits de data contratados,  $B_c$ . Cuando los datos son enviados, el depósito es reducido en una cantidad igual al número de bits entrando a la red. Las tramas continúan siendo enviadas en el tiempo  $T_c$  mientras el depósito tenga una cantidad positiva de fichas. Si el depósito se vacía y siguen llegando tramas a la red, éstas deben ser marcadas como elegibles antes de ser enviadas o descartadas inmediatamente de acuerdo a la clase de servicio.

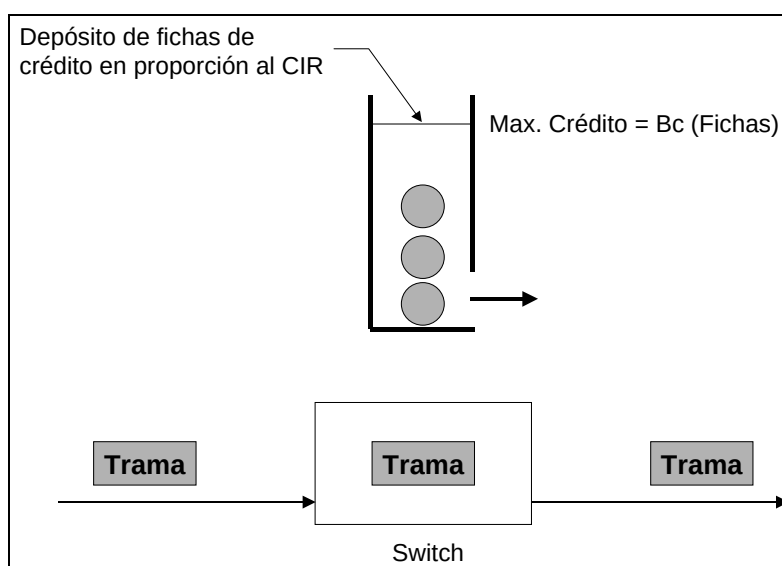


*Figura 2.10. Operación para controlar el CIR.*

La red intentará entregar las tramas marcadas con el bit DE como tramas en exceso. Para ello emplea un mecanismo de control para el EIR muy similar al del CIR. En éste caso, el depósito está lleno de una cantidad de fichas equivalentes al  $B_e$ . Si una trama DE es enviada, la capacidad del depósito se reduce en una cantidad igual al número de bits que entran a la red en cada trama. Si el usuario marca tramas con el bit DE, se descuenta automáticamente la capacidad del depósito  $B_e$  más no el del  $B_c$ .

El procedimiento que se sigue es el siguiente: Cuando una trama arriba a la red, el depósito Bc es chequeado por la disponibilidad de fichas. Si quedan fichas disponibles, el depósito se reduce. En caso contrario si existe un depósito Be y contiene fichas, éste es reducido y la trama es entonces marcada con el bit DE y relevada. El flujo de datos en condiciones normales de operación de la red se muestra en la figura 2.11.

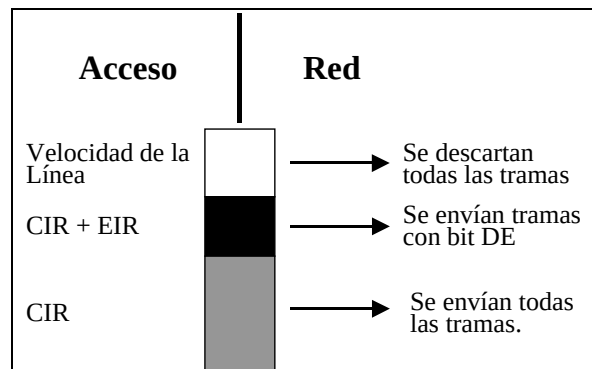


*Figura 2.11. Envío de tramas de acuerdo a la calidad de servicio.*

Uno de los talones de Aquiles del protocolo Frame Relay reside en el manejo de la congestión. Es por ello que se debe prevenir para que no alcance niveles considerables, pues el retraso de las tramas se incrementa en gran medida. Existen dos métodos para manejar la congestión: por medio de la notificación explícita, con los bits FECN, BECN y los mensajes CLLM y, con el análisis de protocolos de capas superiores para reducir la ventana de transmisión.

El único procedimiento con que cuenta Frame Relay para liberarse de la congestión es el descarte de tramas, pero esto ocasiona su retransmisión por parte de los protocolos de capas superiores. De esta manera se corre el riesgo de congestionar en mayor medida al canal de transmisión.

Las maneras como actúa una red Frame Relay cuando se presenta una condición de congestión se representan en la figura 2.12. Cuando no existe congestión, la red transmite todas las tramas de acuerdo a los parámetros de tráfico previamente definidos. Esto corresponde a las condiciones normales de operación. El comienzo de la congestión está representado por el punto A, donde la red empieza a saturar sus *buffers* y coloca a uno los bits de congestión explícita (FECN y BECN). Se espera que bajo estas circunstancias, los dispositivos involucrados en la comunicación tomen acciones preventivas. Este estado corresponde al de congestión mediana. Si el tráfico de entrada continúa incrementándose, se alcanza el estado de congestión severa en el punto B. Esto

ocasiona que la red además de colocar a uno los bits de congestión explícita, descarte las tramas marcadas con el bit DE. La única manera de recuperarse de éste estado de congestión, es haciendo uso de mecanismos que reduzcan el tráfico. En caso de que la cantidad de datos ingresando a la red aumente aún más, la red entra en un estado de congestión absoluta en el cual el dispositivo descarta todas las tramas de llegada y activa una alarma.

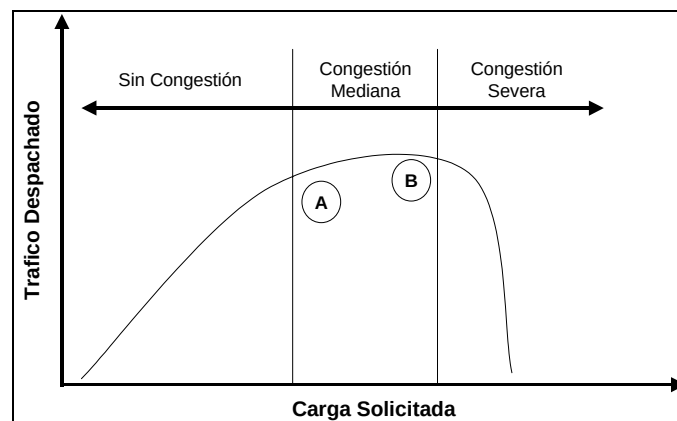


Figura 2.12. Tipos de congestión que se presentan en redes Frame Relay.

Los mecanismos para prevenir la congestión que se aplican en las redes Frame Relay se describen a continuación.

- **Notificación de Congestión Explícita**

Como ya se ha dicho en párrafos anteriores, la notificación explícita se hace por medio de dos bits ubicados en el *header* de la trama conocidos como los bits de notificación explícita hacia adelante y hacia atrás. Sirven para notificar a los usuarios y a los nodos de la red que las tramas han encontrado congestión en el camino de transmisión. El objetivo de estos bits es que los usuarios tomen medidas para reducir el flujo de información y son colocados a uno en los casos de congestión mediana. El FECN se usa para alertar al extremo receptor y el BECN para alertar al transmisor.

Existe otro modo de notificarle explícitamente a los usuarios que se ha experimentado congestión en la red y es por medio del mensaje consolidado de capa de enlace o CLLM (*Consolidated Link Layer Message*). Si la información fluye en un sólo sentido, los bits de congestión explícita no informan a la fuente de congestión del estado de la red. En éstos casos se utilizan los mensajes CLLM que se envían en el campo de información de las tramas que viajan por el DLCI 1023. Estos son incompatibles con la señalización LMI especificada por el FRF, pues usan el mismo canal virtual (La señalización LMI se

---

explicará con detalle más adelante). Es por ello que el Frame Relay Forum especifica que el uso de mensajes CLLM está fuera del alcance de sus acuerdos de implementación.

- **Control del cumplimiento del CIR**

La red restringe la velocidad de transmisión de datos del usuario al valor prefijado. Este valor viene dado por los parámetros Bc, Be, CIR, EIR y Tc. Dicho control se lleva cabo por DLCI y garantiza a los usuarios que comparten la interfaz, que tendrán disponible el ancho de banda contratado. Cuando las tramas que ingresan a la red no cumplen con el contrato establecido, son descartadas.

- **Adaptación de la Velocidad**

La red no puede confiar en que el usuario siempre responderá rápidamente a una condición de congestión (por ejemplo, los dispositivos que no responden a los bits de notificación). En estos casos, se puede invocar una característica conocida como “adaptación de velocidad” donde la relación a la cual los datos entran a la red, es ajustada basándose en el estado de congestión.

Esta es una característica opcional y se implementa reduciendo el EIR (en caso de que aplique) y el CIR en los momentos en los que la red experimenta congestión. Si el usuario no reduce su flujo de información a la misma velocidad en que se disminuyen éstos parámetros, la red comenzará a descartar tramas. Existen dos esquemas: en el primero sólo el EIR es reducido, y en el segundo se reduce también el CIR. Cuando el estado de congestión es superado, la red restituye progresivamente el valor de los parámetros hasta llevarlos a su estado original.

## **Implementaciones de Frame Relay usando Circuitos Virtuales Permanentes (PVCs)**

La tecnología Frame Relay está basada en el concepto de circuitos virtuales. Hoy día existen dos tipos de conexiones posibles, circuitos virtuales conmutados (SVCs) y circuitos virtuales permanentes (PVCs). Los PVCs constituyen la manera original en que el servicio Frame Relay fue ofrecido. Es por ello que son los usados con mayor frecuencia.

Los circuitos virtuales permanentes son establecidos por el operador de la red a través de un sistema de gestión. Estos son inicialmente definidos como una conexión entre dos

---

sitios. Sin embargo, nuevos PVCs pueden ser adicionados cuando existe demanda de conexión hacia otros lugares, de mayor ancho de banda o de rutas alternativas.

Los PVCs definen un camino fijo entre dos puntos y no pueden ser establecidos dinámicamente. Aunque el camino dentro de la red puede tomar varias formas por razones de reenrutamiento del tráfico, los extremos finales de la comunicación permanecen sin cambios. En este sentido un circuito virtual permanente es semejante a un circuito dedicado punto a punto. Sin embargo, empleando PVCs, varios usuarios pueden compartir el ancho de banda disponible en el circuito físico. Esto les proporciona ventajas económicas con respecto a las líneas dedicadas ya que se aprovecha de manera más eficiente la capacidad del canal.

Para el manejo de los PVCs, el protocolo Frame Relay cuenta con mecanismos de señalización. Estos definen la manera como los extremos de una interfaz Frame Relay pueden comunicarse para intercambiar información acerca de los PVCs existentes dentro del enlace.

La información de estado (*status*) es proporcionada por medio del uso de tramas de gestión con una dirección DLCI específica dentro de la interfaz UNI o NNI. El mecanismo que controla el estado de la conexión ha sido definido por los tres cuerpos de estándares más involucrados en el desarrollo de Frame Relay. Existen por ello tres protocolos muy similares entre sí, que se sumarizan en la tabla 2.3. Aunque el término LMI (*Local Management Interface*) está referido al acuerdo de implementación FRF 1.1, con frecuencia es usado para referirse a cualquiera de las especificaciones.

*Tabla 2.3. Especificaciones asociadas a la gestión de los PVCs.*

| Protocolo | Especificación           |
|-----------|--------------------------|
| LMI       | Frame Relay Forum FRF1.1 |
| Annex D   | ANSI T1.617              |
| Annex A   | ITU-T Q.933              |

Normalmente, todos los equipos soportan el protocolo LMI y muchos soportan también el Anexo D, mientras que el Anexo A es implementado por pocos fabricantes. De cualquier modo, para asegurar la interoperatividad de una red constituida por equipos de distintos fabricantes, la misma versión del protocolo de gestión debe estar presente en cada dispositivo.

---

### ▪ **Gestión de los PVCs**

Los procedimientos de gestión permiten efectuar las siguientes funciones:

1. Verificar de la integridad del enlace.
2. Notificar la adición de un PVC.
3. Detectar la supresión de un PVC.
4. Notificar el estado de disponibilidad (activo)<sup>1</sup> o indisponibilidad (inactivo)<sup>2</sup> de un PVC configurado.

La ejecución de éstos procedimientos es efectuada por medio del intercambio de mensajes de capa 3 que son transferidos transparentemente por tramas de información de capa 2 con el DLCI 0 (en el caso del Anexo A y Anexo D) o con el DLCI 1023 (en el caso del LMI). Adicionalmente, los bits FECN, BECN y DE pertenecientes al campo de dirección de la trama, deben ser colocados en cero en la transmisión y no ser interpretados en el extremo receptor.

Los mensajes que se utilizan en los procedimientos de gestión de PVCs son sólo dos: CONSULTA DE ESTADO y ESTADO. Cada uno de ellos está constituido por elementos de información. Algunos son obligatorios y los demás definen el significado del mensaje. Los mensajes son intercambiados dentro de una interfaz UNI o NNI. Es decir, sólo tienen significado local. El formato general de una trama de señalización se muestra en la figura 2.13.

---

<sup>1</sup> Por activo se entiende que la conexión virtual permanente está disponible para ser utilizada.

<sup>2</sup> Por inactivo se entiende que el PVC está configurado, pero no está disponible para ser utilizado.

---

|        |                            |   |   |   |   |   |   |   |
|--------|----------------------------|---|---|---|---|---|---|---|
| Octeto | 8                          | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 1      | Bandera                    |   |   |   |   |   |   |   |
| 2      | 0                          | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3      | 0                          | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 4      | Discriminador de Protocolo |   |   |   |   |   |   |   |
| 5      | 0                          | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
|        | Elementos de Información   |   |   |   |   |   |   |   |
|        | FCS                        |   |   |   |   |   |   |   |
|        | Bandera                    |   |   |   |   |   |   |   |

*Figura 2.13. Formato general de las tramas que transportan los mensajes de señalización.*

### **Mensaje de ESTADO**

Este mensaje se envía en respuesta a un mensaje de CONSULTA DE ESTADO para indicar el estado de los PVCs que existen dentro de una interfaz o para verificar la integridad del enlace. Opcionalmente, puede ser enviado para notificar EL ESTADO de un PVC en particular, caso en el cual se le conoce como mensaje asíncrono de situación de un PVC. En la tabla 2.4 se ilustra el contenido de un mensaje de ESTADO.

*Tabla 2.4. Elementos de información que constituyen al mensaje ESTADO.*

| Elemento de Información                  | Tipo                 | Longitud  |
|------------------------------------------|----------------------|-----------|
| Discriminador de Protocolo               | Obligatorio          | 1 Octeto  |
| Referencia de Llamada                    | Obligatorio          | 1 Octeto  |
| Tipo de Mensaje                          | Obligatorio          | 1 Octeto  |
| Tipo de Informe                          | Obligatorio          | 3 Octetos |
| Verificación de la Integridad del Enlace | Opcional/Obligatorio | 4 Octetos |
| Situación del PVC                        | Opcional/Obligatorio | 5 Octetos |

El elemento de información verificación de integridad del enlace, es opcional sólo en los casos en los que el mensaje de ESTADO sea para reportar el estado de un PVC particular. En otras circunstancias es obligatorio. De manera similar, el elemento de información situación del PVC es obligatorio en los mensajes de ESTADO COMPLETO (*full status*) o cuando se reporta el estado de un sólo PVC. En el primer caso, habrá dentro del mensaje *full status* un elemento de información Situación del PVC por cada PVC configurado dentro del enlace. Estarán dispuestos en orden

---

ascendente de manera que el estado del PVC con el DLCI más bajo, sea reportado primero.

Los mensajes asíncronos de situación de un PVC son opcionales y se transmiten independientes de los mensajes de CONSULTA de ESTADO.

### **Mensaje CONSULTA de ESTADO**

Se envía para solicitar el estado de los PVCs o para verificar la integridad del enlace. El contenido de un mensaje de CONSULTA DE ESTADO se muestra en la tabla 2.5.

*Tabla 2.5. Elementos de información que componen al mensaje CONSULTA DE ESTADO.*

| Elemento de Información                  | Tipo        | Longitud  |
|------------------------------------------|-------------|-----------|
| Discriminador de Protocolo               | Obligatorio | 1 Octeto  |
| Referencia de Llamada                    | Obligatorio | 1 Octeto  |
| Tipo de Mensaje                          | Obligatorio | 1 Octeto  |
| Tipo de Informe                          | Obligatorio | 3 Octetos |
| Verificación de la Integridad del Enlace | Obligatorio | 4 Octetos |

#### **▪ Descripción de los Elementos de Información**

En todo mensaje es obligatoria la presencia de los elementos de información: Discriminador de Protocolo, Referencia de Llamada, Tipo de Mensaje y Tipo de Informe. El discriminador de protocolo sirve para identificar el protocolo de señalización empleado (LMI, Anexo A o Anexo D) y una vez que éste es determinado tiene un valor fijo. Ocupa un octeto dentro del campo de información de la trama. La referencia de llamada que se utiliza en los procedimientos de gestión de los PVCs es ficticia y tiene un valor fijo dado por una secuencia de ocho ceros. El elemento de información Tipo de Mensaje, que le sigue al de referencia de llamada, tiene un octeto de longitud y sólo puede tomar dos valores. Existen sólo dos tipos de mensajes: CONSULTA de ESTADO y ESTADO. En el primer caso, la secuencia binaria del elemento de información es 01110101 y para el segundo, 01111101. El resto de los elementos de información son específicos de cada mensaje. En general, cada uno de ellos tiene un primer octeto que indica el elemento del que se trata. Le sigue un campo que indica la cantidad de octetos que ocupa y, por último, lo que podría llamarse la carga útil de elemento de información.

---

## **Elemento de Información Tipo de Informe**

Este tiene como finalidad indicar el tipo de consulta solicitada o el contenido de un reporte según el tipo de mensaje. Su longitud es de tres octetos y el reporte puede tomar los siguientes valores<sup>3</sup>:

*Tabla 2.6. Valores posibles para el elemento de información tipo de informe.*

| Valores   | Tipo de Informe                            |
|-----------|--------------------------------------------|
| 0000 0000 | Situación total (full status)              |
| 0000 0001 | Sólo verificación de integridad del enlace |
| 0000 0010 | Situación asíncrona de un PVC              |

## **Elemento de Información Verificación de la Integridad del Enlace**

Su finalidad es intercambiar periódicamente una secuencia numérica entre la red y el equipo de usuario. Ocupa 4 bytes. Su contenido se muestra en la figura 2.14.

|        |                                           |   |   |   |   |   |   |   |
|--------|-------------------------------------------|---|---|---|---|---|---|---|
| Octeto | 8                                         | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 1      | 0                                         | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
|        | Identificador del Elemento de Información |   |   |   |   |   |   |   |
| 2      | Longitud del Elemento de Información      |   |   |   |   |   |   |   |
| 3      | Número Secuencial en Emisión              |   |   |   |   |   |   |   |
| 4      | Número Secuencial en Recepción            |   |   |   |   |   |   |   |

*Figura 2.14. Estructura del elemento de información verificación de integridad del enlace.*

Los octetos 3 y 4 corresponden a las secuencias numéricas de emisión y recepción respectivamente. La primera de ellas corresponde a la secuencia válida para el que origina el mensaje y la segunda para el que lo recibe.

## **Elemento de Información Situación del PVC**

Este sirve para reportar el estado de los PVCs existentes en la interfaz. Se puede repetir tantas veces como PVCs existan en caso de que se solicite un mensaje de *full status*. Su longitud depende de la extensión de los DLCIs utilizados en el canal. Si se utiliza el

---

<sup>3</sup> Todos los demás valores están reservados.

formato de 10 bits, éste elemento de información ocupa 5 *bytes*. Su contenido se ilustra en la figura 2.15.

| Octeto | 8                                         | 7          | 6          | 5 | 4 | 3 | 2 | 1 |
|--------|-------------------------------------------|------------|------------|---|---|---|---|---|
| 1      | 0                                         | 1          | 0          | 1 | 0 | 1 | 1 | 1 |
|        | Identificador del Elemento de Información |            |            |   |   |   |   |   |
| 2      | Longitud del Elemento de Información      |            |            |   |   |   |   |   |
| 3      | 0                                         | 0          | DLCI (MSB) |   |   |   |   |   |
| 4      | 1                                         | DLCI (LSB) |            |   |   | 0 | 0 | 0 |
| 5      | 1                                         | 0          | 0          | 0 | N | 0 | A | 0 |

*Figura 2.15. Estructura del elemento de información situación del PVC.*

El bit A colocado a uno indica que el PVC está activo. En caso contrario, el usuario final debe dejar de usar ese circuito virtual para transmitir información. Cuando el bit N está colocado a uno notifica que el PVC es nuevo. En otros casos (cuando está en cero), implica que el PVC ya está presente.

#### ▪ Descripción de los Procedimientos

Estos procedimientos basan su funcionamiento en interrogaciones periódicas (*polling*) que el equipo de usuario efectúa al equipo de red, en el caso de la interfaz UNI. Para la interfaz NNI las consultas son bidireccionales. En la UNI se pueden implementar opcionalmente procedimientos bidireccionales, en los cuales la red puede consultar al equipo de usuario. En cualquiera de los dos casos existen mensajes asíncronos que se implementan opcionalmente para informar de la ocurrencia de un hecho extraordinario. Esta situación se ilustra en la figura 2.16.

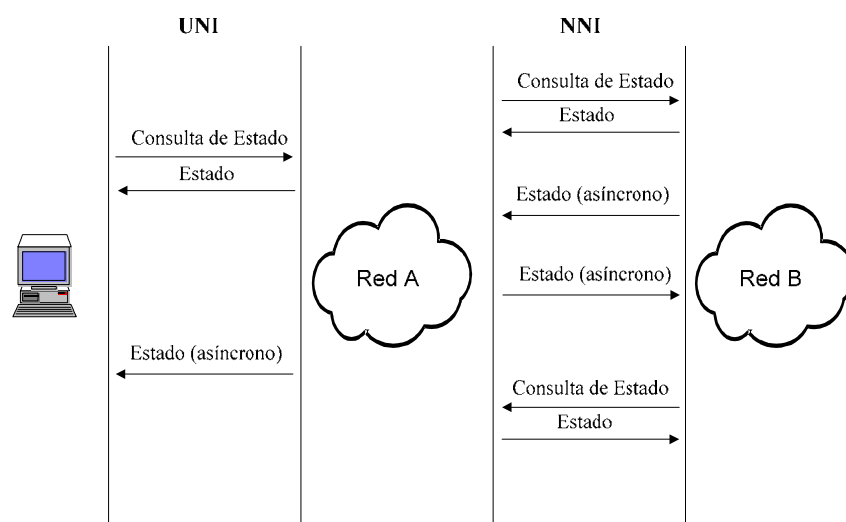


Figura 2.16. Procedimientos de interrogación y respuesta en la señalización de PVCs

Los procedimientos de interrogación secuencial periódica consisten en mensajes de CONSULTA de ESTADO (*status enquiry*) que el usuario envía a la red cada cierto tiempo<sup>4</sup>. Normalmente, éstos sólo solicitan el intercambio de secuencias numéricas para la verificación de integridad del enlace. Después de haber enviado una cierta cantidad de mensajes<sup>5</sup> de éste tipo, el usuario demanda un reporte de *full status* a la red. A cada consulta, la red responde con un mensaje de ESTADO que, en caso de ser sólo para verificación del enlace, contiene los elementos de información tipo de informe y verificación de integridad del enlace. Cuando el mensaje de situación enviado por la red un mensaje de *full status*, contiene además de los elementos de información antes mencionados, un elemento situación del PVC por cada PVC configurado en el enlace.

La red puede responder a cualquier mensaje de consulta con un mensaje de *full status* en caso de que la situación de algún PVC haya cambiado. Cuando un mensaje de *full status* no incluye el estado de algún PVC, del cual se haya proporcionado información antes, el usuario debe interpretar que el PVC ha sido suprimido.

#### ▪ Verificación de la Integridad del Enlace

Dado que las tramas utilizadas para el transporte de información en el nivel 2 son no numeradas, se hace necesario incluir números de secuencias numéricas en el elemento de información verificación de integridad del enlace para determinar la situación del enlace mediante el intercambio de mensajes de señalización.

<sup>4</sup>Éste período de tiempo se especifica en la norma como T391 y corresponde al temporizador de interrogación secuencial de verificación de integridad del enlace. Sus valores pueden ir desde 5 a 30 segundos. Por defecto es de 10 segundos.

<sup>5</sup> La cantidad de mensajes de verificación de integridad del enlace que pasan antes de recibir uno de *full status* es conocido como el parámetro N391. Puede ir desde 1 a 255 y por defecto es 6.

---

Para poder llevar un control de las secuencias numéricas que se intercambian, el usuario y la red cuentan con los contadores de mensajes transmitidos y recibidos<sup>6</sup>. Éstos guardan los valores del número de mensajes emitidos y recibidos por cada dispositivo.

Antes de intercambiar mensajes, los dispositivos involucrados colocan sus contadores en cero. Cada vez que el dispositivo de usuario envía un mensaje de CONSULTA de ESTADO, incrementa su contador de mensajes emitidos y coloca su valor en el tercer octeto del elemento de información verificación de la integridad del enlace. Cuando la red recibe éste mensaje, incrementa el valor del contador de mensajes recibidos y lo compara con el número del contador de mensajes transmitidos, recibido en el respectivo elemento de información. El número de mensajes recibidos por la red debe coincidir con el número de mensajes transmitidos por el usuario. La red realiza el mismo chequeo para el número del contador de mensajes recibidos por el usuario, colocado en el cuarto octeto del elemento de información pertinente. Éste debe ser equivalente al número de mensajes transmitidos por la red. Al responder, la red coloca en el elemento de información verificación de la integridad del enlace contenido en el mensaje de ESTADO, los valores de sus contadores ya actualizados. Cuando el equipo de usuario recibe un mensaje, efectúa un proceso similar al de la red, pero con sus propios contadores. Este proceso queda ilustrado en la figura 2.17. El mismo proceso se repite en la interfaz NNI.

---

<sup>6</sup> Según la recomendación Q.933 de la UIT-T éstos llevan el nombre de contadores de secuencia en emisión y recepción.

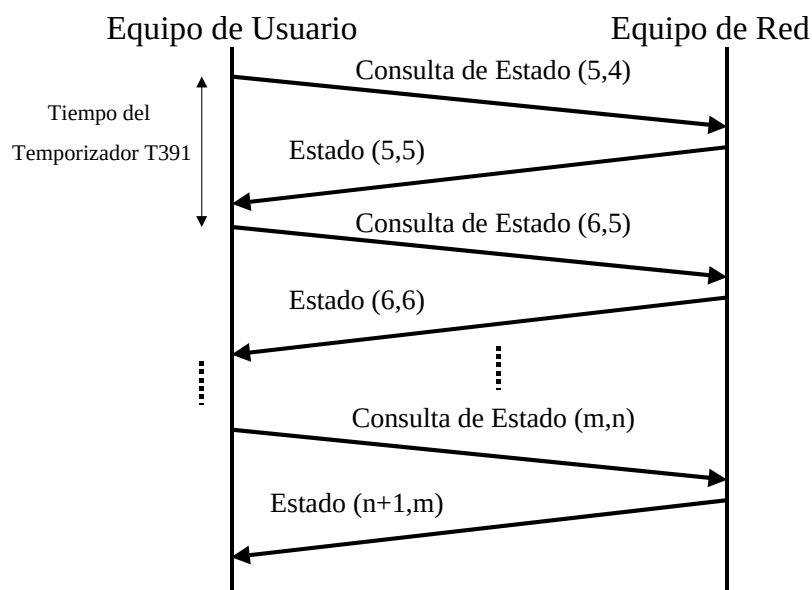


Figura 2.17. Procedimiento de verificación de secuencias numéricas

#### ▪ Incorporación de nuevos PVCs

Una de las funciones de las interrogaciones periódicas es la de notificar al equipo de usuario la adición de nuevos circuitos virtuales permanentes. Este proceso se realiza enviando, por parte de la red, un mensaje de *full status*. De ésta manera se garantiza la imposibilidad de suprimir o agregar un PVC sin que el usuario lo detecte.

Cuando se ha configurado un nuevo PVC, la red transmitirá al usuario un mensaje de *full status* en el que se incluya el elemento de información correspondiente al nuevo PVC, con el bit N puesto a uno. El equipo de usuario actualizará entonces su lista de PVCs. La red no liberará el bit N del elemento de información situación del PVC hasta que reciba un mensaje, consecutivo al de notificación, con una secuencia numérica de mensajes transmitidos y recibidos correcta.

#### ▪ Disponibilidad de los PVCs

La disponibilidad de los PVCs está determinada por el bit A dentro del elemento de información situación del PVC, en cada mensaje de *full status*. Antes de este momento, el usuario no debe transmitir tramas por éste circuito virtual. Para que un PVC esté activo (la red coloque a uno el bit A), se deben cumplir las siguientes condiciones:

1. El PVC ésta configurado y disponible para la transferencia de datos entre los equipos de red involucrados.

- 
2. La interfaz entre el usuario y la red y entre los equipos que conforman la red, está en perfecto estado (se reciben secuencias numéricas correctas).
  3. El equipo remoto del usuario (cuando se soportan procedimientos bidireccionales) reporta el PVC activo.

#### ▪ Manejo de las Condiciones de Error

La red detectará condiciones de error cuando deje de recibir mensajes de CONSULTA de ESTADO por parte del usuario o cuando los reciba con elementos de información inválidos. En ambos casos, cuando se envía un mensaje de *status*, la red inicia un temporizador<sup>7</sup>. Éste indica el tiempo de espera de un mensaje de consulta, antes de retransmitir uno de ESTADO. Si después de una cierta cantidad de mensajes retransmitidos<sup>8</sup> no se reciben mensajes de consulta, la red reporta una condición de error que afecta al servicio y debe colocar los PVCs involucrados en la interfaz como inactivos.

El usuario detecta condiciones de error cuando no recibe mensajes de ESTADO como respuesta a los mensajes de CONSULTA de ESTADO o cuando los recibe con elementos de información inválidos. En este momento debe detener la transmisión de tramas y seguir reenviando los mensajes de *status enquiry* para detectar el reestablecimiento del servicio. El reestablecimiento ocurre cuando se producen N392 eventos sin error.

En el caso de que el usuario reciba información de un PVC nuevo y el elemento de información situación del PVC tenga el bit N en cero, esto es reconocido como una situación de error y el PVC no será agregado a la lista.

### Implementaciones de Frame Relay usando Circuitos Virtuales Conmutados (SVCs)

Es muy ventajoso el hecho de que los usuarios puedan establecer sus comunicaciones, a través de una red Frame Relay, justo en el momento en que lo necesitan. De esta manera se aprovecharían mejor los recursos de la red ya que no habrían conexiones virtuales preestablecidas sin necesidad. Inicialmente este servicio no era ofrecido y, hoy día, no ha sido todavía implementado en muchos países. Sólo fue hasta el año 1996 que el

---

<sup>7</sup> Este temporizador se conoce como T392 y debe ser mayor que el T391. Puede ir desde 5 a 30 segundos y su valor por defecto es de 15 segundos.

<sup>8</sup> Esta cantidad se conoce como contador N392 y corresponde al umbral del número de sucesos monitoreados N393 con error, antes de reportar los PVCs como inactivos. Su valor puede variar de 1 a 10 y, por defecto es 3.

---

Frame Relay Forum concretó los acuerdos de implementación que definen el servicio de SVCs (FRF 4.1 y FRF 10). Estos se basan en el protocolo de señalización especificado en las recomendaciones Q.933 y T1.617 de la UIT-T y ANSI respectivamente, para la interfaz UNI. En la interfaz NNI, los acuerdos de implementación se apoyan en la recomendación X.76 de la UIT-T.

Implementar el servicio de SVCs es mucho más complejo que el de PVCs. Pero por suerte, todos estos detalles son transparentes al usuario. Los circuitos virtuales conmutados son similares a una llamada telefónica. Los usuarios especifican a la red una dirección similar al número telefónico. Basándose en ésta información, la red establece conexiones dinámicas atendiendo las demandas de muchos usuarios. Luego, la red debe liberar la comunicación y facturar de acuerdo a la cantidad de servicio proporcionado.

Los procedimientos de señalización son los que permiten establecer, mantener y liberar una llamada. Básicamente, éstos alertan al destino solicitado de la presencia de una llamada. Si el destino la admite, la red construye un circuito virtual con ayuda de los caminos que dispone. Cuando el SVC queda establecido, los puntos extremos pueden comenzar la transferencia de información. En el momento en que lo deseen, éstos pueden comunicarle a la red su petición para terminar la llamada y ésta se encarga de liberarla.

- **Gestión de los SVCs**

Al igual que en los procedimientos de gestión de los PVCs, los de SVCs se basan en el intercambio de mensajes de capa 3. Todos ellos son transportados a través de las interfaces (NNI o UNI) con un DLCI 0 reservado, por el FRF, para la señalización de los circuitos virtuales conmutados. De esta forma son compatibles con la señalización LMI para los PVCs.

Para el funcionamiento de los SVCs, se debe establecer un plan de numeración de carácter global que identifique a cada usuario en particular. Con este fin se han propuesto los planes de numeración X.121 y E.164 definidos por la UIT-T para los protocolos X.25 e ISDN respectivamente. El Frame Relay Forum apoya, en sus acuerdos de implementación, ambos planes. Se prefiere el plan de numeración E.164.

Dentro de una interfaz, dependiendo de la cantidad de SVCs que existan en un momento dado, pueden haber muchos estados de las llamadas, tanto del lado del usuario como del lado de la red. Estos indican si hay llamadas presentes, en curso, en estado de desconexión, etc<sup>9</sup>.

Los mensajes cuyo intercambio permiten el establecimiento, mantenimiento y liberación de un circuito virtual conmutado se resumen en la siguiente tabla:

*Tabla 2.7. Mensajes involucrados en la gestión de los SVCs*

|                                                   |                                  |
|---------------------------------------------------|----------------------------------|
| <b>Mensajes de Establecimiento</b>                | Conexión                         |
|                                                   | Establecimiento                  |
|                                                   | Llamada en Curso                 |
| <b>Mensajes de Liberación de la Llamada</b>       | Desconexión                      |
|                                                   | Liberación                       |
|                                                   | Liberación Completa              |
| <b>Mensajes Diversos</b>                          | Situación                        |
|                                                   | Consulta de Situación            |
| <b>Mensajes de Restablecimiento</b> <sup>10</sup> | Restablecimiento                 |
|                                                   | Confirmación de Restablecimiento |

De manera similar a la gestión de los PVCs, todos los mensajes de señalización para SVCs, dependiendo del tipo, están constituidos por elementos de información. Adicionalmente, de acuerdo a su utilización, éstos pueden tener los siguientes significados:

1. Local: Sólo es importante para el acceso de origen o de destino.
2. De Acceso: Es significativo para el acceso de origen y de destino.
3. Dual: Significativo en el acceso de origen o de destino y la red.
4. Global: Es importante en los accesos de origen y destino y en la red.

Todos los mensajes tienen presentes elementos de información de carácter obligatorio que son comunes. Como en los procedimientos de gestión de los PVCs, son necesarios los elementos de información: discriminador de protocolo, referencia de llamada y tipo

<sup>9</sup> Una descripción detallada de los estados de las llamadas en ambas interfaces (UNI o NNI), se puede encontrar en las recomendaciones Q.933 y X.76 respectivamente.

<sup>10</sup> Éstos mensajes son exclusivos de la interfaz NNI descrita en la recomendación X.76

de mensaje. La única diferencia es que con SVCs la referencia de llamada no es ficticia. (El elemento de información referencia de llamada se explica con más detalle en la sección posterior identificada como, Elementos de Información Obligatorios).

### **Mensaje de ESTABLECIMIENTO**

Este mensaje es enviado por el usuario que demanda el servicio de SVCs hacia la red, para iniciar el establecimiento de una conexión virtual. Tiene significado global, pues es transportado por la red desde el acceso del usuario de origen hasta el acceso del usuario de destino. Además, puede ser transmitido en ambos sentidos. Está compuesto por los elementos de información que se ilustran en la tabla 2.8.

*Tabla 2.8. Elementos de información que componen al mensaje ESTABLECIMIENTO.*

| Elemento de Información                      | Tipo                 | Longitud      |
|----------------------------------------------|----------------------|---------------|
| Discriminador de Protocolo                   | Obligatorio          | 1 Octeto      |
| Referencia de llamada                        | Obligatorio          | 3 Octetos     |
| Tipo de Mensaje                              | Obligatorio          | 1 Octeto      |
| Capacidad de Portadora                       | Obligatorio          | 4-5 Octetos   |
| Identificador de Conexión de Enlace de Datos | Opcional/Obligatorio | 4 Octetos     |
| Parámetros de Núcleo de Capa de Enlace       | Opcional/Obligatorio | 2-27 Octetos  |
| Número de Parte Llamante                     | Opcional/Obligatorio | 2 Octetos     |
| Subdirección de Parte Llamante               | Opcional             | 2-23 Octetos  |
| Número de Parte Llamada                      | Obligatorio          | 2 Octetos     |
| Subdirección de Parte Llamada                | Opcional             | 2-23 Octetos  |
| Selección de Red de Tránsito <sup>11</sup>   | Opcional             | 2 Octetos     |
| Compatibilidad de Capa Baja                  | Opcional             | 2-8 Octetos   |
| Usuario-Usuario                              | Opcional             | 2-131 Octetos |

El elemento de información identificador de conexión de enlace de datos en el mensaje de establecimiento, es obligatorio en el sentido red - usuario y en la interfaz NNI. El número y subdirección del usuario llamante, al igual que la subdirección del usuario llamado, son opcionales y se usan en el sentido red - usuario sólo cuando el usuario que solicitó la conexión lo incluyó en su mensaje de ESTABLECIMIENTO. En la interfaz

<sup>11</sup> La selección de la red de tránsito se ha pospuesto para estudios futuros.

---

NNI los números de la parte llamante y llamada deben ser especificados en el mensaje de establecimiento.

### **Mensaje LLAMADA EN CURSO**

Este mensaje es enviado por el usuario llamado a la red y por la red al usuario de origen, para indicar que el procedimiento de establecimiento de la conexión solicitada ha sido iniciado. Esto implica que se transmite en ambos sentidos y tiene significado local. Los elementos de información que conforman este mensaje se muestran en la siguiente tabla:

*Tabla 2.9. Elementos de información que componen el mensaje de LLAMADA en CURSO.*

| Elemento de Información                      | Tipo        | Longitud  |
|----------------------------------------------|-------------|-----------|
| Discriminador de Protocolo                   | Obligatorio | 1 Octeto  |
| Referencia de llamada                        | Obligatorio | 3 Octetos |
| Tipo de Mensaje                              | Obligatorio | 1 Octeto  |
| Identificador de Conexión de Enlace de Datos | Opcional    | 4 Octetos |

Si el mensaje de llamada en curso es enviado en respuesta a un mensaje de establecimiento, el elemento de información que identifica a la conexión de enlace de datos debe ser incluido. De esta manera el usuario de origen tiene conocimiento del DLCI asignado.

### **Mensaje de CONEXIÓN**

Cuando el usuario llamado ha terminado el proceso de establecimiento, envía este mensaje a la red para indicar que aceptó la llamada. De manera similar, la red lo envía al usuario de origen para indicar que su solicitud de conexión ha sido concedida. Tiene significado global y puede ser transmitido en ambos sentidos. Este mensaje está constituido por los siguientes elementos de información:

*Tabla 2.10. Elementos de información presentes en el mensaje CONEXIÓN*

| Elemento de Información                      | Tipo        | Longitud     |
|----------------------------------------------|-------------|--------------|
| Discriminador de Protocolo                   | Obligatorio | 1 Octeto     |
| Referencia de llamada                        | Obligatorio | 3 Octetos    |
| Tipo de Mensaje                              | Obligatorio | 1 Octeto     |
| Identificador de Conexión de Enlace de Datos | Opcional    | 4 Octetos    |
| Parámetros de Núcleo de Capa de Enlace       | Opcional    | 2-27 Octetos |

---

|                        |          |               |
|------------------------|----------|---------------|
| Número Conectado       | Opcional | 2 Octetos     |
| Subdirección Conectada | Opcional | 2-23 Octetos  |
| Usuario – Usuario      | Opcional | 2-131 Octetos |

### **Mensaje de DESCONEJÓN**

Cuando un usuario desea que se libere el circuito virtual, envía este mensaje a la red para que lo transporte hasta el otro extremo de la conexión. Es por ello que tiene un significado global. Los elementos de información que componen este mensaje se incluyen en la tabla 2.11.

*Tabla 2.11. Elementos de información presentes en le mensaje DESCONEJÓN*

| Elemento de Información    | Tipo        | Longitud     |
|----------------------------|-------------|--------------|
| Discriminador de Protocolo | Obligatorio | 1 Octeto     |
| Referencia de llamada      | Obligatorio | 3 Octetos    |
| Tipo de Mensaje            | Obligatorio | 1 Octeto     |
| Causa                      | Obligatorio | 2-32 Octetos |

### **Mensaje de LIBERACIÓN**

Éste mensaje es enviado por el usuario o la red para indicar que ha desconectado el enlace de datos y liberará seguidamente el DLCI y la referencia de llamada de la que estaba haciendo uso. El equipo que recibe este mensaje debe liberar el DLCI asociado y prepararse para desocupar la referencia de llamada. Esto ocurrirá justo después de enviar el mensaje de LIBERACIÓN COMPLETA como respuesta. La estructura, de acuerdo a los elementos de información que tiene este mensaje, se muestra en la siguiente tabla:

*Tabla 2.12. Elementos de información que componen el mensaje de LIBERACIÓN.*

| Elemento de Información    | Tipo        | Longitud     |
|----------------------------|-------------|--------------|
| Discriminador de Protocolo | Obligatorio | 1 Octeto     |
| Referencia de llamada      | Obligatorio | 3 Octetos    |
| Tipo de Mensaje            | Obligatorio | 1 Octeto     |
| Causa                      | Opcional    | 2-32 Octetos |

---

El mensaje de liberación tiene significado local. Sin embargo, puede ser de carácter global cuando se utilice como el primer mensaje de liberación del circuito virtual. De cualquier modo, puede ser transmitido en ambos sentidos. El elemento de información que indica la causa de liberación no es incluido necesariamente, pues el motivo ya ha sido especificado en el mensaje de desconexión que le precede.

### ***Mensaje de LIBERACIÓN COMPLETA***

Éste mensaje es enviado por la red o el usuario para indicar que el dispositivo que lo envía ha liberado la referencia de llamada. Tiene significado local y puede ser transmitido en ambos sentidos dentro de una interfaz. Los elementos de información que componen al mensaje de LIBERACIÓN COMPLETA son los mismos que para el mensaje de liberación (Ver Tabla 2.12). Este mensaje sirve como reconocimiento de que la conexión se ha liberado completamente.

### ***Mensajes de CONSULTA de ESTADO y ESTADO***

El formato de éstos mensajes así como también su utilidad, es equivalente a la de los mensajes que se emplean en la gestión de los PVCs. La diferencia es que se transmiten por el canal de señalización con el DLCI 0 en lugar de 1023 y la Referencia de Llamada no es ficticia. Adicionalmente, pueden ser transmitidos en cualquier momento por la red o el usuario. Los mensajes de consulta son para averiguar el estado de la conexión. Los de ESTADO pueden ser enviados en cualquier momento durante una llamada para reportar condiciones de operación extraordinarias o en respuesta a un mensaje de consulta. Los elementos de información que están contenidos en estos mensajes se muestran en las tablas 2.13 y 2.14.

*Tabla 2.13.. Elementos de Información que componen al mensaje de CONSULTA de ESTADO.*

| <b>Elemento de Información</b> | <b>Tipo</b> | <b>Longitud</b> |
|--------------------------------|-------------|-----------------|
| Discriminador de Protocolo     | Obligatorio | 1 Octeto        |
| Referencia de llamada          | Obligatorio | 3 Octetos       |
| Tipo de Mensaje                | Obligatorio | 1 Octeto        |

---

Tabla 2.14. Elementos de información que componen el mensaje de ESTADO.

| Elemento de Información    | Tipo        | Longitud     |
|----------------------------|-------------|--------------|
| Discriminador de Protocolo | Obligatorio | 1 Octeto     |
| Referencia de llamada      | Obligatorio | 3 Octetos    |
| Tipo de Mensaje            | Obligatorio | 1 Octeto     |
| Causa                      | Obligatorio | 4-32 Octetos |
| Estado de la Llamada       | Obligatorio | 3 Octetos    |

### **Mensajes de RESTABLECIMIENTO y CONFIRMACIÓN de RESTABLECIMIENTO**

Estos mensajes sólo son implementados en la interfaz NNI para recuperarse de un estado de falla o bien en una reiniciación del sistema. En la interfaz UNI solo son aplicables cuando el acceso a una red Frame Relay es a través de la ISDN. Como resultado de los procedimientos de restablecimiento, todos los SVCs quedan liberados y en estado nulo. El mensaje de RESTABLECIMIENTO sirve para iniciar el proceso, y el de CONFIRMACIÓN de RESTABLECIMIENTO para aceptar la reiniciación. Aparte de los elementos de información obligatorios, el mensaje de RESTABLECIMIENTO cuenta con un indicador que avisa a los dispositivos que reciben el mensaje, que un procedimiento de restablecimiento será iniciado.

#### **▪ Descripción de los Elementos de Información**

En esta sección se dará una breve descripción de la utilidad de los elementos de información más importantes. No se considera necesario mostrar la codificación de cada uno de ellos. Para encontrar más detalles se pueden consultar los documentos Q.933 y X.76 (Sección 10) de la UIT-T.

#### **Elementos de Información Obligatorios**

Los elementos de información Discriminador de Protocolo, Referencia de la Llamada y Tipo de Mensaje deben estar presentes en todos los mensajes involucrados con los procedimientos de gestión de los SVCs. El Discriminador de Protocolo tiene un valor prefijado cuya secuencia binaria es: 0000 1000 y constituye la primera parte de cada mensaje. La referencia de llamada es un identificador local utilizado para distinguir entre las diferentes llamadas que existen dentro de una interfaz. La codificación se muestra en la figura 2.18. La bandera tiene como finalidad identificar quién originó la

referencia de llamada. El lado de origen la colocará siempre en cero y el sendero la colocará siempre en uno.

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |   |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   | 0 |   |   |   | 0 |
| 0 |   |   |   |   |   |   |   |   |

*Figura 2.18 Estructura del elemento de información referencia de llamada.*

El elemento de información Tipo de Mensaje tiene como finalidad identificar la función del mensaje que está siendo enviado. Existen, de acuerdo a la tabla 2.15, 10 mensajes posibles. Su codificación se muestra en la figura 2.19.

*Tabla 2.15 Codificaciones posibles del elemento de información tipo de mensaje*

| Mensaje                          | Codificación |
|----------------------------------|--------------|
| Establecimiento                  | 000 00101    |
| Conexión                         | 000 00111    |
| Llamada en Curso                 | 000 00010    |
| Desconexión                      | 010 00101    |
| Liberación                       | 010 01101    |
| Liberación Completa              | 010 11010    |
| Situación                        | 011 11101    |
| Consulta de Situación            | 011 10101    |
| Restablecimiento                 | 010 00110    |
| Confirmación de Restablecimiento | 010 01110    |

|   |                 |   |   |   |   |   |   |   |
|---|-----------------|---|---|---|---|---|---|---|
| 8 | 7               | 6 | 5 | 4 | 3 | 2 | 1 |   |
| 0 | Tipo de Mensaje |   |   |   |   |   |   | 1 |

*Figura 2.19. Estructura del elemento de información tipo de mensaje*

### **Elemento de Información Capacidad de Portadora**

El elemento de información capacidad de portadora es obligatorio en el primer mensaje de establecimiento y sirve para identificar el servicio que, de acuerdo a la recomendación I.233, prestará la red. Por ejemplo, especifica que el protocolo de transporte de tramas será el descrito en el anexo A de la recomendación Q.922. En

---

realidad, todos los campos tienen un valor predeterminado pues un solo servicio puede ser ofrecido en Frame Relay. Pero se utiliza para tener consistencia con las especificaciones de la ISDN.

### ***Elemento de Información Estado de la Llamada***

El elemento de información estado de la llamada es usado en los mensajes de SITUACIÓN y sirven para reportar en que fase se encuentra una llamada dentro de la interfaz. Puede reportar llamadas en proceso de establecimiento, activas, en proceso de liberación, etc.

### ***Elementos de Información Números y Subdirecciones del Usuario Llamante y Llamado***

El número del usuario llamado es usado para indicar la dirección del usuario con el que se solicita la conexión. El formato de este elemento de información se muestra en la figura 2.20. Dentro de la codificación, existe un campo que identifica el plan de numeración utilizado (X.121 o E.164) y otro que indica si es un número nacional, internacional, de carácter local, etc. El elemento de información que indica el número del usuario que solicita la llamada tiene un formato muy similar.

|                                           |                |   |   |                                       |   |   |   |   |
|-------------------------------------------|----------------|---|---|---------------------------------------|---|---|---|---|
| 8                                         | 7              | 6 | 5 | 4                                     | 3 | 2 | 1 |   |
| 0                                         | 1              | 1 | 1 | 0                                     | 0 | 0 | 0 | 1 |
| Identificador del Elemento de Información |                |   |   |                                       |   |   |   |   |
| Longitud del Elemento de Información      |                |   |   |                                       |   |   |   | 2 |
| 1                                         | Tipo de Número |   |   | Identificación del Plan de Numeración |   |   |   | 3 |
| 0                                         | Digitos        |   |   |                                       |   |   |   | 4 |

*Figura 2.20. Estructura del elemento de información número de usuario llamado*

Los elementos de información que describen las subdirecciones de los usuarios involucrados en la comunicación, son sólo incluidos en el mensaje de ESTABLECIMIENTO cuando el usuario desea llamar a un destino que posee una subdirección y la especifica en el mensaje.

### ***Elemento de Información Causa***

El elemento de información denominado causa, es el que proporciona información acerca del motivo por el cual una conexión será liberada. Una gama completo de opciones se especifican en la recomendaciones Q.933 y X.76 respectivamente. El formato que posee este elemento de información se muestra en la figura 2.21. Existe un

campo que indica el lugar donde ocurrió el hecho que originó la liberación de la llamada.

|                                           |                   |   |     |           |   |   |   |   |
|-------------------------------------------|-------------------|---|-----|-----------|---|---|---|---|
| 8                                         | 7                 | 6 | 5   | 4         | 3 | 2 | 1 |   |
| 0                                         | 0                 | 0 | 1   | 1         | 0 | 0 | 1 | 1 |
| Identificador del Elemento de Información |                   |   |     |           |   |   |   |   |
| Longitud del Elemento de Información      |                   |   |     |           |   |   |   | 2 |
| 0/1                                       | 0                 | 0 | Res | Ubicación |   |   |   | 3 |
| 1                                         | Valor de la Causa |   |     |           |   |   |   | 4 |

Figura 2.21. Formato del elemento de información causa.

### **Elemento de Información Identificador de Conexión de Enlace de Datos**

El elemento de información identificador de conexión de enlace de datos está siempre incluido en el mensaje de establecimiento en la dirección red – usuario y en la respuesta a una solicitud de conexión por parte del usuario de origen. Opcionalmente, puede ser incluido en la dirección inversa cuando el usuario especifica un DLCI de preferencia. Su codificación se muestra en la figura 2.22.

|                                           |            |            |   |   |            |   |   |   |
|-------------------------------------------|------------|------------|---|---|------------|---|---|---|
| 8                                         | 7          | 6          | 5 | 4 | 3          | 2 | 1 |   |
| 0                                         | 0          | 0          | 1 | 1 | 0          | 0 | 1 | 1 |
| Identificador del Elemento de Información |            |            |   |   |            |   |   |   |
| Longitud del Elemento de Información      |            |            |   |   |            |   |   | 2 |
| 0                                         | 0          | DLCI (msb) |   |   |            |   |   | 3 |
| 1                                         | DLCI (lsb) |            |   |   | Reservados |   |   | 4 |

Figura 2.22. Estructura del elemento de información identificador de conexión de enlace de datos

### **Elemento de Información Parámetros de Núcleo de Capa de Enlace de Datos**

El elemento de información parámetros de núcleo de capa de enlace de datos, es quizás el más importante dentro del establecimiento de un circuito virtual conmutado. Este especifica la calidad de servicio que será ofrecida en la comunicación. Su estructura se muestra en la figura 2.23. Cada campo tiene un identificador y en cada uno de ellos se indican los parámetros de entrada y de salida. Si el circuito virtual es simétrico, estos son equivalentes y solo se especifican en un sentido. Los parámetros de calidad de servicio que se definen en este elemento de información son el CIR, el Bc y el Be, y son negociados entre el usuario y la red antes de comenzar con la transferencia de información. Para el caso del CIR, se especifica un valor deseable y uno mínimo aceptable, que si la red no es capaz de proporcionar, no establecerá el circuito virtual. Se

expresa como un orden de magnitud (en potencias de 10) y un multiplicador entero. Por ejemplo una velocidad de 256Kbps, se representa como  $256 \times 10^3$ .

Cuando el circuito virtual es simétrico, no es necesario especificar los parámetros de entrada y salida. Los octavos bits de cada octeto indican si el campo termina o se especificarán los parámetros en ambos sentidos. Se puede observar que con las detalles proporcionadas por éste elemento de información, quedan determinados los demás parámetros que definen la calidad de servicio.

Cuando el elemento de información parámetro de núcleo de capa de enlace de datos está presente en un mensaje de ESTABLECIMIENTO, indica los parámetros solicitados. Cuando está contenido en un mensaje de CONEXIÓN, especifica los parámetros acordados para la comunicación. Si el usuario no incluye este elemento de información en su solicitud de conexión, la red tomará los valores que tenga configurados por defecto.

|                                                                        |                                                                 |   |   |   |                          |   |   |
|------------------------------------------------------------------------|-----------------------------------------------------------------|---|---|---|--------------------------|---|---|
| 0                                                                      | 1                                                               | 0 | 0 | 1 | 0                        | 0 | 0 |
| Identificador del Elemento de Información Parámetros de Capa de Enlace |                                                                 |   |   |   |                          |   |   |
| Longitud del Contenido del Elemento de Información                     |                                                                 |   |   |   |                          |   |   |
| 0                                                                      | 0                                                               | 0 | 0 | 1 | 0                        | 0 | 1 |
| Tamaño máximo del campo de información de la Trama                     |                                                                 |   |   |   |                          |   |   |
| 0                                                                      | Longitud Máxima del Campo de Información de la Trama de salida  |   |   |   |                          |   |   |
| 0/1                                                                    | Continuación                                                    |   |   |   |                          |   |   |
| 0                                                                      | Longitud Máxima del Campo de Información de la Trama de entrada |   |   |   |                          |   |   |
| 1                                                                      | Continuación                                                    |   |   |   |                          |   |   |
| 0                                                                      | 0                                                               | 0 | 0 | 1 | 0                        | 1 | 0 |
| Caudal (CIR)                                                           |                                                                 |   |   |   |                          |   |   |
| 0                                                                      | Magnitud del caudal de salida                                   |   |   |   | Multiplicador de Salida  |   |   |
| 0/1                                                                    | Multiplicador de salida (cont.)                                 |   |   |   |                          |   |   |
| 0                                                                      | Magnitud de Caudal de Entrada                                   |   |   |   | Multiplicador de Entrada |   |   |
| 1                                                                      | Multiplicador de entrada (cont.)                                |   |   |   |                          |   |   |
| 0                                                                      | 0                                                               | 0 | 0 | 1 | 0                        | 1 | 1 |
| Caudal mínimo aceptable                                                |                                                                 |   |   |   |                          |   |   |
| 0                                                                      | Magnitud de caudal mínimo de salida                             |   |   |   | Multiplicador de salida  |   |   |
| 0/1                                                                    | Multiplicador de salida (cont.)                                 |   |   |   |                          |   |   |
| 0                                                                      | Magnitud de caudal mínimo de entrada                            |   |   |   | Multiplicador de entrada |   |   |
| 1                                                                      | Multiplicador de entrada (cont.)                                |   |   |   |                          |   |   |
| 0                                                                      | 0                                                               | 0 | 0 | 1 | 1                        | 0 | 1 |
| Tamaño de ráfaga comprometido (Bc).                                    |                                                                 |   |   |   |                          |   |   |
| 0                                                                      | Valor del tamaño de ráfaga comprometido de salida               |   |   |   |                          |   |   |
| 0/1                                                                    | Continuación                                                    |   |   |   |                          |   |   |
| 0                                                                      | Valor del tamaño de ráfaga comprometido de entrada              |   |   |   |                          |   |   |
| 1                                                                      | Continuación                                                    |   |   |   |                          |   |   |
| 0                                                                      | 0                                                               | 0 | 0 | 1 | 1                        | 1 | 0 |
| Tamaño de ráfaga en exceso (Be)                                        |                                                                 |   |   |   |                          |   |   |
| 0                                                                      | Valor del tamaño de ráfaga en exceso de salida                  |   |   |   |                          |   |   |
| 0/1                                                                    | Continuación                                                    |   |   |   |                          |   |   |
| 0                                                                      | Valor del tamaño de ráfaga en exceso de entrada                 |   |   |   |                          |   |   |
| 1                                                                      | Continuación                                                    |   |   |   |                          |   |   |

Figura 2.23. Elemento de información parámetros de núcleo de enlace de datos.

---

## Compatibilidad de Capa Baja

El elemento de información compatibilidad de capa baja, es incluido en la dirección usuario-red, solo cuando el usuario de origen desea pasar esta información hacia el usuario llamado. La gran mayoría de los campos presentes en este elemento de información, tienen valores prefijados.

### ▪ Procedimientos de Establecimiento

Cuando un usuario envía un mensaje de ESTABLECIMIENTO a la red por el DLCI 0, se inicia un temporizador que indicará el tiempo de reenvío de dicho mensaje. Si al segundo intento no se ha recibido una respuesta, se cancela la solicitud. En el caso de la interfaz NNI se debe iniciar un proceso de LIBERACIÓN en la dirección contraria, que especifique la causa por la cual este hecho ha sucedido. En respuesta a un mensaje de ESTABLECIMIENTO, la red retorna opcionalmente un mensaje de LLAMADA EN CURSO para indicar que recibió la solicitud y, que el establecimientos de la conexión ha sido iniciado. Al recibir un mensaje de LLAMADA EN CURSO, se debe anular el temporizador y comenzar otra cuenta que espere por un mensaje de CONEXIÓN. Cuando el usuario o la red de destino recibe un mensaje de ESTABLECIMIENTO, debe determinar cuales de las solicitudes puede garantizar y, en el caso de la red, establecer una ruta disponible hacia el usuario llamado. En este momento se envía un mensaje de LLAMADA EN CURSO. Si se satisfacen los valores mínimos aceptables especificados en la solicitud, se devuelve un mensaje de CONEXIÓN. De manera muy general, este proceso se describe en la figura 2.24.

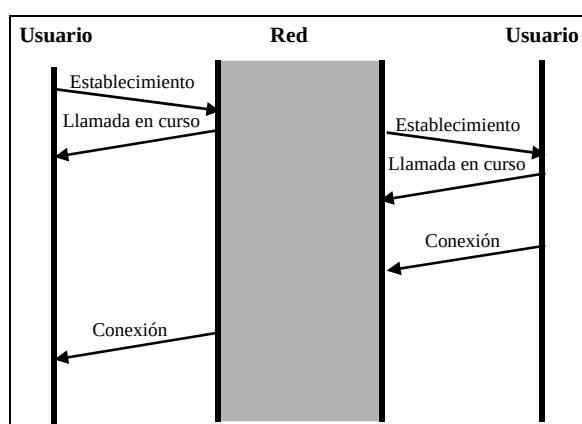


*Figura 2.24. Proceso de establecimiento del circuito virtual.*

En la interfaz UNI, según el Frame Relay Forum en su acuerdo de implementación FRF.4, la inclusión del elemento de información identificador de enlace de datos no

---

debe ser incluido dentro del mensaje de ESTABLECIMIENTO (en el sentido usuario – red). La red colocará uno que esté disponible. Si la red no está en capacidad de proporcionar un DLCI, debe enviar un mensaje de liberación completa que especifique que no hay canal disponible. En la interfaz NNI, este elemento de información debe ser incluido. Si el DLCI indicado está disponible en la interfaz, la red reserva ese DLCI para la llamada. En cualquiera de los casos, los DLCI seleccionados se especifican en el primer mensaje de respuesta a los mensajes de ESTABLECIMIENTO.

Los parámetros de calidad de servicio son negociados durante el establecimiento de la llamada. En base a ellos, la red y el usuario llamado tomarán decisiones en cuanto a: rechazar la trama si los requisitos más bajos aceptables no pueden satisfacerse con los recursos disponibles, continuar el proceso de establecimiento con los parámetros especificados o ajustarlos según la disponibilidad. La especificación del parámetro en el elemento de información es opcional y si no se incluye, se supone el valor por defecto. Después de haber establecido cual es la calidad de servicio que se puede brindar, se devuelve el mensaje de CONEXIÓN con los parámetros acordados.

#### ▪ **Procedimientos de Liberación**

La fase de liberación de la llamada es usada para eliminar un circuito virtual conmutado previamente establecido. Este proceso puede ser iniciado por la red o los usuarios involucrados. En el caso de que sea el usuario el que solicite la liberación, enviará un mensaje de DESCONEXIÓN hacia la red, momento en el cual desconectará<sup>12</sup> el DLCI asociado. Al recibir un mensaje de DESCONEXIÓN, la red también desconectará el DLCI y propagará el mensaje a lo largo del circuito virtual. Cuando un usuario recibe un mensaje de DESCONEXIÓN, desconectará el DLCI y como respuesta enviará un mensaje de LIBERACIÓN hacia la red. Este será propagado hacia el usuario que solicitó la liberación, y en la ruta serán liberados todas las referencias de llamadas y los DLCI<sup>13</sup> involucrados. Por último, un mensaje de LIBERACIÓN COMPLETA será enviado como confirmación de que el proceso ha finalizado. Esta situación se representa en la figura 2.25.

De la misma forma que en los procedimientos de establecimiento, cuando se solicita la liberación de una conexión virtual se inicia un temporizador que puede expirar dos

---

<sup>12</sup> Un DLCI está desconectado cuando no se utiliza en una conexión, pero aún no está disponible para ser reasignado.

<sup>13</sup> Un DLCI está liberado cuando está disponible para ser reasignado.

veces. Después de esto el dispositivo debe liberar la referencia de llamada y el DLCI asociado.

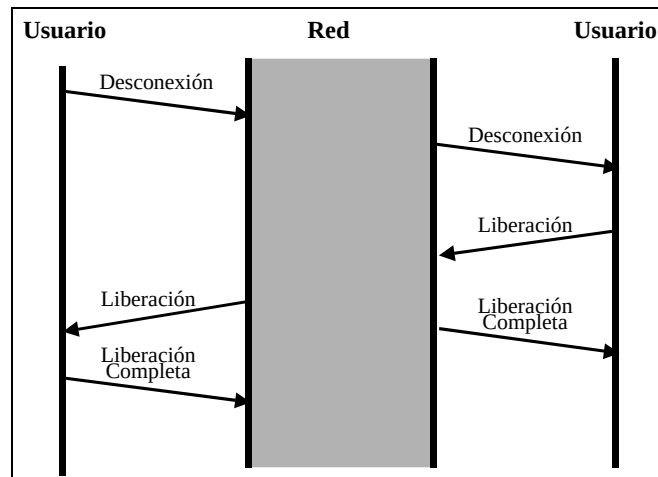


Figura 2.25. Proceso de liberación del SVC.

#### ▪ Manejo de las Condiciones de Error

El manejo de errores depende de cada implementación. Las condiciones de error más relevantes así como las acciones a tomar se presentan a continuación<sup>14</sup>:

1. En los casos en los que se recibe un mensaje cuyo discriminador de protocolo no coincide con la codificación establecida, cuando un mensaje no tiene todos los elementos de información obligatorios (Discriminador de protocolo, referencia de llamada y tipo de mensaje), o cuando se recibe una referencia de llamada con formato inválido, el mensaje debe ser ignorado.
2. Si un mensaje posee una referencia de llamada especificando un SVC que no está activo, se debe iniciar un proceso de liberación (se exceptúan los mensajes de ESTABLECIMIENTO, LIBERACIÓN COMPLETA, SITUACIÓN y CONSULTA DE SITUACIÓN). De la misma forma, en los casos en los que una mensaje de ESTABLECIMIENTO contiene una referencia de llamada que está en uso, el mensaje debe ser ignorado.
3. Cuando se recibe un elemento de información que no contiene la cantidad de campos preestablecida o su longitud no es correcta. Si el elemento de información

<sup>14</sup> Las acciones aquí descritas no son de carácter obligatorio.

---

no es obligatorio, el receptor puede ignorarlo y continuar el proceso. Cuando por el contrario sobrepasa la extensión predefinida, el receptor puede tomar en cuenta sólo el contenido correcto del elemento de información e ignorar el resto.

4. Al recibir elementos de información duplicados, sólo el contenido del primer elemento de información debe ser considerado.
5. Si un mensaje de LIBERACIÓN COMPLETA es recibido inesperadamente, se deben liberar la referencia de llamada, el DLCI asociado y regresar al estado Nulo. Cuando se recibe cualquier otro mensaje que no coincide con la secuencia esperada, se debe retornar un mensaje de SITUACIÓN indicando que el mensaje recibido no corresponde con el estado de la llamada. Alternativamente puede ser enviado también un mensaje de CONSULTA de SITUACIÓN.
6. Cuando se reciben mensajes de ESTABLECIMIENTO o LIBERACIÓN con más de un elemento de información obligatorio omitido o inválido, se debe liberar el circuito virtual asociado. Cuando se trata de otros mensajes, no deben tomarse acciones sino enviar un mensaje de SITUACIÓN.
7. Si los elementos de información LIBERACIÓN o LIBERACIÓN COMPLETA se reciben con el elemento de información que indica la causa de inválido, debe asumirse como un proceso de liberación normal. En el caso particular del mensaje de LIBERACIÓN, la confirmación de respuesta debe ser retornada indicando que se recibió una causa inválida.
8. Si se encuentran uno o más elementos de información no obligatorios dentro de un mensaje con contenido inválido, se deben tomar las acciones correspondientes de acuerdo a los elementos de información valederos. Adicionalmente, un mensaje de SITUACIÓN debe ser retornado. Los mismos procedimientos se siguen cuando se reciben elementos de información que no corresponden al mensaje.

En general, la gran mayoría de las condiciones de error son manejadas de acuerdo a la importancia del mensaje y del carácter (opcional u obligatorio) del elemento de información. Cuando se trata de fallas significativas en aquellos mensajes que implican el establecimiento o liberación de un circuito, el canal virtual es liberado. Para el resto de los mensajes se ignoran las fallas y se envían alternativamente mensajes de CONSULTA de SITUACIÓN o SITUACIÓN para verificar el estado del enlace.

### **Redes Privadas Virtuales (VPN) y Firewall**

#### **Introducción**

Hasta no hace mucho tiempo, las diferentes sucursales de una empresa podían tener, cada una, una red local a la sucursal que operara aislada de las demás. Cada una de estas redes locales tenía su propio esquema de nombres, su propio sistema de e-mail, e inclusive usar protocolos que difieran de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa.

A medida que la computadora fue siendo incorporada a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia. Es por eso que escuchamos hablar tanto de los famosos firewalls y las VPN.

#### **¿Qué es una Red Privada Virtual (VPN)?**

El término VPN se refiere a una Red Privada Virtual (Virtual Private Network), la cual utiliza infraestructuras públicas como mecanismo de transporte, manteniendo la seguridad de los datos en la VPN.

Es una red privada que se extiende (mediante un proceso de encapsulación y encriptación de los paquetes de datos) a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

La configuración más común de VPN es a través de una red interna principal y nodos remotos usando VPN para lograr el acceso completo a la red central. Los nodos remotos son comúnmente oficinas remotas o empleados trabajando en casa. También pueden vincularse dos redes más pequeñas para conformar una red simple, incluso más grande. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. (Ver figura siguiente)

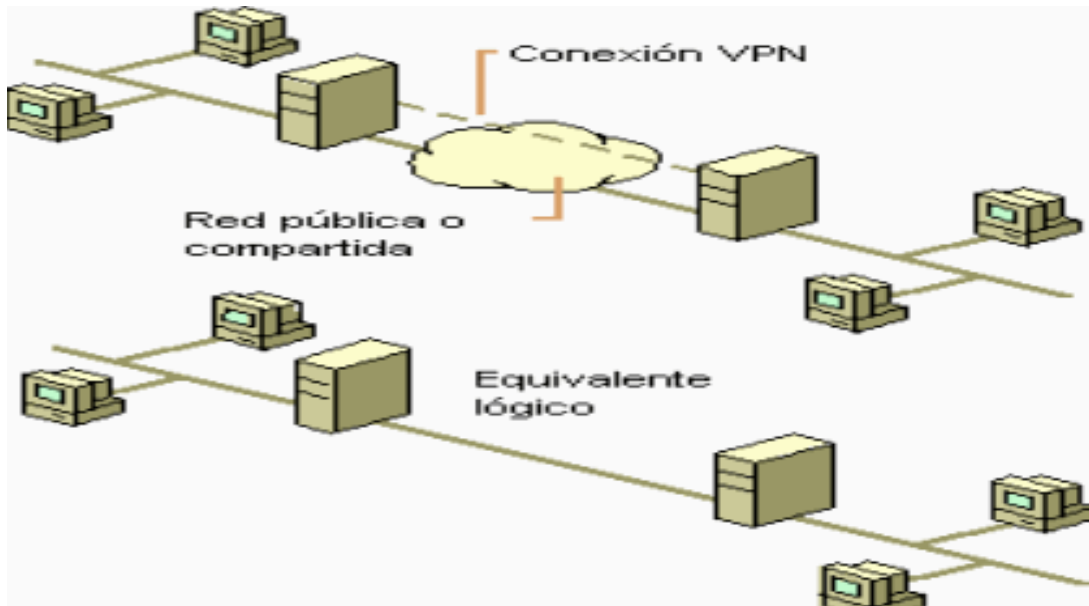


*Figura 3.1. Red Privada Virtual (VPN).*

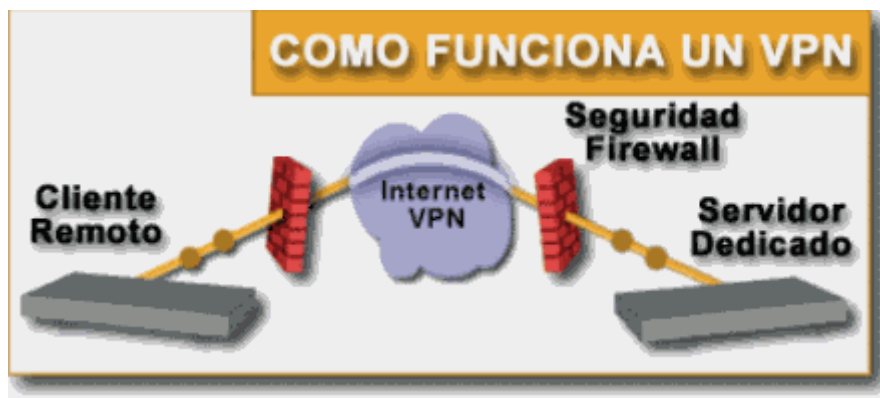


*Figura 3.2. Funcionamiento de una VPN*

En la figura anterior (figura 3.2) se muestra cómo viajan los datos a través de una VPN, la forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autenticación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública. Como se usan redes

---

públicas, en general Internet, es necesario prestar debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autenticación.

Las VPN pueden enlazar las oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como Internet, IP, IPSec, Frame Relay, ATM como lo muestra la figura siguiente.

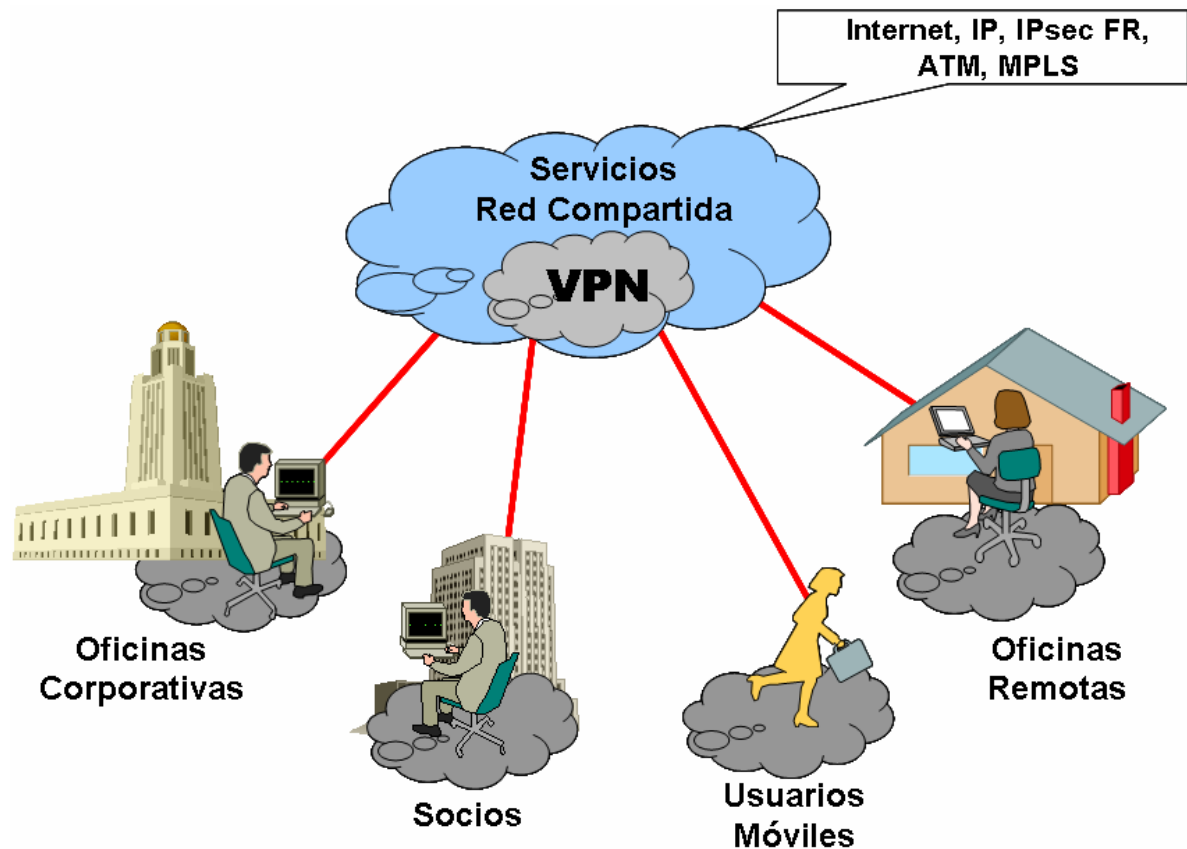


*Figura 3.3. Protocolos utilizados*

## **Tecnología de túnel**

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos y esto se le conoce como encapsulación. Además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

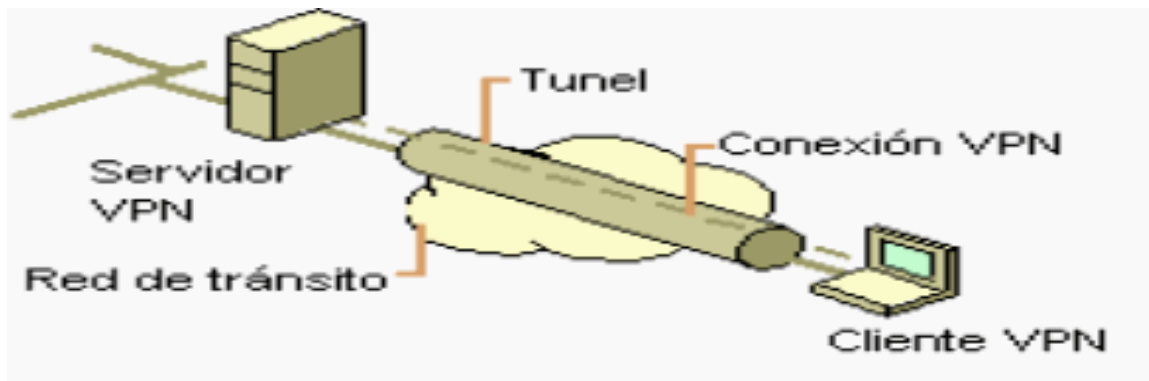


*Figura 3.4. Tecnología de túnel.*

El servidor busca mediante un enrutador la dirección IP del cliente VPN y en la red de tránsito se envían los datos sin problemas.

### **Protocolos utilizados en las VPNs**

#### **▪ PPTP**

Point-to-Point Tunneling Protocol fue desarrollado por los ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser enrutado a través de una red IP, como Internet.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si estuvieran físicamente conectados directamente al servidor.

Existen dos escenarios comunes para este tipo de VPN:

- el usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.
- el usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto establece una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el segundo

---

escenario, el usuario remoto se conecta al ISP mediante PPP y luego “llama” al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, no necesita conexión alguna y se realiza directamente sobre IP. Se utiliza entre otros para encapsular tramas de protocolo de nivel superior.

El paquete PPTP está compuesto por un header de envío, un header IP, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, Frame Relay, PPP. El header IP contiene información relativa al paquete IP, como direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. La siguiente figura ilustra las capas del encapsulamiento PPTP.

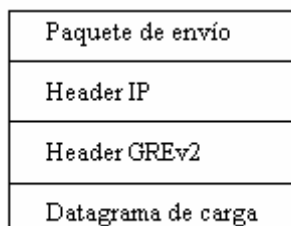


*Figura 3.5. Capas del encapsulamiento PPTP*

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, standard en el que se intercambia un “secreto” y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows 2000, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un standard propietario de Microsoft y resulta

---

ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Authentication Protocol), que no encripta las contraseñas. Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

▪ **IPSec (IP Seguro, descrito en el RFC 2411)**

IPSec trata de remediar algunas carencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP.

Protocolo que sirve para establecer una sesión segura entre dos hosts que se comuniquen a través de IP, proporcionando encriptación a nivel de la capa de red.

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

- Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.
- Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.
- Por autenticidad se entiende por la validación de remitente de los datos.
- Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

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

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

AH sigue al header IP y contiene disseminaciones criptográficas tanto en los datos como en la información de identificación. Las disseminaciones pueden también cubrir las partes invariantes del header IP.

El header de ESP permite describir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

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

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

El protocolo IPSec cubre las siguientes cuestiones de seguridad principales:

- *Autenticación de origen de datos:* Verifica que cada datagrama ha sido originado por el remitente indicado.
- *Integridad de datos:* Verifica que el contenido de un datagrama no se ha cambiado por el camino, ni deliberadamente ni debido a errores aleatorios.
- *Confidencialidad de datos:* Oculta el contenido de un mensaje, normalmente mediante cifrado.
- *Protección de reproducción:* Impide que un agresor pueda interceptar un datagrama y reproducirlo posteriormente.
- *Gestión automatizada de claves criptográficas y asociaciones de seguridad:* Permite implementar la política VPN en toda la red con poca o ninguna configuración manual.

#### ▪ **L2TP**

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

El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local, es el que se muestra en la siguiente figura:

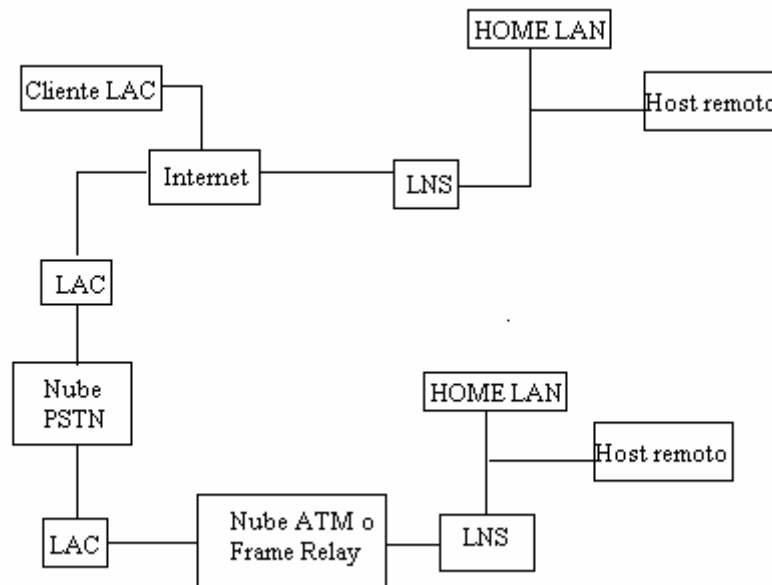


*Figura 3.6. Escenario típico L2TP.*

Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el Home LAN's Management Domain.

L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

La siguiente figura muestra la relación entre las tramas PPP y los mensajes de control a través de los canales de control y datos de L2TP.

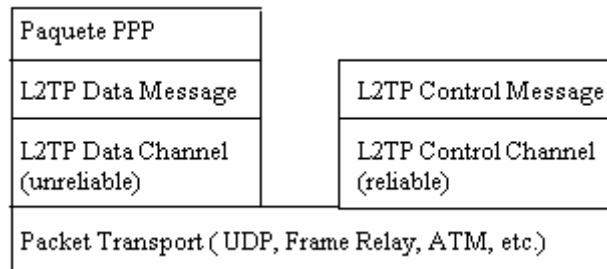


*Figura 3.7. Relación entre los marcos PPP y los mensajes de control.*

Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autenticación de L2TP, tanto el LAC como el LNS comparten un secreto único. Cada extremo usa este mismo secreto al actuar tanto como autenticado como autenticador.

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.

---

## Categorías de VPN

Las VPN pueden dividirse en tres categorías, a saber:

- **VPN de Acceso Remoto:**

Conectan usuarios móviles con mínimo tráfico a la red corporativa. Proporcionan acceso desde una red pública, con las mismas políticas de la red privada. Los accesos pueden ser tanto sobre líneas analógicas, digitales, RDSI o DSL.

- **VPN de Intranet:**

Permite conectar localidades fijas a la red corporativa usando conexiones dedicadas.

- **VPN de Extranet:**

Proporciona acceso limitado a los recursos de la corporación a sus aliados comerciales externos como proveedores y clientes, facilitando el acceso a la información de uso común para todos a través de una estructura de comunicación pública.

## Requerimientos básicos de una VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

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

### **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.

### **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.

### **Encriptación 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.

---

**Administración de claves:**

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

**Soporte a protocolos múltiples:**

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

**Controles y riesgos asociados a la tecnología VPN**

Cuando se desea implantar una VPN se debe estar consciente de las ventajas que va a aportar a la organización, sin embargo, es importante considerar los riesgos que estas facilidades implican en caso de no adoptarse las medidas necesarias al implantar una VPN “segura”. Los estándares utilizados para la implementación de VPNs, garantizan la privacidad e integridad de los datos y permiten la autenticación de los extremos de la comunicación, pero esto no es suficiente: el uso erróneo de las VPN puede ser catastrófico para el negocio.

Las medidas para implantar una VPN “segura” incluyen el uso de certificados digitales para la autenticación de equipos VPN, token cards o tarjetas inteligentes para la autenticación “fuerte” de usuarios remotos, y para el control de acceso es importante contar con un Firewall y sistemas de autorización.

**▪ Certificados digitales:**

Con el uso de certificados digitales, se garantiza la autenticación de los elementos remotos que generan el túnel y elimina el problema de la distribución de claves. Implantar un sistema PKI (Infraestructura de Clave Pública) para emitir los certificados digitales, permite tener el control absoluto de la emisión, renovación y revocación de los certificados digitales usados en la VPN. El uso de PKI no se limita sólo a las VPNs sino que puede utilizarse para aplicaciones como firmas digitales, cifrado de correo electrónico, entre otras.

**▪ Autenticación fuerte:**

En la implantación de una VPN se debe verificar que se estén realmente autenticando los usuarios. Esto dependerá de dónde se almacene el certificado digital y la clave privada. Si el certificado digital y la clave privada se almacenan, protegidos por un PIN, en una tarjeta inteligente que el usuario lleva consigo, se está autenticando al usuario. Desafortunadamente, aun no existe un estándar definido que permita la implantación a gran escala de lectores de tarjetas en los PCs. Por lo que esta opción en algunos casos

---

no es factible. Si, por el contrario, el certificado digital y la clave privada se almacenan en el propio PC, no se está autenticando al usuario sino al PC. Para autenticar al usuario, algunos fabricantes de sistemas VPN han añadido un segundo nivel de autenticación. El uso de contraseñas es un nivel adicional de seguridad, pero no es el más adecuado, ya que carecen de los niveles de seguridad necesarios debido a que son fácilmente reproducibles, pueden ser capturadas y realmente no autentican a la persona. El método más adecuado es autenticar a los usuarios remotos mediante un la utilización de sistemas de autenticación fuerte. Estos sistemas se basan en la combinación de dos factores: el token y el PIN. De esta forma se asegura que sólo los usuarios autorizados acceden a la VPN de la organización.

▪ **Firewall y Sistemas de Autorización:**

El control de acceso se puede realizar utilizando Firewalls y sistemas de autorización; de esta manera se aplican políticas de acceso a determinados sistemas y aplicaciones de acuerdo al tipo de usuarios o grupos de usuarios que los acceden.

### **Ventajas de una VPN**

Dentro de las ventajas más significativas podremos mencionar:

- La integridad, confidencialidad y seguridad de los datos.
- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows.
- Control de acceso basado en políticas de la organización
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC's remotas.

### **Protegiendo la red: VPN y Firewall**

La mayoría de las organizaciones hoy día protegen sus instalaciones mediante firewalls. Estos dispositivos deben configurarse para que permitan pasar el tráfico VPN. En la Figura 3.7 se muestra la configuración típica, donde el servidor VPN está colocado detrás del firewall, en la zona desmilitarizada (DMZ) o en la propia red interna.

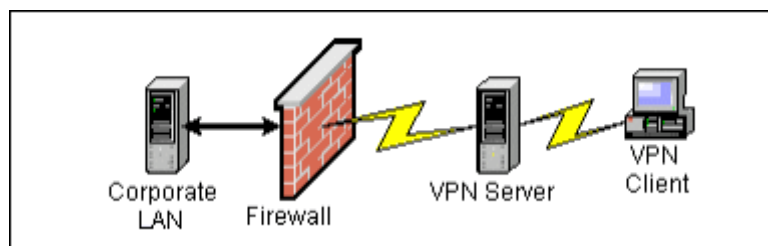


*Figura 3.8. Firewall y servidor VPN en dispositivos separados*

En la práctica, muchos firewalls incorporan un servidor VPN (Ver Figura 3.9). Las reglas del firewall deben permitir el tráfico PPTP, L2TP e IPSec en base a los puertos utilizados.

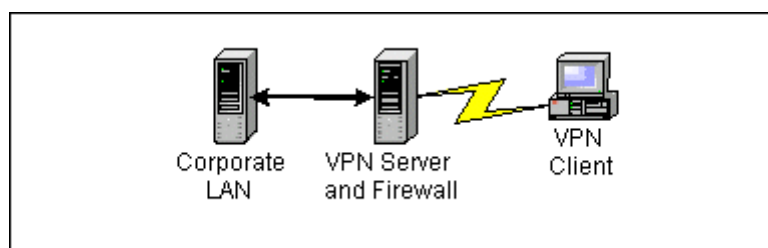


*Figura 3.9. Firewall y servidor VPN incorporados en un mismo dispositivo*

## **El Firewall ó Cortafuego**

Un firewall es un sistema que permite ejercer políticas de control de acceso entre dos redes, tales como una red LAN privada e Internet, una red pública y vulnerable. El firewall define los servicios que pueden accederse desde el exterior y viceversa. Los medios a través de los cuales se logra esta función varían notoriamente, pero en principio, un firewall puede considerarse como: un mecanismo para bloquear el tráfico y otro para permitirlo.

Un firewall constituye más que una puerta cerrada con llave al frente de una red. Es un servicio de seguridad particular. Los firewalls son también importantes porque proporcionan un único punto de restricción, donde se pueden aplicar políticas de seguridad y auditoria. Un firewall proporciona al administrador de la red, entre otros datos, información acerca del tipo y cantidad de tráfico que ha fluido a través del mismo y cuántas veces se ha intentado violar la seguridad. De manera similar a un sistema de circuito cerrado de TV, un firewall no sólo bloquea el acceso, sino también monitorea a

---

aquellos que están merodeando y le ayuda a identificar los usuarios que han intentado violar su seguridad.

### Funciones Básicas de un Firewall

Un firewall lleva a cabo tres funciones básicas para proteger una red:

- Bloquea los datos entrantes que pueden contener el ataque de un hacker.
- Oculta la información acerca de la red, haciendo que todo parezca como si el tráfico de salida se originara del firewall y no de la red. Esto también se conoce como NAT (*Network Address Translation*).
- Filtra el tráfico de salida, con el fin de restringir el uso de Internet y el acceso a localidades remotas.

En la siguiente figura se puede observar gráficamente la función de bloqueo de los ataques de un hacker.

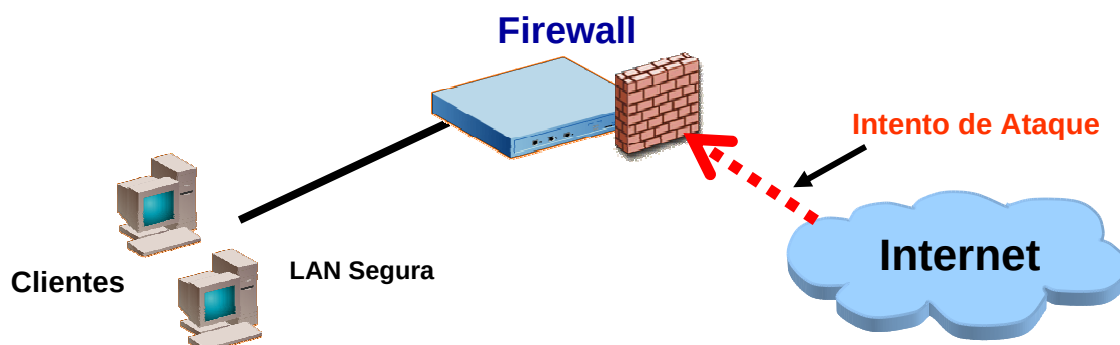


*Figura 3.10. Firewall: Bloqueo de ataques externos.*

### Niveles de Filtrado de un Firewall

Un firewall puede filtrar tanto el tráfico que sale como el que entra. Debido a que el tráfico que entra constituye una amenaza mucho mayor para la red, éste es inspeccionado mucho más estrictamente que el tráfico que sale. Existen básicamente tres tipos de filtrado:

- El filtrado que bloquea cualquier dato de entrada que no haya sido específicamente solicitado por un usuario de la red.
- El filtrado basado en la dirección del remitente.

- 
- El filtrado basado en el contenido de la comunicación.

Los niveles de filtrado se pueden comparar con un proceso de eliminación. El firewall inicialmente determina si la transmisión entrante ha sido solicitada por un usuario de la red y, de no ser así, la rechaza. Luego, cualquier dato que haya sido permitido se inspecciona cuidadosamente. El firewall verifica la dirección de la computadora del remitente, con el fin de certificar que proviene de un sitio confiable. Finalmente, se encarga de verificar el contenido de la transmisión.

## **Tipos de Firewall**

Las funciones de un firewall pueden implementarse ya sea como software o como una adición a un router o gateway.

- **Firewalls basados en Routers / Firmware**

Algunos routers proveen capacidades limitadas de firewall. Estas pueden incrementarse con software u opciones de firmware adicional. No obstante, es importante tener cuidado de no sobrecargar un router con servicios adicionales de firewall. Además, es posible que algunas funciones de firewall, como VPN, DMZ, filtrado de contenido o protección a través de antivirus, no estén disponibles o sean muy costosas de implementar.

- **Firewalls basados en Software**

Por lo general, los firewalls basados en software son aplicaciones sofisticadas y complejas que se ejecutan en servidores dedicados UNIX o 2000. Estos productos se tornan aún más costosos cuando se suman los costos de software, sistema operativo, hardware de servidor y mantenimiento continuo requerido para soportar la implementación. Resulta esencial también que el administrador del sistema monitoree constantemente e instale las actualizaciones más recientes de seguridad y del sistema operativo, tan pronto como se encuentren disponibles. Sin estas actualizaciones que cubren los nuevos peligros de seguridad, el software de firewall puede volverse totalmente inservible.

- **Dispositivos de Firewall dedicados**

La mayoría de los dispositivos de firewall son sistemas de hardware dedicados. Estos dispositivos son menos susceptibles a las fallas de seguridad inherentes de los sistemas operativos Windows 2000 o UNIX, gracias a que integran sistemas operativos desarrollados específicamente para utilizarse como firewall. Estos

---

firewalls de alto rendimiento han sido diseñados para satisfacer los altos requerimientos de rendimiento o del procesador. Debido a que no es necesario fortalecer el sistema operativo, por lo general, los dispositivos de firewall son más fáciles de instalar y configurar que los productos de firewall de software. Estos ofrecen potencialmente un nivel de instalación plug-and-play, requieren mínimo mantenimiento y una solución completa.

## **Ventajas de un Firewall**

A parte de las funciones adicionales de los firewalls, a continuación se mencionan en líneas generales las ventajas de los mismos.

- *Protección de la red:* Mantiene alejados a los crackers (piratas informáticos) de la red al mismo tiempo que permite acceder a todo el personal de la oficina.
- *Control de acceso a los recursos de la red:* Al encargarse de filtrar, en primer nivel antes que lleguen los paquetes al resto de las computadoras de la red, el firewall es idóneo para implementar en él los controles de acceso.
- *Control de uso de Internet:* Permite bloquear el material no adecuado, determinar los sitios que puede visitar el usuario de la red interna y llevar un registro.
- *Concentra la seguridad:* El firewall facilita la labor a los responsables de seguridad, dado que su máxima preocupación es encarar los ataques externos y vigilar, manteniendo un monitoreo.
- *Control y estadísticas:* Permite controlar el uso de Internet en el ámbito interno y conocer los intentos de conexiones desde el exterior y detectar actividades sospechosas.
- *Choke-Point:* Permite al administrador de la red definir un embudo manteniendo al margen los usuarios no autorizados fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques.
- *Genera alarmas de seguridad:* El administrador del firewall puede ser alertado a tiempo de ataques a externos mediante el aviso de alarmas de seguridad.

- 
- *Audita y registra Internet:* Permite al administrador de red justificar el gasto que implica la conexión a Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda.

## **Limitaciones de un Firewall**

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación, en este caso:

- Conexión dial-out sin restricciones que permita entrar a la red protegida; el usuario puede hacer una conexión SLIP o PPP a Internet. Este tipo de conexiones deriva de la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque.
- El firewall no puede protegerse de las amenazas a que está sometido por traidores o usuarios inconscientes.
- El firewall no puede protegerse contra los ataques de ingeniería social, en este caso, un craker que quiera ser un supervisor o aquel que persuade a los usuarios menos sofisticados.
- El firewall no puede protegerse de los ataques posibles a la red interna por virus informáticos a través de archivos y software.
- Tampoco puede protegerse contra los ataques en la transferencia de datos, estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados.

---

## **Capítulo 4**

### ***Infraestructura Actual***

#### **Situación Actual**

En el proceso de transición y entrega del sistema SIGECOF a su ente rector La Oficina Nacional de Contabilidad Pública (ONCOP) del Ministerio de Finanzas, lo concerniente a la plataforma de telecomunicaciones y redes se encontraban en un nivel muy incipiente, hecho que se tradujo en un cronograma de trabajo en equipo, de recurso humano y económico, de logística e inversión, para poder así lograr en el menor tiempo posible la metas exigidas por la ONCOP en esta primera fase de gestión, que se traducía en la interconexión de la Oficina con todos los Organismos Ordenadores de Compromisos y Pagos (OOCOP) de la administración Central.

El desarrollo de la red y las telecomunicaciones de la ONCOP a nivel central, supone en su nivel máximo de ejecución, la utilización de canales de comunicación de banda ancha; a través de los cuales se pueda transmitir datos de alta velocidad.

Los enlaces desde la ONCOP a cada una de estas localidades (OOCOP) se realiza a través de líneas dedicadas y conexiones por Antenas Inalámbricas provistas por diferentes empresas de Telecomunicaciones, específicamente CANTV, a través de la Red WAN del Ministerio de Finanzas y la Red PLATINO.

De aquí la importancia de la continuidad y disponibilidad de los enlaces de comunicación y demás servicios, lo cual aumentará la calidad y la productividad de los procedimientos implicados en el área de negocios de la oficina.

## Plataforma Tecnológica Actual

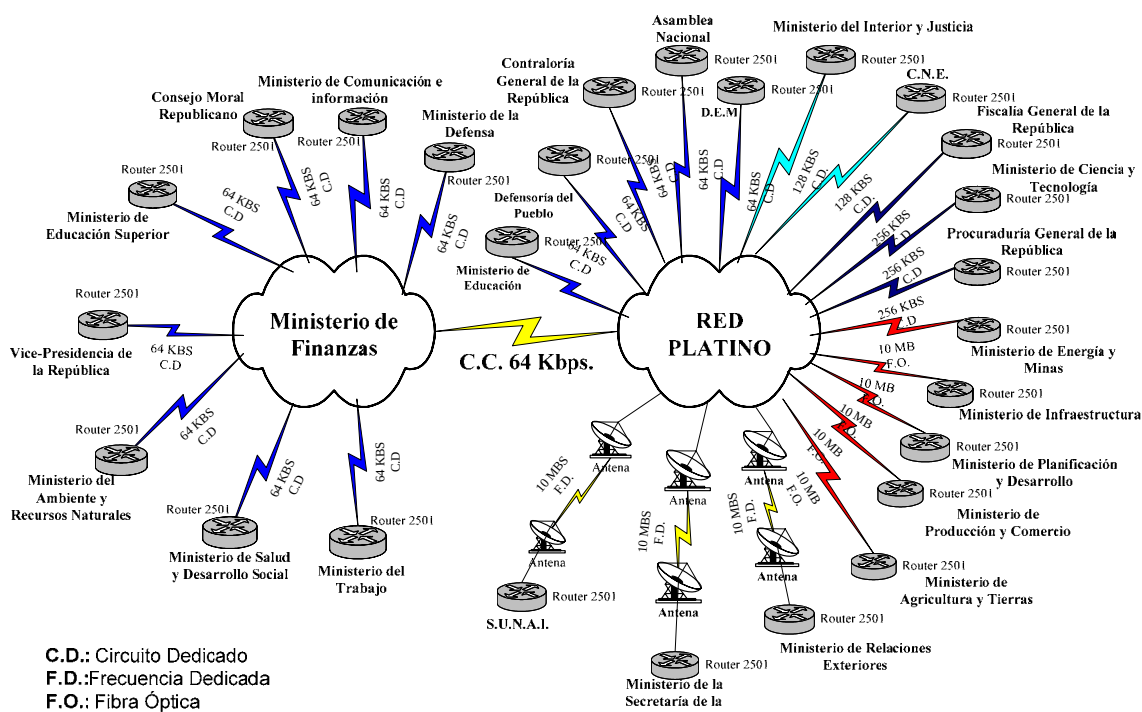
El estudio y análisis que se realizó a la plataforma tecnológica actual, permitió evaluar alternativas que conllevaron a la actualización de la plataforma actual y a reforzar la seguridad de la información para mejorar y brindar una mayor protección a las conexiones remotas y al acceso a la información del sistema SIGECOF.

A continuación se muestra un esquema general de la plataforma tecnológica actual.

*Figura 4.1. Esquema red actual*

**Esquema de Conexión: Plataforma Actual**

**SIGECOF**



---

## Sistema de Acceso al Sigecof

El Sistema de Acceso a cada una de las localidades remotas, donde residen los Servidores de Base de Datos y Aplicaciones del Sistema Integrado de Gestión y Control de las Finanzas Públicas (SIGECOF), se realiza a través de líneas dedicadas y conexiones por Antenas Inalámbricas provistas por diferentes empresas de Telecomunicaciones, específicamente CANTV, a través de la Red WAN del Ministerio de Finanzas y la Red PLATINO.

Las siguientes tablas muestra la distribución de enlaces SIGECOF, entre las diferentes redes.

*Tabla 4.1. Distribución de enlaces Sigecof conectados por la red de Finanzas*

| N ° | Localidades del Proyecto: OOCF               | Tipo de Enlace |
|-----|----------------------------------------------|----------------|
| 1   | Ministerio del Trabajo                       | Dedicado 64 K  |
| 2   | Ministerio de Salud y Desarrollo Social      | Dedicado 64 K  |
| 3   | Ministerio del Ambiente y Recursos Naturales | Dedicado 64 K  |
| 4   | Vice-Presidencia de la Republica             | Dedicado 64 K  |
| 5   | Ministerio de Educación Superior             | Dedicado 64 K  |
| 6   | Consejo Moral Republicano                    | Dedicado 64 K  |
| 7   | Ministerio de Comunicación e Información     | Dedicado 64 K  |
| 8   | Ministerio de la Defensa                     | Dedicado 64 K  |

*Tabla 4.2. Distribución de enlaces Sigecof conectados por la red de Platino*

| N ° | Localidades del Proyecto: OOCF                | Tipo de Enlace |
|-----|-----------------------------------------------|----------------|
| 1   | Fiscalía General de la Republica              | Dedicado 256 K |
| 2   | Ministerio de Ciencia y Tecnología            | Dedicado 256 K |
| 3   | Ministerio de Relaciones Exteriores           | Inalámbrica    |
| 4   | Ministerio de Educación                       | Dedicado 64 K  |
| 5   | Ministerio de la Secretaría de la Presidencia | Inalámbrica    |
| 6   | Defensoría del Pueblo                         | Dedicado 64 K  |
| 7   | Contraloría General de la República           | Dedicado 64 K  |
| 8   | Procuraduría General de la Republica          | Dedicado 256 K |
| 9   | Ministerio de Interiores y Justicia           | Dedicado 128 K |
| 10  | Consejo Nacional Electoral (C.N.E)            | Dedicado 128 K |
| 11  | Ministerio de Energía y Minas                 | Fibra Óptica   |
| 12  | Ministerio de Infraestructura                 | Fibra Óptica   |

|    |                                                        |               |
|----|--------------------------------------------------------|---------------|
| 13 | Ministerio de Planificación y Desarrollo               | Fibra Óptica  |
| 14 | Ministerio de Producción y Comercio                    | Fibra Óptica  |
| 15 | Asamblea Nacional                                      | Dedicado 64 K |
| 16 | Ministerio de Agricultura y Tierra                     | Fibra Óptica  |
| 17 | Direcion Ejecutiva de la Magistratura.                 | Dedicado 64 K |
| 19 | Superintendencia Nacional de Auditoría Interna (SUNAI) | Inalámbrica   |

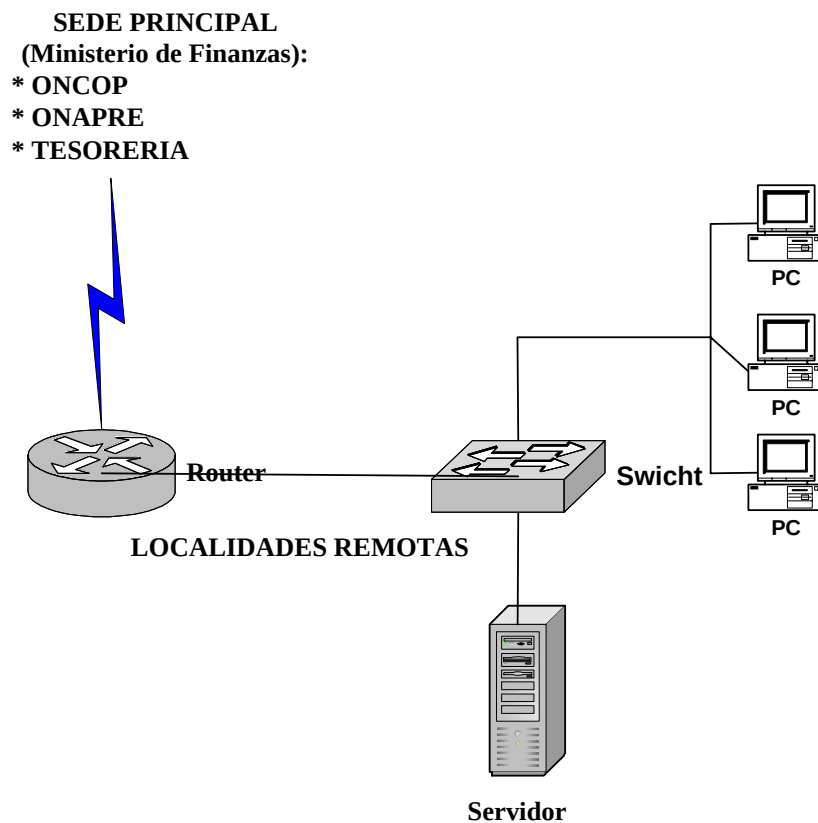


*Figura 4.2. Sistema de acceso actual*

La administración de los equipos de comunicación utilizados en la plataforma actual son administrados directamente por estos dos proveedores respectivamente, lo que imposibilita en muchos casos la solución inmediata de problemas ya que dependemos de un tercero para la solución del mismo.

Nosotros como Organismo Administrador del Sigecof nos encargamos de monitorear y detectar las fallas presentadas por dichos enlaces, a través de una serie de herramientas de monitoreo como el HostMonitor y el HPOpenView.

---

## **Sistema de Seguridad del Sigecof**

La información es uno de los recursos más valiosos de las instituciones y aunque intangible, necesita ser controlada y revisada con el mismo cuidado que los demás activos de la institución, por tal motivo uno de los principales problemas de todo sistema es que cuente con un sistema integral de los componentes de seguridad, con el fin de lograr una utilización más eficiente y segura de la información que sirve para una adecuada toma de decisiones.

Para contar con un adecuado nivel de seguridad es importante tener presente que existen una serie de componentes que interrelacionados llevan al logro del nivel de seguridad planteado ya que cada uno de ellos en forma particular y conjunta juega un papel trascendental dentro del esquema de seguridad, donde la falta o debilidad de alguno de ellos implica un factor de riesgo en el uso eficiente y seguro de la información.

El SIGECOF Actualmente no dispone de un Sistema de Seguridad a nivel de Redes y Comunicaciones, no se disponen de dispositivos de Seguridad para tal fin, solo contamos con Seguridad a Nivel de Aplicación a través de los mecanismo de Identificación, Autenticación y Control de Acceso garantizando en todo momento la confidencialidad, integridad y disponibilidad de los Datos.

Esta base de seguridad que actualmente disponemos nos hace muy propensos y vulnerables a ataques mal intencionados y que expertos en la materia puedan violar los mecanismos con los que contamos actualmente.

## **Limitaciones en la Plataforma Actual**

Actualmente la Red Actual del SIGECOF permite satisfacer las demandas básicas de servicios y de comunicación, aunque sumado a la evolución de nuevas tecnologías y aplicaciones de redes, debe ser revisado y evaluado en cuanto a fin de mejorar el flujo de tráfico que circula por la red.

- La administración de los equipos de comunicaciones de la plataforma actual depende del proveedor del servicio, en nuestro caso CANTV y la red PLATINO.
- No se dispone de una plataforma de telecomunicación uniforme, la velocidad de conexión puede variar en cada nodo de acuerdo al tipo de enlace provisto, lo que implica que no todos los procesos de negocios ejecutados en los servidores SIGECOF, pueden tardar el mismo tiempo, el tiempo varia de acuerdo a la conexión.

- 
- No se dispone de un esquema de seguridad estándar para cada nodo, la seguridad depende de cada uno de ellos y en muchos casos la red de usuarios del SIGECOF está aislada de la Red LAN de cada nodo.
  - La Red Platino tiende a ser bastante inestable, y los tiempos de respuesta de las aplicaciones es bastante lento.

### **Requerimientos de la Plataforma Tecnológica Actual**

El análisis y estudio que se le realizó a la plataforma tecnológica actual, conjuntamente con la información recopilada y la investigación documental sobre las diferentes tecnologías de Firewall que se ofrecen actualmente en el mercado, condujo a identificar las necesidades y requerimientos del sistema de seguridad actual. Estos requerimientos se exponen a continuación:

- El sistema de seguridad debe tener alta disponibilidad, proveer una infraestructura informática moderna y eficiente.
- La solución a implementar debe soportar todos los servicios que actualmente no son procesados por el sistema de seguridad.
- Debe preverse la posibilidad de instalar nuevas tecnologías o expandir ante nuevas necesidades, tomando en cuenta las aplicaciones y los servicios que están en proyecto.
- La administración de la plataforma debe ser sencilla, amigable y que cuente con una interfaz gráfica, con ayuda en línea, de manera que pueda simplificar su administración sin consumir mucho tiempo.
- El dispositivo de seguridad debe contar con una amplia garantía, con soporte técnico de la compañía que lo fabrica y poseer una certificación avalada por algún organismo de seguridad internacional.
- Debe contar con un puerto DMZ para crear un área de información protegida desmilitarizada en la red, a fin de que los usuarios externos puedan ingresar al área protegida, pero no puedan acceder al resto de la red.
- La solución debe contar con alta disponibilidad de manera de garantizar la continuidad del acceso a los servicios, aplicaciones en línea y la operatividad segura de la red privada.
- Contar con una red cien por cien inteligente y amigable.

- 
- Establecer e implantar un plan para la modernización de la infraestructura de transmisión de datos.
  - Adicionalmente debe soportar conexiones VPN para una conectividad privada virtual basada en IPSec que permita un acceso remoto seguro.

---

## **Capítulo 5**

### **Desarrollo del Proyecto**

Durante la realización de este proyecto, se hicieron gran cantidad de pruebas, muchas de las cuales se diferenciaban unas de otras debido a la estructura de red que posee cada Nodo. Resultaría reiterativo mencionar cada una de las pruebas realizadas. Por el contrario, nombrar el tipo de pruebas que se realizaron en cada momento y el objetivo, así como los resultados, aportaría mayores beneficios a la comprensión de dichas pruebas.

#### **Descripción de la Solución**

Tomando en cuenta los problemas presentados en la situación actual y basado en los requerimientos planteados, se elaboró el siguiente diseño para la Actualización de la Infraestructura Tecnológica del SIGECOF e Implementación del Esquema de Seguridad:

- **Localidades y Requerimientos**

Se requiere la interconexión de 27 localidades con la sede del Ministerio de Finanzas, consolidando el tráfico de datos e implementando una red, definiendo políticas de seguridad entre todas las localidades del proyecto, así como los usuarios del sistema SIGECOF.

El equipo a utilizar para la seguridad debe permitir la creación de VPN y contar con el Internet Protocol Security.

En la siguiente tabla se muestra las localidades del proyecto, las cuales son los Organismos Ordenadores de Compromisos y Pagos (OOCOP) de la administración central:

*Tabla 5.1. Localidades del proyecto*

| N ° | Localidades del Proyecto: OOC                          |
|-----|--------------------------------------------------------|
| 1   | Principal Ministerio de Finanzas                       |
| 2   | Fiscalía General de la Republica                       |
| 3   | Ministerio de Ciencia y Tecnología                     |
| 4   | Ministerio de Relaciones Exteriores                    |
| 5   | Ministerio de Educación                                |
| 6   | Ministerio de la Secretaría de la Presidencia          |
| 7   | Defensoría del Pueblo                                  |
| 8   | Contraloría General de la República                    |
| 9   | Procuraduría General de la Republica                   |
| 10  | Ministerio de Interiores y Justicia                    |
| 11  | Consejo Nacional Electoral (C.N.E)                     |
| 12  | Ministerio del Trabajo                                 |
| 13  | Ministerio de Salud y Desarrollo Social                |
| 14  | Ministerio del Ambiente y Recursos Naturales           |
| 15  | Ministerio de Energía y Minas                          |
| 16  | Ministerio de Infraestructura                          |
| 17  | Ministerio de Planificación y Desarrollo               |
| 18  | Ministerio de Producción y Comercio                    |
| 19  | Vice-Presidencia de la Republica                       |
| 20  | Asamblea Nacional                                      |
| 21  | Ministerio de Agricultura y Tierra                     |
| 22  | Ministerio de Educación Superior                       |
| 23  | Dirección Ejecutiva de la Magistratura.                |
| 24  | Consejo Moral Republicano                              |
| 25  | Ministerio de la Defensa                               |
| 26  | Ministerio de Comunicación e Información               |
| 27  | Superintendencia Nacional de Auditoría Interna (SUNAI) |

▪ **Interconexión Sede Principal – Sedes Remotas**

Para la interconexión de la Sede Principal del Ministerio con las 26 localidades remotas se propone utilizar como plataforma de transporte la Red Conmutada de

CANTV, consolidando la comunicación de datos solicitados sobre enlaces Frame Relay.

En la siguiente tabla se muestra la velocidad de la conexión Frame Relay hacia la red y el CIR asociado, de acuerdo al número de canales de voz que deben ser manejados y el tráfico de datos.

*Tabla 5.2. Configuración Frame Relay para transporte de tráfico de voz y datos*

| Cantidad  | Localidad      | Tipo de enlace     | Velocidad del Acceso | CIR (Kbps) |    |    |    |          |     |
|-----------|----------------|--------------------|----------------------|------------|----|----|----|----------|-----|
|           |                |                    |                      | 8          | 16 | 32 | 48 | 64       | 128 |
| <b>1</b>  | Sede Principal | <b>FRAME RELAY</b> | <b>2048</b>          |            |    |    |    |          |     |
| <b>27</b> | Sedes Remotas  | <b>FRAME RELAY</b> | <b>128</b>           |            |    |    |    | <b>X</b> |     |

Los equipos de acceso a la Red Frame Relay (Router) propuestos para la Sede Principal y para las localidades remotas son marca Cisco, específicamente el modelo 3660 (Sede Principal) y 1720 (Sedes Remotas), los cuales cumplen técnicamente con todos los requerimientos solicitados.

El equipo Cisco 3660 a instalar en la Sede Principal dispondrá de 2 puertos seriales, 2 interfaz Ethernet (10/100 BaseT).

El equipo Cisco 1720 a instalar en las localidades remotas dispondrá de 1 puerto serial, 1 puerto LAN Ethernet (10/100 BaseT).

La siguiente tabla muestra los puertos de datos que dispondrán los equipos Cisco por localidad.

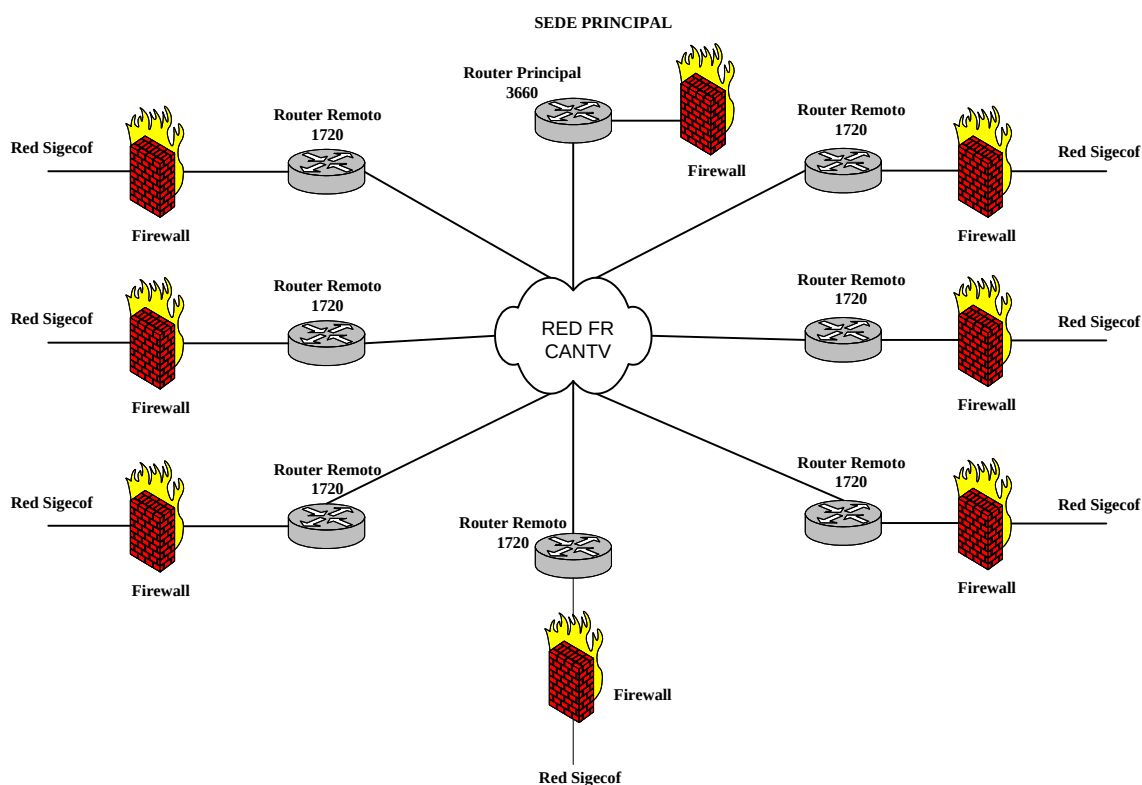
*Tabla 5.3. Disponibilidad de datos en los Routers por localidad.*

| N ° | Localidad        | Modelo | Puertos Seriales | Puertos LAN    |
|-----|------------------|--------|------------------|----------------|
| 1   | 1 Sede Principal | 3660   | 2                | 2 10/100Base T |
| 2   | 26 Sedes Remotas | 1720   | 1                | 1 10/100Base T |

La solución incluye el cableado necesario para las conexiones a los equipos de última milla de CANTV, el cableado de voz y las conexiones LAN a los hubs/switches del cliente.

A continuación se muestra un esquema simplificado de la red a implementar entre el Ministerio de Finanzas y las Localidades Remotas.

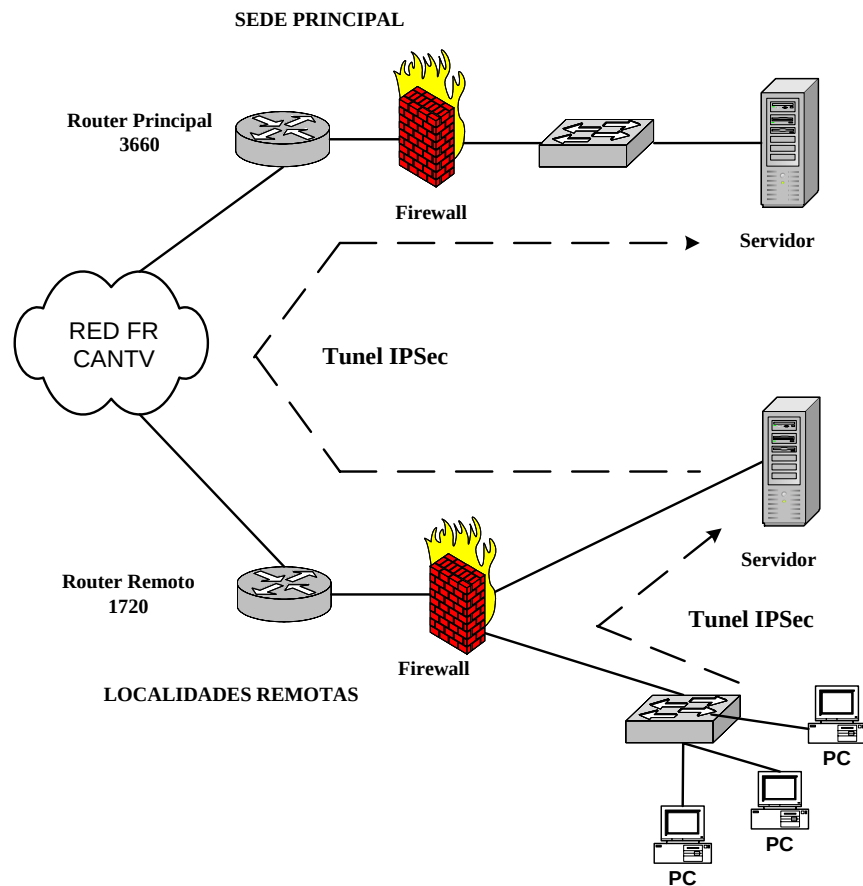
Figura 5.1. Esquema simplificado red a implementar



Considerando los requerimientos planteados, tenemos que la conexión desde cada una de las localidades a la Sede Principal se realizará a través de enlaces Frame Relay, estableciendo un túnel VPN, para la seguridad requerida. Cabe destacar que la conexión de los usuarios a los servidores en la localidad también se realizara a través de una VPN con su respectiva autenticación en el firewall.

Esta plataforma permitirá brindar a futuro una cantidad de servicios adicionales que generarán recursos y disminuirán costos operativos. Por otro lado la línea de dispositivos seleccionada es totalmente modular, lo que disminuye considerablemente los costos de actualización, expansión y adecuación a nuevas tecnologías.

Figura 5.2. Conexión a través de túneles VPN IPSec



Esta solución no contempla la integración de las redes en las localidades remotas, es decir, en cada localidad remota existirá una red independiente para SIGECOF, con su respectivo plan IP del Ministerio de Finanzas. Cabe destacar que para lograr la integración con cada uno de los ministerios u organismos del estado, se requiere del esquema de su red, así como del equipamiento (switches, router, etc).

▪ **Configuración de los Equipos Router Cisco 3660 y 1720**

**Routers:** La serie de routers cisco es modular, ofrece flexibilidad en cuanto a la instalación de módulos adicionales de acuerdo a los requerimientos.

**Ventajas de router Cisco:**

Al formar parte de las completas soluciones de red Cisco de extremo a extremo, la serie Cisco permite a las organizaciones ampliar la infraestructura de red de forma transparente y rentable a las pequeñas y medianas empresas y ofrece las siguientes ventajas:

- **Protección de la inversión:** ya que la serie Cisco admite componentes modulares actualizables en la instalación, los clientes pueden cambiar con facilidad las interfaces de red sin tener que realizar una “actualización

integral” de la solución implementada en la red de la oficina remota. Además protege la inversión económica permitiendo la capacidad de expansión necesaria para admitir servicios avanzados, tales como compresión y cifrado de datos asistida por hardware.

- **Costo de Operación Reducido:** mediante la integración de las funciones de las CSU/DSU, dispositivos de terminación de red RDSI (NTI), módems, firewalls, dispositivos de compresión o cifrado y demás equipamiento de los recintos de cableado de las oficinas remotas en una sola unidad la serie Cisco ofrece una solución que ahorra espacio y que puede gestionarse remotamente usando aplicaciones de administración de redes tales como Cisco Works o Cisco View.
- **Integración multiservicio voz/datos:** Cisco ofrece la solución de integración multiservicio voz/datos más amplia y con mayores posibilidades de crecimiento.
- **Solución de clase empresarial y proveedor:** cumple los requisitos que exigen las empresas de multiservicio y sus proveedores de servicios gestionados de terminal de abonado con características de alta fiabilidad, conexiones WAN múltiples y la posibilidad a nuevas plataformas.

A continuación se presenta la configuración de los router para cada una de las localidades:

Tabla 5.4. Configuración Router para la sede principal

|  <p><b>Cisco 3660</b></p> | Ítem | Descripción                                                   |
|--------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------|
|                                                                                                              | 1    | Dual 10/100 E Cisco 3660 6-slot Modular Router –AC with IP SW |
|                                                                                                              | 2    | Cisco 1700 IOS IP                                             |
|                                                                                                              | 3    | A MB Blank Flash PCMCIA Card for the Cisco 3600 Series        |
|                                                                                                              | 4    | 32 to 64 MB DRAM Factory Upgrade for the Cisco 3660           |
|                                                                                                              | 5    | 2 Port Serial WAN Interface Card.                             |
|                                                                                                              | 6    | V.35 Cable, DTE, Male, 10 Feet                                |
|                                                                                                              | 7    | M34 (Female) to DB25 (Male) Converter Cable.                  |

Tabla 5.5. Configuración Router para las 26 localidades remotas

|  <p><b>Cisco 1720</b></p> | Ítem | Descripción                                                   |
|------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------|
|                                                                                                            | 1    | 10/100 Base T Modular Router w/2 Wan slot, 8M Flash/32M DRAM. |
|                                                                                                            | 2    | 1 Port Serial WAN Interface Card.                             |
|                                                                                                            | 3    | Cisco 1700 IOS IP                                             |
|                                                                                                            | 4    | V.35 Cable, DTE, Male, 10 Feet                                |
|                                                                                                            | 5    | M34 (Female) to DB25 (Male) Converter Cable.                  |

### Implantación del Esquema de Seguridad Firewall

La propuesta de seguridad que se escogió como solución para este proyecto fue el Firewall WatchGuard Modelo Firebox III 700 para las sedes remotas y 4500 para la sede principal.

### Sistema de Seguridad WatchGuard

El sistema Firebox es una solución de seguridad de gran eficacia que incluye numerosas funciones fáciles de utilizar y gestionar desde una ubicación centralizada. Los modelos Firebox® III integran la función prevención de intrusiones, protección de firewalls y soporte de VPNs.

El sistema Firebox de WatchGuard incluye un extenso abanico de características de seguridad diseñadas para pequeñas y medianas empresas, oficinas centrales y concentradores de VPN.

### Características de Seguridad más destacadas del Sistema Firebox

- Prevención de intrusiones en el nivel de las aplicaciones
- Funciones de firewall de gran eficacia
- Gestión de VPN simplificada
- Gestión remota segura
- Seguridad en conexiones por cable/inalámbricas

- 
- Asistencia técnica proactiva
  - **Prevención de intrusiones**

WatchGuard integra la funcionalidad prevención de intrusiones en sus dispositivos de firewall/VPN desde 1997. Hoy ofrece un conjunto de funciones de prevención de intrusiones maduras e integradas que responde a las necesidades del mercado de las PYME.

La función prevención de intrusiones constituye un componente vital de la seguridad de la red distribuida en niveles. Reduce la vulnerabilidad de la red y los datos e incrementa el rendimiento de la inversión en cualquier solución de seguridad. La tecnología prevención de intrusiones integrada se gestiona mediante el mismo sistema de Firebox que sirve de base a las funciones de firewall y VPN.

**Inspección en el nivel de las aplicaciones (nivel 7)** mediante tecnología de proxy. Los paquetes de datos, incluidos el encabezado y la carga, son inspeccionados exhaustivamente y se descarta el contenido peligroso. Los modelos Firebox III incluyen proxies FTP, SMTP, HTTP y DNS.

**Bloqueo selectivo de direcciones IP de origen** para impedir que se realicen, durante un tiempo definido por el usuario, nuevos intentos de conexión con tráfico malintencionado.

**Detección de anomalías de protocolo**, que exige estándares por lo que respecta a los protocolos.

**El armado de los paquetes** garantiza la inspección completa del contenido de los paquetes.

**Tecnología de prevención de intrusiones integrada**, que elimina la necesidad de recurrir a componentes de hardware o software adicionales.

**Integra la función prevención de intrusiones** con los sistemas prevención de intrusiones (detección pasiva) existentes para una protección activa ante acciones hostiles.
  - **Seguridad con firewalls**

**El software de firewall** incluye la función (con homologación ICSA) de filtrado dinámico de paquetes con estado, por la que se examina el tráfico en los niveles 3 y 4 (red y transporte) para descartar la existencia de información malintencionada en los encabezados.

---

**La autenticación de usuarios a través de firewalls** impone procedimientos de acceso basados en usuarios o en grupos. Para la autenticación, el sistema Firebox System utiliza el servidor incorporado de WatchGuard®, Windows®, RADIUS®, SecurID® y CRYPTOCARD™.

**Con la traducción de direcciones de red (NAT)** se ocultan las direcciones IP internas para una mayor seguridad, se simplifica la gestión de direcciones IP y se reduce la necesidad de direcciones IP públicas. Los modelos Firebox III admiten NAT dinámica, estática, de uno a uno el IPSec Transversal, lo que contribuye a aumentar la productividad y a imponer procedimientos de acceso de ámbito corporativo.

**Con el filtrado de contenido Web** se controla el acceso a Web de usuarios o grupos por medio de una base de datos que se actualiza periódicamente.

**El software High Availability** permite instalar un dispositivo Firebox de respaldo para garantizar la protección en caso de que falle el Firebox activo. Los modelos deben ser iguales.

- **Seguridad en el escritorio**

**McAfee® VirusScan® ASaP** protege sus sistemas de escritorio. Cada producto Firebox incluye un número limitado de licencias de escritorio (es posible adquirir licencias adicionales). Podrá contar con asesoría y gestión antivirus centralizada por medio del servicio LiveSecurity®.

**El software SpamScreen** (opcional) filtra el correo electrónico no solicitado, con lo que se reduce el tráfico de red y aumenta la productividad de los empleados.

- **Compatibilidad con VPN**

**Con una función de optimización de VPN** se dirige el tráfico de las redes privadas virtuales hacia múltiples puntos finales por medio de un solo túnel VPN.

**Mobile User VPN** ofrece a los empleados remotos conexiones seguras compatibles con IPSec y un firewall personal con reglas de acceso y niveles de seguridad configurables. Mobile User VPN puede ejecutarse en cualquier equipo con Windows 98/2000/XP o Windows NT Workstation.

**La autenticación de usuarios de VPN** impone procedimientos de VPN basados en usuarios o en grupos, con autenticación mediante el servidor WatchGuard, Windows NT®, RADIUS®, SecurID® y CRYPTOCARD™.

---

**Mediante los certificados PKI** generados por la entidad interna emisora de certificados de WatchGuard se autentican los túneles de VPN.

- **Servicios de seguridad**

**El servicio LiveSecurity®** mantiene actualizada la seguridad. Cada sistema Firebox incluye una suscripción inicial renovable del servicio LiveSecurity, respaldado por excelentes profesionales expertos en seguridad, representantes de soporte y entrenadores.

Con el servicio LiveSecurity se recibirá asistencia técnica, actualizaciones de software, alertas y medidas frente a riesgos, noticias de asistencia, editoriales y herramientas de autoayuda en línea.

La siguiente tabla resume las funciones de seguridad destacadas:

*Tabla 5.6. Funciones de seguridad Firebox® III*

| Funciones de Seguridad                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Firewall:</b> Controla el tráfico internet de entrada y de salida, mediante avanzados proxies de seguridad y filtrado de paquetes.                         |
| <b>VPN:</b> Gestión de túneles VPN entre dispositivos y usuarios móviles.                                                                                     |
| <b>NAT:</b> Oculta las direcciones IP internas, y permite a los servidores internos con direcciones IP no registradas ser accesibles vía web de forma segura. |
| <b>Autenticación de usuarios:</b> Permite establecer políticas de acceso por usuarios o por grupos, así como monitorizar su uso de internet.                  |
| <b>Filtrado URL:</b> Controla los accesos web por parte de los usuarios, mediante Cyberpatrol®.                                                               |

## **Características de gestión destacadas**

El software de gestión del Sistema firebox simplifica la creación y administración de procedimientos de seguridad complejos, y permite gestionar la seguridad desde una ubicación centralizada, dentro o fuera de la red en la que se confía (incluso desde un PC portátil).

**VPN Manager** crea túneles de VPN entre oficinas centrales y sucursales rápidamente, con lo que se reduce en gran medida la complejidad de la gestión de VPN que abarcan varios centros de trabajo.

Se puede configurar procedimientos de seguridad para limitar el acceso a la red y garantizar el funcionamiento seguro de extranets basadas en VPN.

---

**Actualización de puerto ISP dual** la cual permite utilizar el puerto OPT con el fin de establecer una segunda conexión de ISP para la protección en caso de falla del sistema principal y para aumentar el tiempo de actividad.

**Las funciones de acceso centralizado y protección** contra fallas ofrece registros de inicio de sesión cifrados muy fiables, mantienen una disponibilidad inmediata de los datos de tráfico y permiten ver todos los dispositivos instalados desde una misma estación. Syslog (UDP) y el acceso cifrado seguro basado en TCP posibilitan la exportación de registros a aplicaciones de generación de informes externas, tales como WebTrends®.

- **Certificación de sistemas firebox**

Las tecnologías de firewalls y VPN de WatchGuard se adhieren a las normas reconocidas y publicadas, por lo que los productos de WatchGuard se integran fácilmente en las soluciones de seguridad existentes. El sistema Firebox sigue las normas ICSA para firewalls e IPsec para VPN.

La siguiente tabla resume las características de gestión destacadas de los **Modelos Firebox® III** utilizados en la implantación de la solución de seguridad:

*Tabla 5.7. Características de gestión Firebox® III*

| Gestión                                                                                                                                                                                                                                                                                                                                                                                  | Características                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Asistente de instalación rápida</li><li>• Security Policy Manager</li><li>• VPN Manager, 4 nodos (N/D en FB700 y FB500)</li><li>• Supervisión en tiempo real</li><li>• HostWatch™</li><li>• Informes de historiales</li><li>• Acceso seguro cifrado con protección contra fallas</li><li>• Fácil administración</li><li>• Notificación</li></ul> | <ul style="list-style-type: none"><li>• Prevención de intrusión con tecnología proxy en el nivel de la aplicaciones</li><li>• Filtrado de paquetes con estado</li><li>• Mobile User VPN</li><li>• Branch Office VPN</li><li>• NAT estática y dinámica</li><li>• NAT uno a uno</li><li>• Autenticación a través de firewalls</li><li>• NAT IPsec Traversal</li><li>• PKI con entidad interna emisora de certificados (CA, Certificate Authority)</li><li>• Filtrado de contenido Web</li><li>• Autenticación de VPN (Windows NT, RADIUS, PKI, servidor WG)</li></ul> |

|  |                                                                                                                                                                                                                                                                                                                                                     |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>• Detección de rastreo e intrusión</li> <li>• Bloqueo de puertos y sitios</li> <li>• Protección contra peticiones falsas de sincronización</li> <li>• Antivirus de escritorio</li> <li>• Compatibilidad con DHCP (<i>cliente y servidor</i>)</li> <li>• Compatibilidad con PPPoE (<i>cliente</i>)</li> </ul> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Especificaciones Técnicas

WatchGuard ofrece un sistema de protección contra posibles ataques externos, además de la capacidad de monitorear y controlar tanto la comunicación que proviene del exterior como la que se origina en la red interna.

### ▪ Firebox® 4500 Firewall

Firewall escalable de muy altas prestaciones, para empresas que requieran un elevado número de conexiones VPN.

El Firewall WatchGuard en su versión Firebox 4500 consta de tres interfaces: External, Optional y Trusted de 10/100. El puerto External se utiliza para la conexión a la red WAN a través de un router. El puerto Optional esta diseñado para conectar de manera segura los servicios y servidores de Application Server y Base de Datos y el puerto Trusted se utiliza para conectar la red privada de las sedes remotas. La conexión de los servidores en la zona desmilitarizada DMZ del firewall permitirá aumentar la seguridad de los mismos debido a que dichos equipos se encontrarán en una red físicamente distinta a la red privada y para su acceso desde la Sede Principal no es necesario acceder la red LAN. A su vez, el firewall permite acceder los servicios que se encuentran en la zona desmilitarizada DMZ desde la red privada LAN.

Figura 5.3. Vista física del Firebox® 4500 Firewall



La siguiente tabla resume las especificaciones técnicas y de funcionamiento del **Modelo Firebox® III 4500 (Sede Principal)** utilizado en la implantación de la solución de seguridad:

*Tabla 5.8. Especificaciones técnicas modelo Firebox® III 4500*

| <b>Especificaciones Técnicas</b> |                                                                                                   |
|----------------------------------|---------------------------------------------------------------------------------------------------|
| Procesador                       | AMD K6-3E+ 500MHz                                                                                 |
| Memoria                          | 256 MB, 8 MB Flash Disk                                                                           |
| Encriptación                     | High Performance Accelerator Board                                                                |
| Interfaces                       | Tres (3) puertos Ethernet 10/100TX Ethernet (incl. 1 DMZ) DB-9 Serial Port, PCI Expansion Option. |
| Alimentación                     | Tensión de Entrada: 100-240 VAC<br>Frecuencia de Funcionamiento: 50/60 Hz                         |
| Dimensiones                      | Ancho: (15.5" ) Alto: (2.85" ) Profndidad: (10.5")                                                |
| Peso                             | (8 Libras)                                                                                        |
| Frontal (Face Plate)             | Color Oro                                                                                         |

*Tabla 5.9. Especificaciones de funcionamiento Firebox® III 4500*

| <b>Funcionamiento</b>                               |             |
|-----------------------------------------------------|-------------|
| Numero maximo de Branch Office VPNs                 | 3000        |
| Numero maximo Mobile User VPNs                      | 3000        |
| Vel. de transf. con filtrado de paquetes con estado | 200 Mbps    |
| Vel. de transf. con prevención de intrusiones       | 60 Mbps     |
| Vel. de transf. VPN                                 | 100 Mbps    |
| Autenticación de usuarios                           | 5000        |
| Licencia de usuario                                 | Sin limite. |

#### ▪ **Firebox® 700 Firewall**

El sistema de seguridad de WatchGuard en su versión Firebox 700 presenta un hardware basado en un procesador AMD K6-2E 233MHz con un sistema operativo tipo Linux endurecido, además de un sistema de administración que trabaja sobre cualquier estación de trabajo tipo Windows NT, 2000, 95 o 98, el WatchGuard Policy Manager.

La combinación de Hardware y Software de WatchGuard (el Firebox 700, el WatchGuard Security Suite y el WatchGuard Policy Manager) cumplen todas las

necesidades de protección de las redes actuales, y en conjunto con el LiveSecurity System.

El Firebox 700 se conecta fácilmente a la red ubicándose entre la conexión a Internet y la red interna, mediante tres interfaces independientes de red. Esta configuración define una conexión para Internet, otra para la red corporativa protegida y además una red pública opcional para los servidores de Web, de e-mail, de FTP y en general de cualquier servicio público a Internet (conocida como la zona desmilitarizada). Cada interfaz de la red se vigila independientemente, aumentando los niveles de seguridad. Los indicadores delanteros y traseros informan inmediatamente a los encargados de redes estado de actividad mostrando el tráfico permitido o rechazado.

*Figura 5.4. Vista física del Firebox® 700 Firewall*



La siguiente tabla resume las especificaciones técnicas y de funcionamiento del **Modelo Firebox® III 700 (Sedes Remotas)** utilizado en la implantación de la solución de seguridad:

*Tabla 5.10. Especificaciones técnicas modelo Firebox® III 700*

| Especificaciones Técnicas |                                                                            |
|---------------------------|----------------------------------------------------------------------------|
| Procesador                | AMD K6-2E+ 233MHz                                                          |
| Memoria                   | 64 MB, 8 MB Flash Disk                                                     |
| Encriptación              | Software                                                                   |
| Interfaces                | Tres (3) puertos Ethernet 10/100TX Ethernet (incl. 1 DMZ) DB-9 Serial Port |
| Alimentación              | Tensión de Entrada: 100-240 VAC<br>Frecuencia de Funcionamiento: 50/60 Hz  |
| Dimensiones               | Ancho: (15.5" ) Alto: (2.85" ) Profndidad: (10.5")                         |
| Peso                      | (8 Libras)                                                                 |
| Frontal (Face Plate)      | Color Gris                                                                 |

---

*Tabla 5.11. Especificaciones de funcionamiento Firebox® III 700*

| <b>Funcionamiento</b>                               |                         |
|-----------------------------------------------------|-------------------------|
| Numero maximo de Branch Office VPNs                 | 150                     |
| Numero maximo Mobile User VPNs                      | 5 incluido, 150 maximo. |
| Vel. de transf. con filtrado de paquetes con estado | 150 Mbps                |
| Vel. de transf. con prevención de intrusiones       | 43 Mbps                 |
| Vel. de transf. VPN                                 | 5 Mbps                  |
| Autenticación de usuarios                           | 250                     |
| Licencia de usuario                                 | Sin limite.             |

---

## **Estrategia e Implantación de la Solución**

A continuación se detalla cada una de las actividades realizadas en el proceso de migración de la nueva plataforma de telecomunicaciones del proyecto SIGECOF, y las acciones llevadas a cabo para la puesta en producción de la solución, las cuales para fines descriptivos y logísticos se clasificaron en cinco fases principales:

1. Diseño e implementación de la arquitectura de red a instalar.
2. Instalación y configuración de equipos router.
3. Configuración del Firewall III WatchGuard 4500 (Sede Principal) y 700 (Sedes Remotas)
4. Configuración de las Redes Privadas Virtuales - VPN
5. Pruebas de servicios

## 1. Diseño e implementación de la arquitectura de red a instalar.

Tomando en cuenta los problemas presentados en la situación actual y basado en los requerimientos planteados en el capítulo anterior, se elaboró el siguiente diseño para la nueva plataforma de la infraestructura tecnológica del SIGECOF.

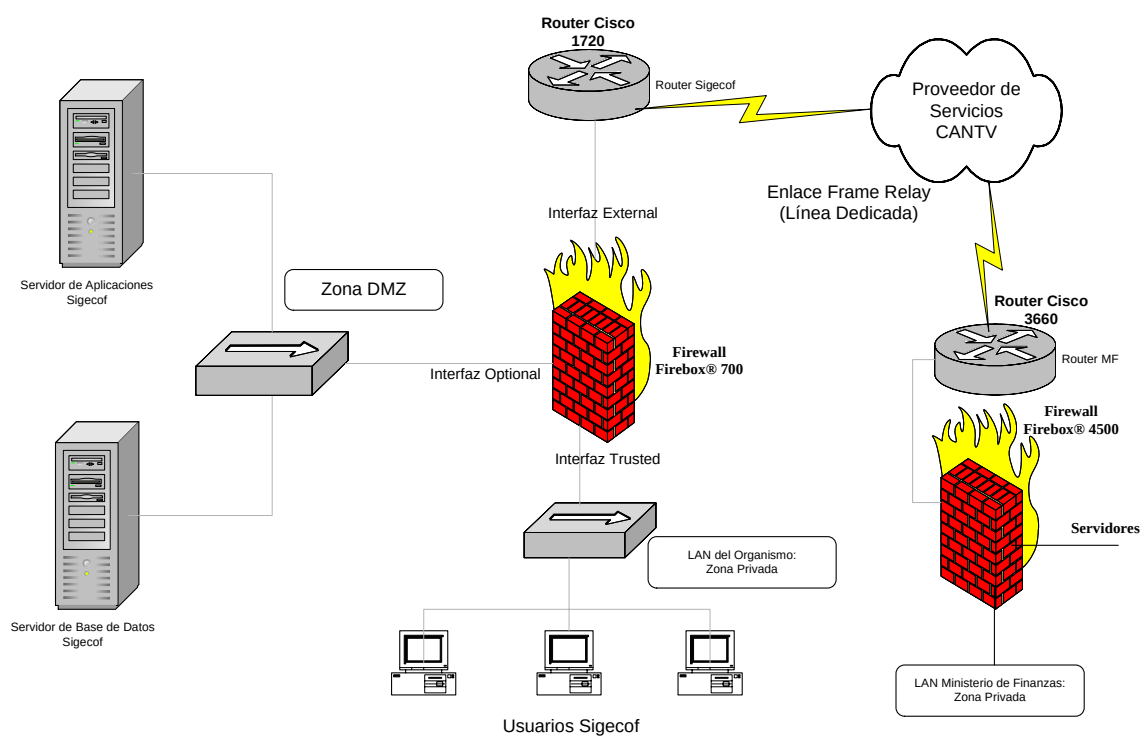


Figura 5.5. Arquitectura de red a montar

A continuación se explica en detalle la arquitectura de red a montar tanto en la sede principal como en las sedes remotas.

---

### Sede Principal:

#### Características Principales:

- Enlace Dedicado: Frame Relay de 2048 Kbps.
- Dispositivo Enrutador: Router Cisco 3660.
- Dispositivo de Seguridad: Firewall WatchGuard III 4500.

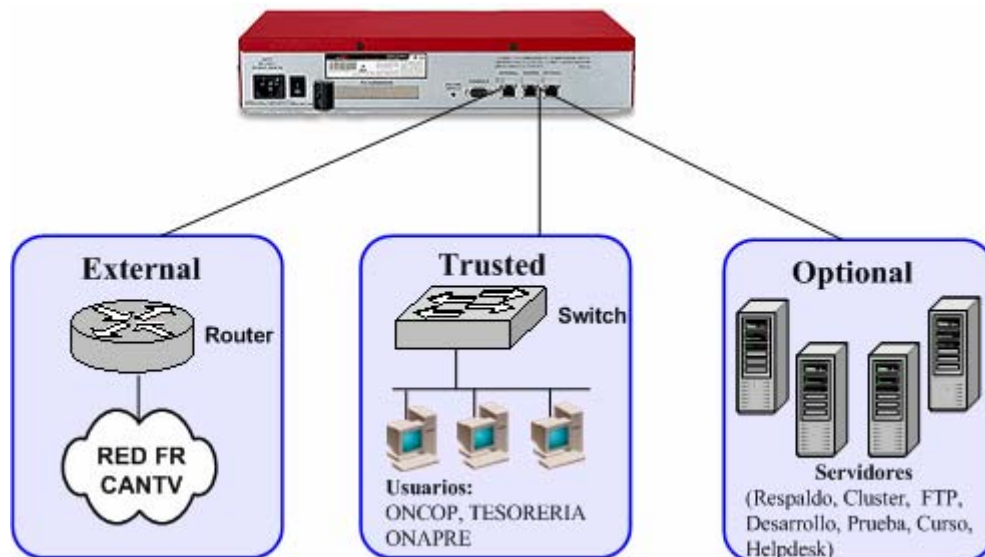


*Figura 5.6. Arquitectura de red sede principal*

### Sedes Remotas:

#### Características Principales:

- Enlace Dedicado: Frame Relay de 128/64.
- Dispositivo Enrutador: Router Cisco 1720.
- Dispositivo de Seguridad: Firewall WatchGuard III 700.

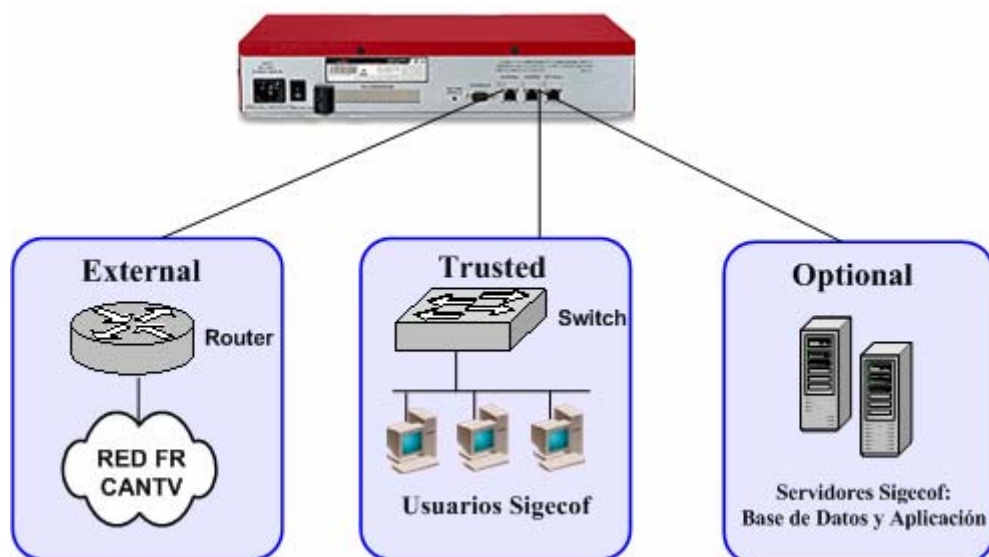


*Figura 5.7. Arquitectura de red sedes remotas*

---

## 2. Instalación y configuración de equipos Router.

El Router de conexión a la Red Frame Relay de CANTV son equipos Cisco 3660 (Sede Principal) y 1720 (Sedes Remotas).

El equipo Cisco 3660 a instalar en la Sede Principal dispondrá de 2 puertos seriales para la conexión WAN con el proveedor de servicios CANTV, 2 interfaz Ethernet (10/100 BaseT) para la conexión LAN hacia la red privada del Ministerio de Finanzas.

El equipo Cisco 1720 a instalar en las localidades remotas dispondrá de 1 puerto serial para la conexión WAN con el proveedor de servicios CANTV, 1 puerto LAN Ethernet (10/100 BaseT) para la conexión LAN hacia la red privada de cada Organismo.

El segmento de direcciones IP para la WAN / LAN fue proporcionado por CANTV, y las direcciones para los Servidores fue suministradas por la ONCOP. A continuación se especifica el segmento de direcciones asignadas y la configuración del Router Principal y las Sedes Remotas:

*Tabla 5.12. Direcccionamiento IP Routers*

| DIRECCIONAMIENTO IP |                     |     |                            |                  |     |                  |     |
|---------------------|---------------------|-----|----------------------------|------------------|-----|------------------|-----|
| WAN                 |                     |     | LAN                        |                  |     | SERVIDORES       |     |
| Localidad Remota    | Localidad Prinaipal | MSK | Puerto FastEthernet Router | Puertos Firewall | MSK | Localidad Remota | MSK |
| XX.XX.XX.XX         | XX.XX.XX.XX         | 30  | XX.XX.XX.XX                | XX.XX.XX.XX      | 30  | XX.XX.XX.XX      | 24  |

---

### **Configuración Router 3660 (Sede Principal):**

```
Current configuration : 9330 bytes
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname SIGECOF
logging buffered 32000 debugging
enable secret 5 $1$tvFb$SDmAJmaS803HRPDqVHXAd/
ip subnet-zero
mta receive maximum-recipients 0
interface FastEthernet0/0
description Conexion hacia LAN Local
ip address XX.XXX.X.X 255.255.255.252
load-interval 30
duplex auto
speed auto
interface Serial0/0
description Circuito Principal
no ip address
encapsulation frame-relay
no ip mroute-cache
load-interval 30
clockrate 2000000
no fair-queue
cdp enable
frame-relay traffic-shaping
frame-relay lmi-type ansi
interface Serial0/0.501 point-to-point
description Conexion con Min Defensa
ip address XXX.XX.X.XXX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 501
class enlace128/64
interface Serial0/0.502 point-to-point
description Conexion con Fiscalia General
ip address XXX.XX.X.X 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 502
class enlace128/64
interface Serial0/0.503 point-to-point
description Conexion con Min. Ciencia y Tecnologia
ip address XXX.XX.X.X 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 503
class enlace128/64
interface Serial0/0.504 point-to-point
description Conexion con Min. Relaciones Exteriores
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
```

---

```
frame-relay interface-dlci 504
  class enlace128/64
interface Serial0/0.505 point-to-point
description Conexion con Min. de Educacion
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 505
  class enlace128/64
interface Serial0/0.506 point-to-point
description Conexion con Min. Secretaria de la Presidencia
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 506
  class enlace128/64
interface Serial0/0.507 point-to-point
description Conexion con Tribunal Supermo de Justicia
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 507
  class enlace128/64
interface Serial0/0.509 point-to-point
description Conexion con Contraloria Gral.
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 509
  class enlace128/64
interface Serial0/0.511 point-to-point
description Conexion con Procuraduria Gral.
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 511
  class enlace128/64
interface Serial0/0.512 point-to-point
description Conexion con Min. Interior y Justicia
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 512
  class enlace128/64
interface Serial0/0.513 point-to-point
description Conexion con CNE
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 513
  class enlace128/64
interface Serial0/0.514 point-to-point
description Conexion con Min. del Trabajo
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 514
  class enlace128/64
```

---

```
interface Serial0/0.515 point-to-point
description Conexion con MSDS
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 515
class enlace128/64
interface Serial0/0.516 point-to-point
description Conexion con Ministerio de Ambiente y R. Natura
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 516
class enlace128/64
interface Serial0/0.518 point-to-point
description Conexion con Min. de Infraestructura
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 518
class enlace128/64
interface Serial0/0.519 point-to-point
description Conexion con Min. de Planificacion y Desarrollo
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 519
class enlace128/64
interface Serial0/0.520 point-to-point
description Conexion con Min. Produccion y Comercio
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 520
class enlace128/64
interface Serial0/0.521 point-to-point
description Conexion con Vicepresidencia de la Republica
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 521
class enlace128/64
interface Serial0/0.522 point-to-point
description Conexion con Asamblea Nacional
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 522
class enlace128/64
interface Serial0/0.523 point-to-point
description Conexion con Min. Agricultura y Tierra
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 523
class enlace128/64
interface Serial0/0.524 point-to-point
description Conexion con Min. Educacion Superior
```

---

```
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 524
  class enlace128/64
interface Serial0/0.525 point-to-point
description Conexion con Dir. Ejecutiva Magistratura
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 525
  class enlace128/64
interface Serial0/0.526 point-to-point
description Conexion con Consejo Moral Republicano
ip address XXX.XX.X.XXX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 526
  class enlace128/64
interface Serial0/0.530 point-to-point
description Conexion con Defensoria del Pueblo
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 530
  class enlace128/64
interface Serial0/0.540 point-to-point
description Conexion con Min. Energia Mina (PDVSA)
ip address XXX.XX.X.XX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 540
  class enlace128/64
interface Serial0/0.550 point-to-point
description Conexion con SUNAI
ip address XXX.XX.X.XXX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 550
  class enlace128/64
interface Serial0/0.555 point-to-point
description Conexion con Ministerio Comunicaciones
ip address XXX.XX.X.XXX 255.255.255.252
no ip mroute-cache
frame-relay interface-dlci 555
  class enlace128/64
interface FastEthernet0/1
description Conexion hacia LAN Local
no ip address
load-interval 30
shutdown
duplex auto
speed auto
interface Serial0/1
no ip address
shutdown
```



---

```
ip route XX.XXX.X.XXX 255.255.255.252 XXX.XX.X.XXX
ip route XX.XXX.X.XXX 255.255.255.252 XXX.XX.X.XXX
ip route XX.XXX.X.XXX 255.255.255.252 XXX.XX.X.XXX
ip route XX.XXX.X.XXX 255.255.255.252 XXX.XX.X.XXX
ip http server
map-class frame-relay enlace128/64
  frame-relay cir 64000
  frame-relay be 64000
  frame-relay mincir 64000
snmp-server community Sunacic RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server host XX.XX.X.XX Oncop
snmp-server host XX.XX.X.XX Oncop
call rsvp-sync
mgcp profile default
dial-peer cor custom
line con 0
  password
  login
line aux 0
line vty 0 4
  password XXXXXX
  login
end
```

### **Configuración Router 1720 (Sedes Remotas):**

```
Current configuration : 1278 bytes
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname Min_Rela_Exte
enable secret 5 $1$aN2Y$9Mvr5nH9eDgL8LP8/JFFt1
memory-size iomem 25
ip subnet-zero
no ip finger
interface Serial0
  description Circuito Principal
  no ip address
  encapsulation frame-relay
  no ip route-cache
  no fair-queue
  cdp enable
  frame-relay traffic-shaping
  frame-relay lmi-type ansi
interface Serial0.504 point-to-point
  description Conexion con Principal
```

---

```
ip address XXX.XX.X.XX 255.255.255.252
no ip route-cache
frame-relay interface-dlci 504
  class enlace128/64
interface FastEthernet0
  description Conexion hacia LAN Local
  ip address XX.XXX.X.XX 255.255.255.252
  speed auto
  ip classless
  ip route 0.0.0.0 0.0.0.0 XXX.XX.X.XXX
  no ip http server
  map-class frame-relay enlace128/64
  no frame-relay adaptive-shaping
  frame-relay cir 64000
  frame-relay be 64000
  frame-relay mincir 64000
snmp-server community Sunacic RO
snmp-server enable traps snmp
snmp-server enable traps frame-relay
snmp-server host XX.XX.X.XX Oncop
snmp-server host XX.XX.X.XX Oncop
line con 0
  password
  login
  transport input none
line aux 0
line vty 0 4
  password XXXXXX
  login
no scheduler allocate
end
```

---

### 3. Configuración del Firewall III WatchGuard 4500 (Sede Principal) y 700 (Sedes Remotas)

Firewall controla el tráfico de entrada y de salida, mediante avanzados proxies de seguridad y filtrado de paquetes.

Los dispositivos de seguridad usados en la nueva plataforma son Firewall WatchGuard Modelo Firebox III 700 para las Sedes Remotas y 4500 para la Sede Principal.

El Software de gestión del Firewall WatchGuard simplifica la creación y administración de procedimientos de seguridad complejos, y permite gestionar la seguridad desde una ubicación centralizada, dentro o fuera de la red mediante cifrado 3DES.

El Firewall WatchGuard en su versión Firebox 4500 / 700 consta de tres interfaces: External, Optional y Trusted, las cuales fueron configuradas de la siguiente manera:

- El puerto External o puerto WAN utilizado para la conexión a la red WAN Frame Relay de nuestro proveedor de servicio CANTV.
- El puerto Optional o zona desmilitarizada DMZ utilizado para conectar de manera segura los servicios y servidores de Application Server y Base de Datos del SIGECOF.
- El puerto Trusted o puerto LAN utilizado para conectar la red privada del Ministerio de Finanzas (En la Sede Principal) a los usuarios del Organismo administrador del SIGECOF (ONCOP) y los Órganos Rectores (ONAPRE y Tesorería) y en la Sede Remota utilizado para conectar a la Red LAN del Organismo a los usuarios finales del Sistema.

La conexión de los servidores en la zona desmilitarizada DMZ del firewall permitirá aumentar la seguridad de los mismos debido a que dichos equipos se encontrarán en una red físicamente distinta a la red privada y para su acceso desde la Sede Principal no es necesario acceder la red LAN. A su vez, el firewall permite acceder los servicios que se encuentran en la zona Desmilitarizada DMZ desde la red privada LAN.

A continuación se detalla la configuración del Firewall 4500 (Sede Principal) y Firewall 700 Sedes Remotas:

---

### Firewall III WatchGuard 4500 (Sede Principal):

A dicho firewall le fue asignado el siguiente direccionamiento IP:

- Puerto External o puerto WAN: XX.XX.XX.XX / 30.
- Puerto Optional o zona desmilitarizada DMZ: XX.XX.XX.XX / 24,
- Puerto Trusted o puerto LAN: XX.XX.XX.XX / 24, dirección de Red perteneciente al Segmento de Red Privada del Ministerio de Fianzas, específicamente a la VLAN asignada a la ONCOP, a través de este puerto se accesa directamente a cada uno de los Servidores de la Sede Principal y las Sedes Remotas los Usuarios de la ONCOP.

Fueron además agregadas como Redes Secundarias al puerto Trusted las Redes pertenecientes a las VLAN de los Usuarios de la ONAPRE y la Tesorería, las cuales son VLAN diferentes a la de la ONCOP.

A través de este puerto se administra el dispositivo de Seguridad desde la Sede Principal.

### Firewall III WatchGuard 700 (Sedes Remotas):

A dicho firewall le fue asignado el siguiente direccionamiento IP:

- Puerto External o puerto WAN: XX.XX.XX.XX / 30.
- Puerto Optional o zona desmilitarizada DMZ: XX.XX.XX.XX / 24,
- Puerto Trusted o puerto LAN: XX.XX.XX.XX / 24, dirección de Red perteneciente al Segmento de Red Privada de la Sede Remota.

La contraseña que le fue asignada para efecto de su administración es la siguiente:

**Firebox:** XX.XX.XX.XX

**Passphrase:** XXXXXXXX



*Figura 5.8. Conexión Firewall.*

---

### Configuración Network:

La configuración Network del equipo incluye direcciones IP y el modo de direccionamiento de la red.

El Firewall es configurado en el modo de operación Routed, este modo de configuración permite separar lógicamente las redes en cada una de sus tres interfaces. Este tipo de configuración es usado primordialmente cuando el número de direcciones públicas es limitado o cuando se tiene una IP dinámica asignada sobre la interfaz external.

La ventaja de este modo de configuración es que las redes son definidas de una forma que permite manejar fácilmente la creación de Redes Privadas Virtuales (VPN).

Todas las interfaces del Firewall son configuradas con redes diferentes y los equipos conectados detrás de cada una de ellas deben pertenecer al segmento de red configurado respectivamente.

La dirección IP asignada al puerto External del firewall es XX.XX.XX.XX / 30 y la puerta de enlace del firewall (Default Gateway) hacia la Red Frame Relay es el puerto FastEthernet del router Cisco cuya dirección IP es la XX.XX.XX.XX.

La siguiente tabla muestra la lista de Interfaces Configuradas:

*Tabla 5.13. Lista de interfaces configuradas Firewall principal.*

| Interface                    | Address     | Network        | Netmask         | Default Gateway |
|------------------------------|-------------|----------------|-----------------|-----------------|
| External Interface (eth0)    | XX.XX.XX.XX | XX.XX.XX.XX/30 | 255.255.255.252 | XX.XX.XX.XX     |
| Trusted Interface (eth1)     | XX.XX.XX.XX | XX.XX.XX.XX/24 | 255.255.255.0   | none            |
| Optional Interface (eth2)    | XX.XX.XX.XX | XX.XX.XX.XX/24 | 255.255.255.0   | none            |
| Secondary Interface (eth1:0) | XX.XX.XX.XX | XX.XX.XX.XX/24 | 255.255.255.0   | none            |
| Secondary Interface (eth1:1) | XX.XX.XX.XX | XX.XX.XX.XX/24 | 255.255.255.0   | none            |

### Rutas Adicionales Configuradas:

Se configuraron rutas adicionales en la interfaces Trusted del Firewall, para las Sub redes de ONAPRE y la Tesorería Nacional, que pertenecen a un segmento de Red diferente a la VLAN de la ONCOP.

*Tabla 5.14. Rutas adicionales configuradas en la sede principal.*

| Type | Device | Destination    | Mask          | Gateway     |
|------|--------|----------------|---------------|-------------|
| Net  | any    | XX.XX.XX.XX/24 | 255.255.255.0 | XX.XX.XX.XX |
| Net  | any    | XX.XX.XX.XX/24 | 255.255.255.0 | XX.XX.XX.XX |

En el caso de la configuración de rutas secundarias en las sedes remotas, se configuraron de acuerdo a las necesidades de cada nodo, es decir, en aquellos nodos donde el Organismo maneja entes descentralizados provenientes físicamente de otras redes diferentes a la Red LAN del Organismo se habilitaron en el Firewall dichas Redes. De esta forma el router principal del Organismo una vez que reciba la petición de solicitud de los Servicios del Servidor SIGECOF, debe enrutar los paquetes a la puerta o interfaces Trusted del Firewall.

En este caso se trabajó, muy coordinadamente con cada uno de los nodos para detectar cada una de las redes necesarias que necesitaban llegar al servidor, de esta forma se garantizaba el día de la migración la disponibilidad de los datos para todos los entes involucrados.

#### **Traducción de Direcciones de Red (NAT) Dinámico:**

Se realizó NAT dinámico para enmascarar las direcciones Trusted de los Firewall, en cada uno de los nodos, a la dirección de la interfaces External de los mismos, ya que en muchos casos los diferentes nodos poseen el mismo segmento de red en sus redes LAN.

NAT dinámica: Asignación de puerto a host interno.

NAT estática: Asignación de dirección IP a dirección IP.

NAT uno a uno: Asignación de direcciones de rango a rango.

#### **Configuración NAT:**

|                          |   |                          |
|--------------------------|---|--------------------------|
| Enable dynamic NAT       | → | yes                      |
| Dynamic NAT              | → | entries trusted-external |
| Dynamic NAT exceptions   |   |                          |
| Enable service based NAT | → | no                       |
| 1 to 1 NAT enabled       | → | no                       |

A continuación una vista de las pantallas finales de la configuración del Firewall:

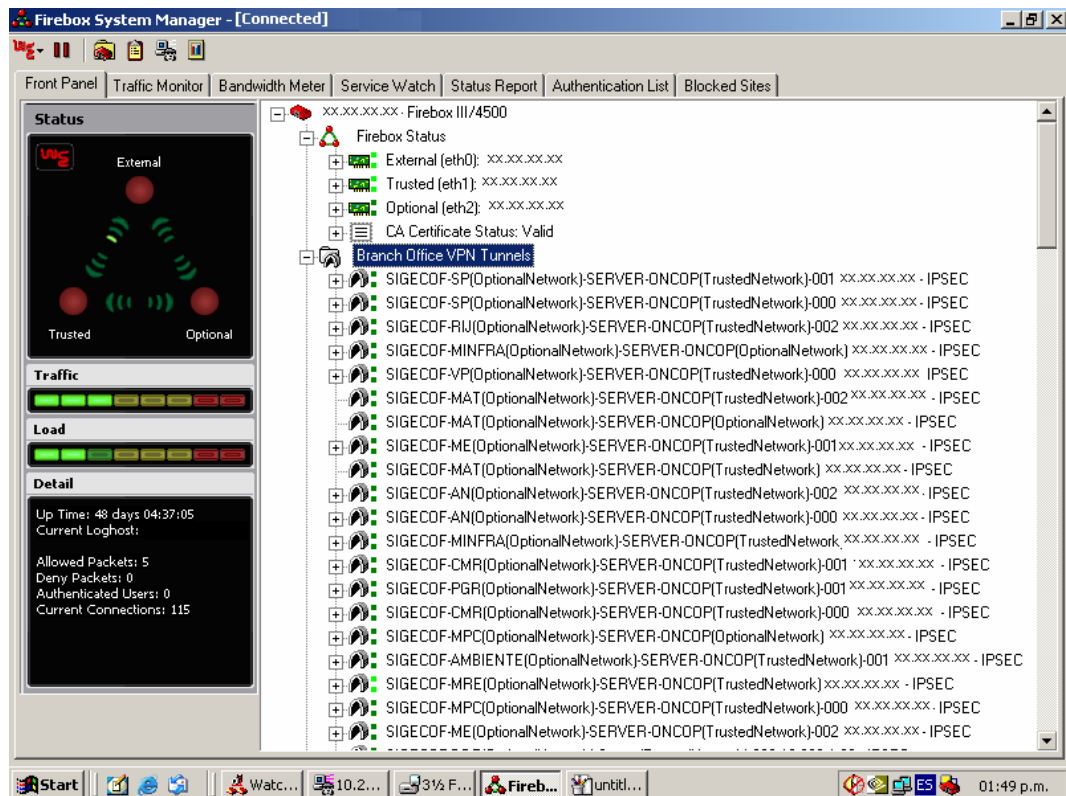


Figura 5.9. Configuración final Firewall 4500.

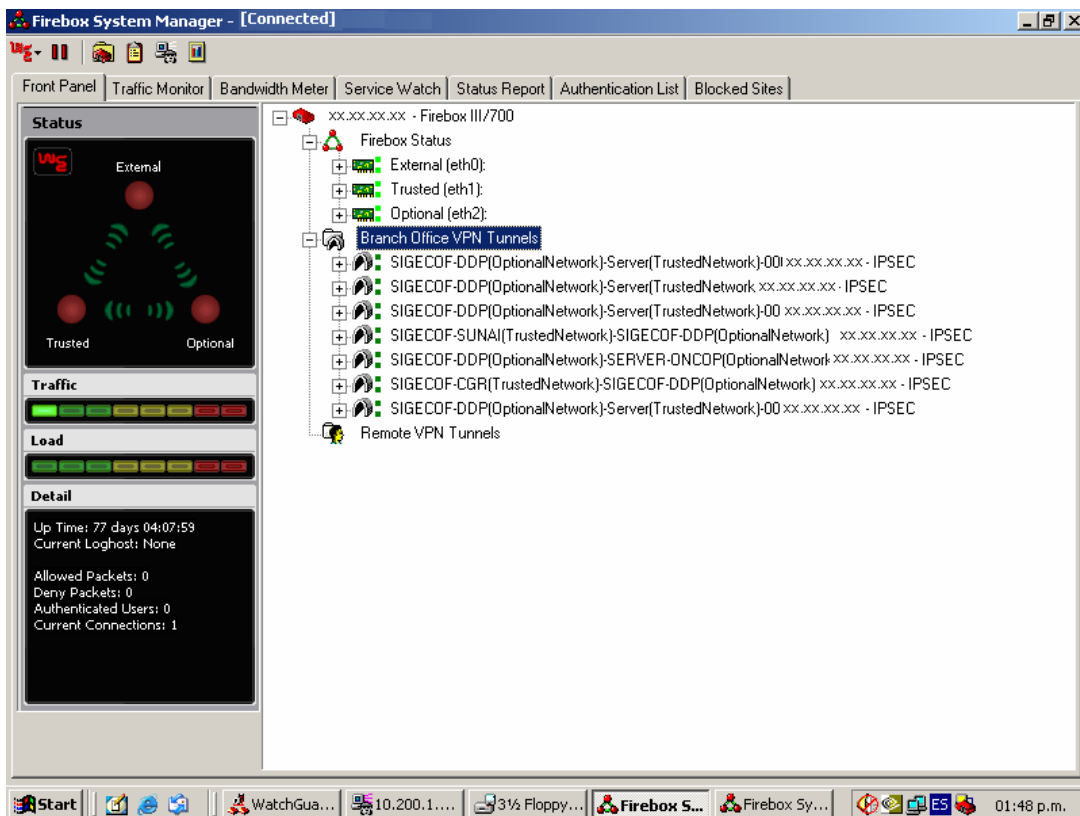


Figura 5.10. Configuración final Firewall 700.

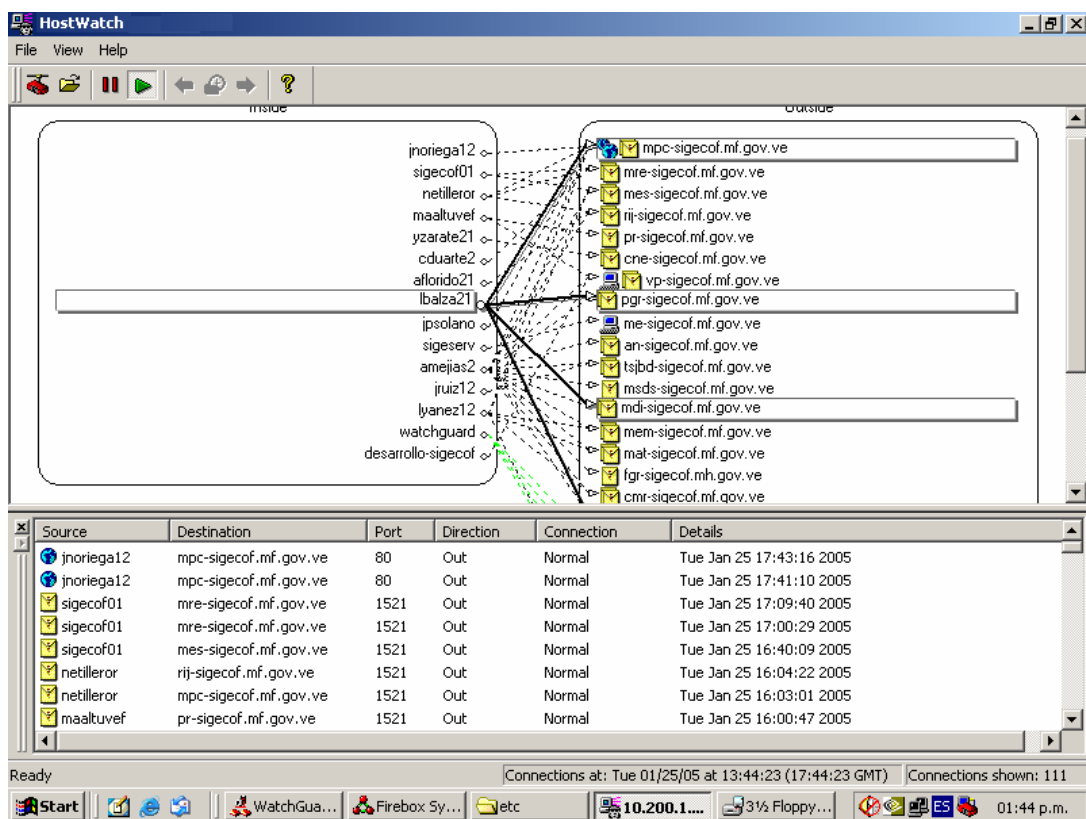


Figura . 5.11. Conexiones en tiempo real sede principal sedesremotas.

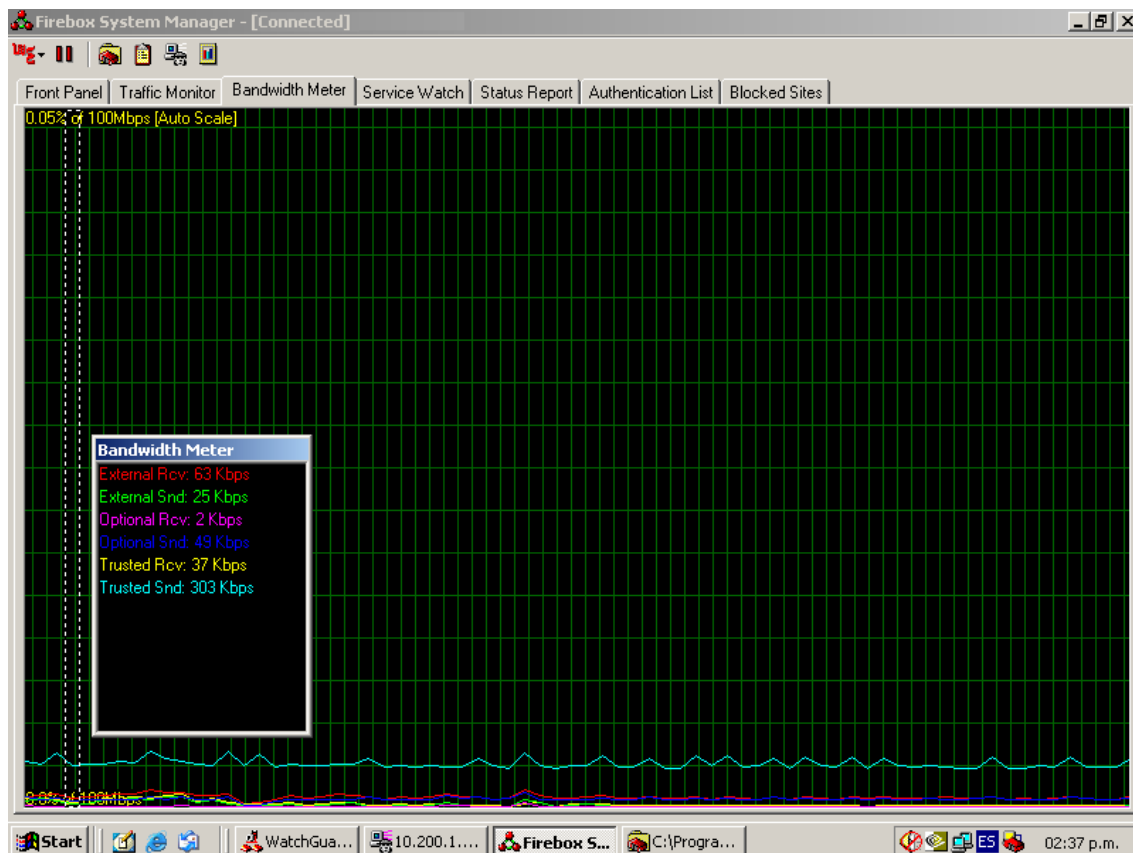


Figura . 5.12. Uso del enlace en tiempo real.

---

## **Configuración de filtrado Web**

Para el caso del Firewall tanto en la Sede Principal como en la Sede Remota no se configuró ningún tipo de filtrado Web debido a que a través de este enlace solo se acceden a los servicios del Servidor SIGECOF, el enlace Frame Relay es dedicado utilizado solo para el acceso al Sistema.

## **Configuración de Políticas**

Las políticas configuradas en el firewall WactGuard definen cuales servicios de red son bloqueados y cuales servicios son autorizados por el equipo; esto permite regular el tráfico TCP/IP a través de los diferentes puertos del firewall. El firewall fue configurado para que bloqueara el tráfico TCP/IP en sentido entrante desde la WAN hacia la LAN y permitiese todo el tráfico TCP/IP en sentido saliente (desde la LAN hacia la WAN y desde la LAN hacia la DMZ).

Dependiendo de las aplicaciones de red que sean necesarias implementar, se autoriza o se niega un determinado servicio (puertos TCP/IP) entre los diferentes puertos del firewall. Esto permite controlar el tráfico entre los puertos del equipo de una forma segura evitando posibles puntos de acceso a la red innecesarios, los cuales son utilizados por hackers para efectuar ataques a la red privada LAN. Al realizar este tipo de configuración hay que tener sumo cuidado de cuales servicios se permiten y cuales se bloquean, ya que una mala configuración puede permitir vulnerar la seguridad de la red privada.

En este sentido, las aplicaciones principales tomadas en cuenta para la configuración del firewall son: el servicio de FTP y el servicio para la administración remota del equipo.

El primero el cual se habilitó para realizar los respectivos respaldos vía FTP, puerto 21, de las base de datos del SIGECOF de las diferentes Sedes Remotas a la Sede Principal, es decir desde el área DMZ del Firewall 700 (Sede Remota) al área DMZ del Firewall 4500 (Sede Principal), donde se encuentra ubicado nuestro servidor de Respaldos.

El segundo servicio fue configurado de tal forma que los Firewall en la Sede Remota puedan ser administrados desde la Sede Principal a través de la interfaz External, y el firewall en la Sede Principal pueda ser administrado solamente desde la interfaz Trusted del mismo.

---

#### 4. Configuración de las Redes Privadas Virtuales – VPN

La configuración VPN se implementó para crear túneles VPN desde los usuarios del Sistema hacia los servidores SIGECOF.

Se creó un túnel o conducto de un sitio a otro para transferir los datos en forma encapsulada además que los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

La conexión desde cada una de las Sedes Remotas a la Sede Principal se realizó a través de enlaces Frame Relay estableciendo un túnel VPN IPSEC, para la seguridad requerida.

Los túneles VPN que fueron creados son los siguientes:

- Sede Principal (Interfaz Trusted) – Sedes Remotas (Interfaz Optional):  
A través de este túnel los usuarios de la ONCOP el Organismo administrador del SIGECOF, la ONAPRE y la Tesorería Nacional los Órganos Rectores de la Administración Pública, podrán acceder en forma segura a los servidores SIGECOF en cada una de las Sedes Remotas ubicados en la interfaz optional o zona DMZ del firewall.
- Sede Principal (Interfaz Optional) – Sedes Remotas (Interfaz Optional):  
A través de este túnel la granja de servidores de la ONCOP (Servidores de Respaldo, FTP, Prueba, Desarrollo, Curso) ubicados en la interfaz optional del firewall principal podrá acceder los servidores SIGECOF en cada una de las Sedes Remotas.
- Sede Remota Contraloría Genreal de la República (Interfaz Trusted) – Sedes Remotas (Interfaz Optional):  
A través de este túnel los usuarios SIGECOF de la C.G.R. podrán acceder a los servidores SIGECOF de las demás Sedes Remotas. Estos túneles adicionales fueron creados ya que la C.G.R. a través de ciertos Roles de algunos usuarios del Sistema debe aprobar ciertos procesos o partidas en el presupuesto del resto de los Organismos los cuales son manejados en el sistema.
- Sede Remota Superintendencia Nacional de Auditoria Interna (Interfaz Trusted) – Sedes Remotas (Interfaz Optional):  
A través de este túnel los usuarios SIGECOF de la S.U.N.A.I. podrán acceder a los servidores SIGECOF de las demás Sedes Remotas, al igual

que la C.G.R. la S.U.N.A.I. realiza ciertos procesos de auditoria interna manejados en el sistema.

La siguiente tabla resume los túneles VPN que fueron creados:

Tabla 5.15. Túneles VPN.

| Origen                                                                               | Destino                                 |
|--------------------------------------------------------------------------------------|-----------------------------------------|
| Trusted Interface (eth1) Sede Principal                                              | Optional Interface (eth2) Sedes Remotas |
| Optional Interface (eth2) Sede Principal                                             | Optional Interface (eth2) Sedes Remotas |
| Trusted Interface (eth1) Nodo Contraloría General de la República (CGR)              | Optional Interface (eth2) Sedes Remotas |
| Trusted Interface (eth1) Nodo Superintendencia Nacional de Auditoria Interna (SUNAI) | Optional Interface (eth2) Sedes Remotas |

Figura 5.13. Esquema VPN general.

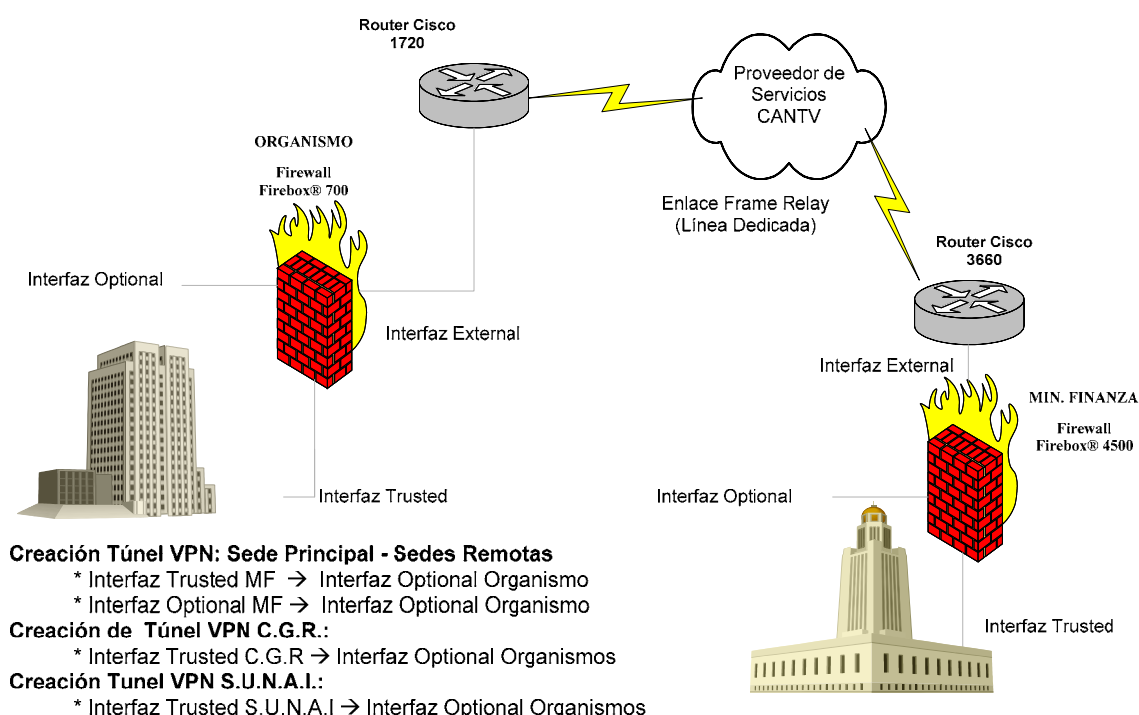
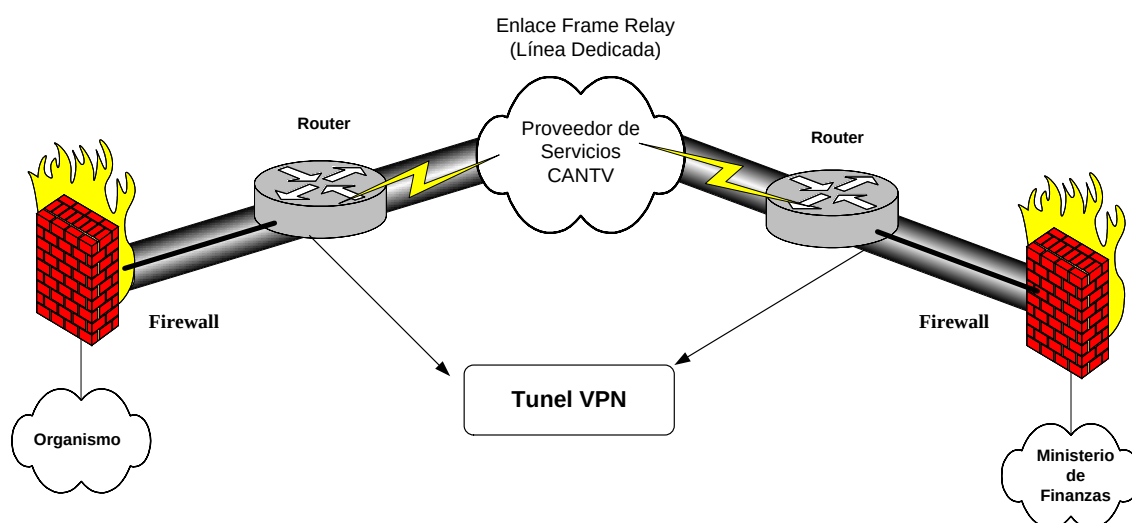


Figura 5.14. Túnel VPN.



La creación de los túneles VPN se realizó a través del Software VPN Manager.

**VPN Manager** crea túneles de VPN entre oficinas centrales y sucursales rápidamente, con lo que se reduce en gran medida la complejidad de la gestión de VPN que abarcan varios centros de trabajo.

El software de gestión simplifica la creación y administración de procedimientos de seguridad complejos, y permite gestionar la seguridad desde una ubicación centralizada, dentro o fuera de la red en la que se confía (incluso desde un PC portátil) mediante cifrado 3DES.

El proceso de encriptación y autenticación se realiza utilizando una de las siguientes tecnologías:

DES - CBC & MD5 - HMAC (menor seguridad mayor velocidad de respuesta)

DES - CBC & SHA1 - HMAC

3DES - CBC & MD5 - HMAC

3DES - CBC & SHA1 - HMAC (mayor seguridad menor velocidad de respuesta)

VPN Manager facilita la instalación y gestión de VPN. El software VPN Manager de WatchGuard permite configurar y gestionar VPN con varios sitios en tres pasos:

1. Se seleccionó los dos Firewall a conectar a través de un túnel VPN, y la interfaz a configurar en cada uno.

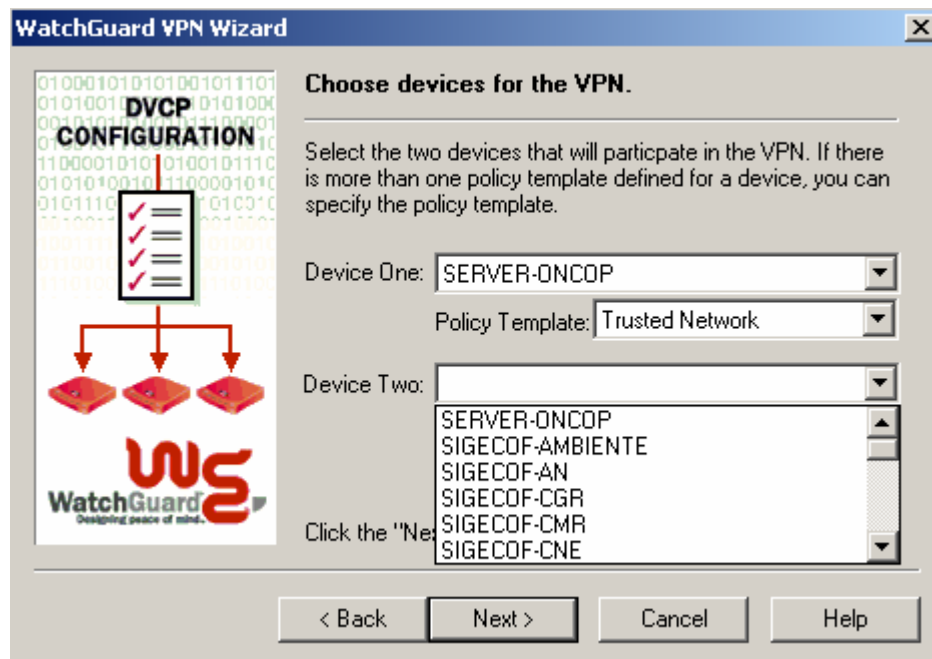


Figura 5.15. Configuración VPN.

2. Se escogió el nivel de seguridad requerido para el túnel VPN.

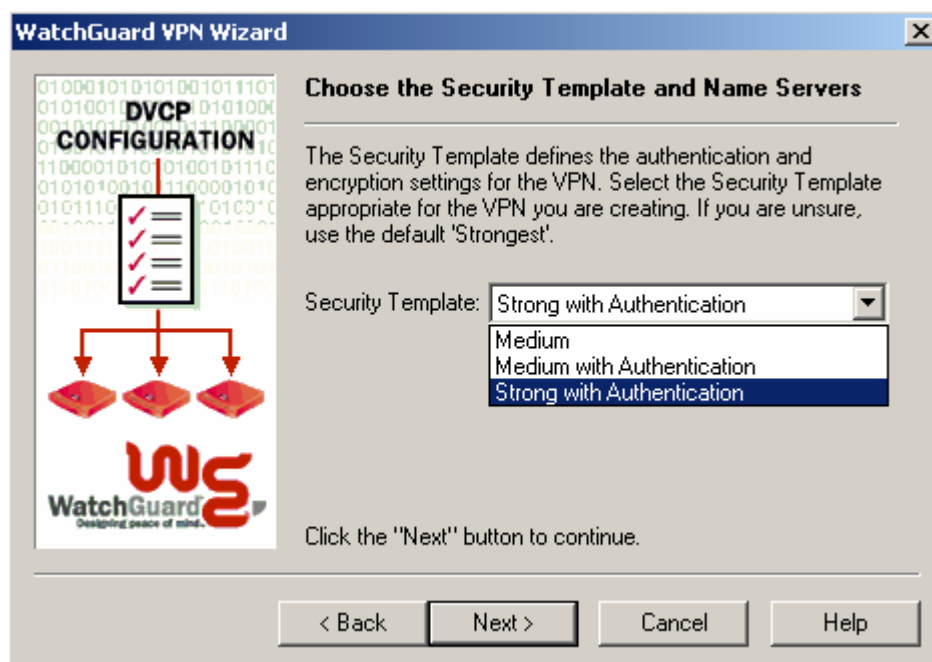


Figura 5.16. Configuración VPN Security.

3. Finalmente la VPN Manager automáticamente crea el túnel VPN

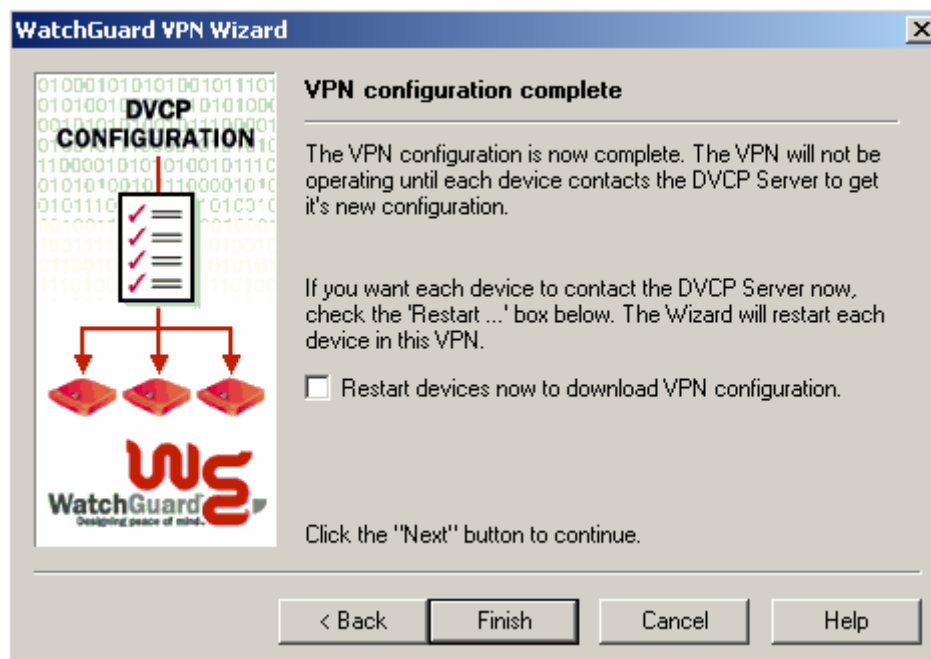


Figura 5.17. Configuración VPN final.

A continuación algunas vistas finales de la configuración de las VPN:

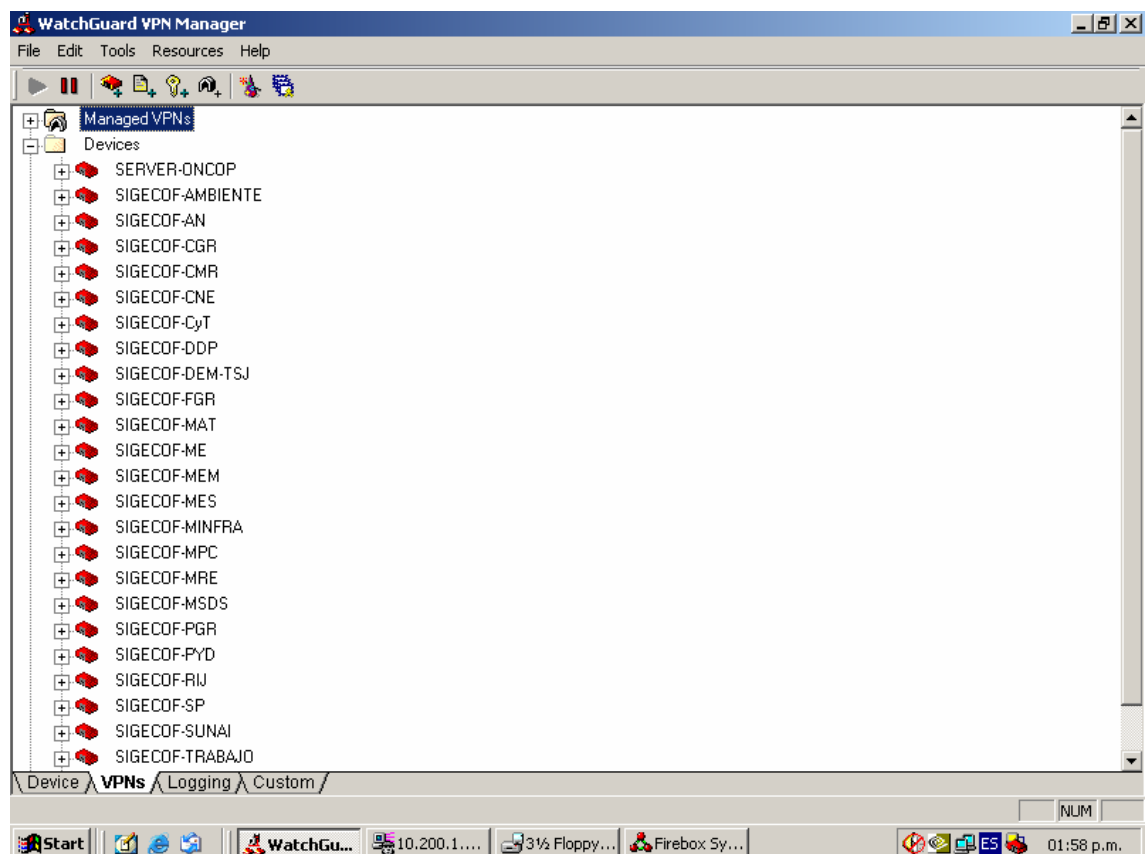


Figura 5.18. VPN Manager.

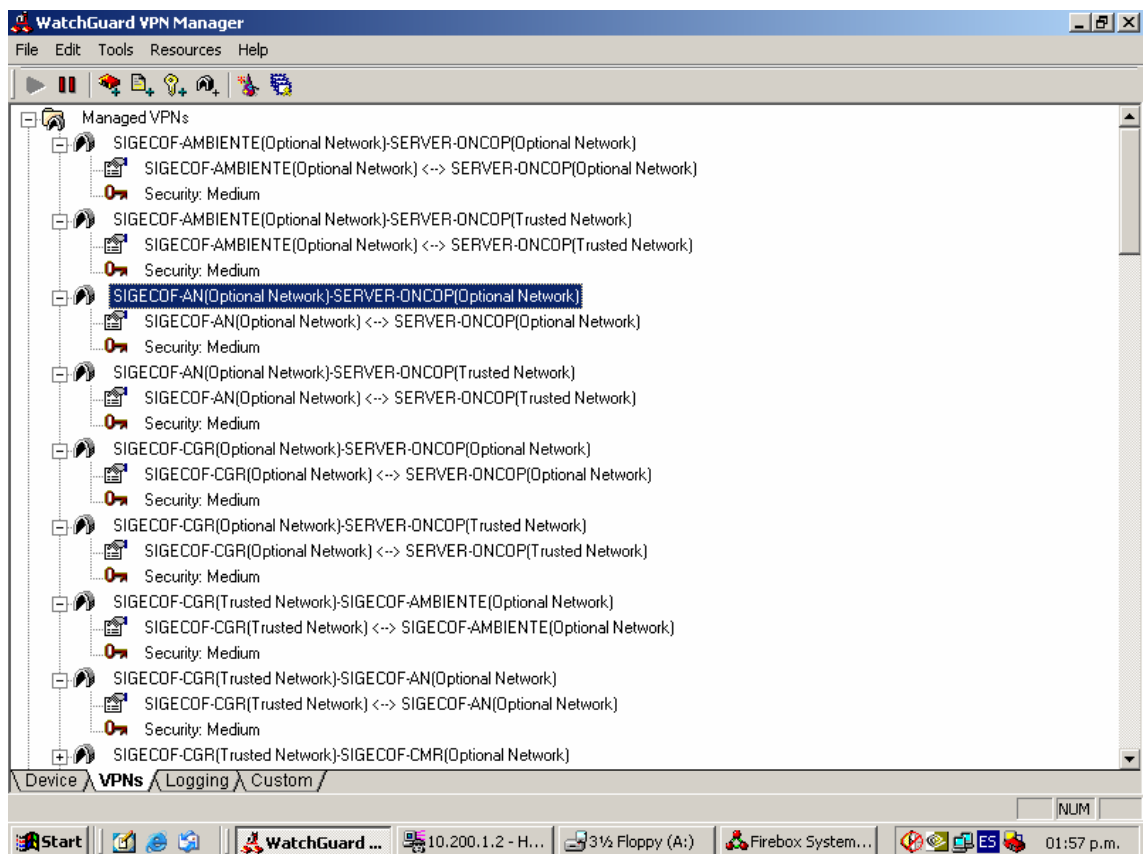


Figura 5.19. VPN creadas.

## 5. Pruebas de Servicios

Se realizaron las pruebas necesarias para verificar que todos los servicios involucrados en el proceso de la implantación de la nueva plataforma de Telecomunicaciones estuvieran operando satisfactoriamente. Entre las pruebas de funcionalidad que se realizaron tenemos:

- **Direccionamiento IP**

Verificación de la comunicación entre los segmentos de redes diferentes LAN, DMZ y WAN.

- **Ping:**

A través del comando ping se verificó la conexión a los Servidores Sigecof, enrutadores y dispositivos de seguridad, enviando paquetes de eco ICMP (Internet Control Message Protocol) a los componentes remotos, y registrando los paquetes de eco de respuesta.

Se estableció la prueba a los puertos seriales (Red WAN) de los equipos enrutadores tanto en la localidad principal como en las localidades remotas para verificar el enlace entre ambos nodos, de igual forma se verifico puerto fast-ethernet del router en la localidad remota.

El propósito de la prueba fue determinar fallas del enlace en los diferentes puntos del mismo.

En aquellos casos en que la prueba fue fallida se procedió a utilizar otro método de verificación para determinar en que punto presenta falla el enlace. El método utilizado en este caso fue el comando Trace, el cual se explica más adelante.

| PRUEBAS DE CONECTIVIDAD - PLATAFORMA FRAME RELAY                                                                                                                                                                                                                                                                                                   |                     |                     |        |                  |        |                            |        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|---------------------|--------|------------------|--------|----------------------------|--------|
| <b>Método utilizado: Ping.</b><br><b>Observaciones Equipo de Prueba:</b><br><b>1.- Dirección IP:</b> Perteneciente al Segmento de Red XX.XX.X.X (Interfaz Trusted del FW Ppla.)<br><b>2.- Default Gateway:</b> Dir. Ip de la Interfaz Trusted del FW Ppla.<br><b>3.- Resultado de la Prueba:</b> O.K. = Prueba Exitosa, <b>X</b> = Prueba Fallida. |                     |                     |        |                  |        |                            |        |
|                                                                                                                                                                                                                                                                                                                                                    | Localidad           | Localidad Principal | Prueba | Localidad Remota | Prueba | Puerto FastEthernet Router | Prueba |
| 1                                                                                                                                                                                                                                                                                                                                                  | Localidad Principal | XXX.XX.X.X          |        | XXX.XX.X.X       |        | XX.XXX.X.X                 |        |
| 2                                                                                                                                                                                                                                                                                                                                                  | Localidades Remotas | XXX.XX.X.X          |        | XXX.XX.X.X       |        | XX.XXX.X.X                 |        |

Tabla 5.16. Pruebas de conectividad método Ping.

---

- **Rastreo (Trace)**

Esta prueba fue hecha en aquellos casos en que la prueba anterior fue fallida, el propósito de la misma fue rastrear la ruta al equipo remoto a través de la red. Se verificó la ruta que todos los paquetes siguen desde el equipo de prueba ubicado en la localidad principal al equipo remoto.

Una vez determinada la falla, se procedió a verificar el equipo donde se perdían los paquetes, en este caso, los problemas encontrados eran de configuración de rutas en los router, los mismo fueron resueltos y posteriormente aplicada la prueba nuevamente.

- **VPN**

Una vez verificado el enlace se procedió a la configuración de las VPN, luego a la realización de pruebas de conexión mediante las redes privadas virtuales.

**Pruebas de Conectividad:**

Usuarios Sigecof → Servidores Sigecof.

Usuarios Sigecof → Centro de Atención al Usuario Sigecof

Usuarios ONCOP/Tesorería/Onapre → Servidores Sigecof

- **URL (Universal Resource Locator)**

Verificación del correcto funcionamiento del URL basado en protocolo HTTP (web) de las siguientes paginas del sistema SIGECOF:

A continuación algunos ejemplos de los URLs probados:

<http://mre-sigecof.mf.gov.ve>

<http://defensa-sigecof.mf.gov.ve>

<http://fgr-sigecof.mf.gov.ve>

<http://cgr-sigecof.mf.gov.ve>

<http://cne-sigecof.mf.gov.ve>

<http://desarrollo.mf.gov.ve>

<http://sigecof.mf.gov.ve>

- **Reglas de Protocolos**

Demostración del funcionamiento correcto de las reglas configuradas.

Demostración de cambios en la configuración mediante la adición, eliminación y modificación de las reglas.

---

## CONCLUSIONES

Todas las empresas deben dar una solución a sus necesidades de comunicación de datos, logrando una buena administración y seguridad de los mismos. Es por ello que la ONCOP ha actualizado su plataforma tecnológica a enlaces *Frame Relay* para proporcionar una integración en un único enlace, constituyendo hoy día la mejor tecnología para la transmisión de datos, mejorando la prestación de servicio, y optimizando el uso del ancho de banda de los enlaces dedicados contratados.

Al solicitar el servicio de *Frame Relay* a CANTV, se especificó detalladamente todos los parámetros: CIR, EIR, con el fin de establecer todos los beneficios de esta tecnología.

La implantación de una plataforma de seguridad para el acceso a los datos estudiada en este Trabajo de Grado ha permitido brindar una conexión eficiente con un intercambio de información confiable y seguro. Esto radica fundamentalmente en la instalación y configuración de un dispositivo de seguridad avanzado y a la definición de políticas de seguridad ajustadas a los requerimientos de la oficina.

Con la implementación de este dispositivo de seguridad se garantiza un uso más eficiente de la red, con el fin de monitorear el tráfico cursado e imponer restricciones de acceso a los usuarios.

Es importante mencionar que la implementación de esta plataforma se pudo aprovechar además para realizar reingeniería en muchos nodos donde los usuarios del Sistema estaban aislados de la red LAN del Organismo.

Esta nueva plataforma de comunicaciones permitirá tener un servicio gestionado extremo a extremo, es decir se podrá administrar, configurar, mantener y supervisar la red y los elementos de red durante las 24 horas del día.

Además se tiene flexibilidad de servicio, debido a que se pueden establecer múltiples Redes Privadas Virtuales entre los diferentes nodos de la red y entre las diferentes interfaces del firewall, es adaptable a necesidades cambiantes, permitiendo una fácil incorporación de nuevas sedes a esta red.

Los procesos realizados por la ONCOP, han mejorado en un 99 %, el tiempo de falla de los enlaces se ha reducido notablemente, y el proceso de respaldos de las Base de Datos se realiza en tiempos muchos menores a los que actualmente se venían realizando.

---

Adicionalmente a la seguridad y a las políticas implementadas cabe destacar el estudio y configuración de las VPN configuradas sobre los enlaces Frame Relay, ofreciendo la gran ventaja de permitirles a los usuarios una conexión segura y estable a través de un túnel en donde la información viajará encriptada.

Esta implantación de la plataforma tecnológica y el esquema de seguridad, permitirán optimizar al máximo las tareas a realizar a la ONCOP, con la finalidad de poder brindar los mejores servicios, con los mejores tiempos de respuesta y alta confiabilidad.

---

## RECOMENDACIONES

Si bien, se pudo observar todas las ventajas que traería esta implantación a nivel tecnológico es necesario tomar en cuenta las siguientes recomendaciones:

- La definición de políticas de seguridad y planes de contingencia que nos ayuden a prevenir posibles desastres o ataques externos.
- La ejecución de pruebas externas que simulen posibles ataques hacia la red privada, logrando identificar de manera precisa los huecos de seguridad que puedan existir.
- La actualización respectiva y al día del software de los equipos de seguridad utilizados. Para ello disponemos del Servicio de WatchGuard\_LiveSecurity, que nos mantiene al día con las actualizaciones respectivas y las vulnerabilidades detectadas en los equipos.
- El control y monitoreo periódico de la información suministrada por los archivos (log) del firewall que permitan detectar y corregir posibles vulnerabilidades del sistema.
- La ejecución de reportes periódicos utilizando el generador de Reportes de los Firewall para detectar posibles fallas o vulnerabilidades.

---

## GLOSARIO DE TERMINOS Y ABREVIATURAS

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AH</b>                  | Authentication Header. Cabecera de Autenticación. Modo de autenticación que se encarga de proporcionar soporte para la autenticación e integridad de datagramas IP. Su propósito es detectar alteraciones del contenido de un paquete y autenticar la identidad del que lo envía, bien como usuario o por su dirección IP.                                                                                                                                                                                                                                       |
| <b>Bc</b>                  | Committed Burst Size o ráfaga comprometida                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Be</b>                  | Excess Burst Size, o ráfaga en exceso                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>CAUS</b>                | Centro de Atención al Usuario SIGECOF                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>CIR</b>                 | Committed Information Rate, o tasa de información comprometida                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Circuitos Virtuales</b> | El concepto de circuito virtual se refiere a una asociación bidireccional, a través de la red, entre dos ETD (Equipo Terminal de Datos), circuito sobre el cual se realiza la transmisión de los paquetes. Al inicio, se requiere una fase de establecimiento de la conexión, denominado: "llamada virtual". Durante la llamada virtual los ETDs se preparan para el intercambio de paquetes y la red reserva los recursos necesarios para el circuito virtual. Los paquetes de datos contienen sólo el número del circuito virtual para identificar al destino. |
| <b>Datagrama IP</b>        | Forma de un paquete enviado por una interred TCP/IP. Cada datagrama tiene una cabecera que identifica tanto al transmisor como al receptor, seguida de datos.                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Dirección IP</b>        | (Dirección de protocolo de Internet). La forma estándar de identificar un equipo que está conectado a Internet, de forma similar a como un número de teléfono identifica un número de teléfono en una red telefónica. La dirección IP consta de cuatro números separados por puntos y cada número es menor de 256. El administrador del servidor Web o su proveedor de servicios de Internet asignará una dirección IP a su equipo.                                                                                                                              |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Encapsulamiento</b> | El encapsulamiento es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. El encapsulado consiste pues en ocultar los detalles de implementación de un objeto, pero a la vez se provee una interfaz pública por medio de sus operaciones permitidas. Considerando lo anterior también se define el encapsulado como la propiedad de los objetos de permitir el acceso a su estado únicamente a través de su interfaz o de relaciones preestablecidas con otros objetos. |
| <b>Encriptar</b>       | Técnica por la que la información se hace ilegible para terceras personas. Para poder acceder a ella es necesaria una clave que sólo conocen el emisor y el receptor. Se usa para evitar el robo de información sensible, como números de tarjetas de crédito.                                                                                                                                                                                                                                                                                                  |
| <b>Enrutador</b>       | Un enrutador es una computadora que se conecta a dos o más redes y reenvía paquetes de acuerdo con la información encontrada en su tabla de enrutamiento. Los enrutadores de la Ethernet ejecutan el protocolo IP.                                                                                                                                                                                                                                                                                                                                              |
| <b>Fibra óptica</b>    | Sistema de transmisión que utiliza fibra de vidrio como conductor de frecuencias de luz visible o infrarrojas. Este tipo de transmisión tiene la ventaja de que no se pierde casi energía pese a la distancia (la señal no se debilita) y que no le afectan las posibles interferencias electromagnéticas que sí afectan a la tecnología de cable de cobre clásica.                                                                                                                                                                                             |
| <b>Firewall</b>        | Mecanismo que permite que las comunicaciones entre una red local e Internet se realicen conforme a las políticas de seguridad de quien los instala. Estos sistemas suelen incorporar elementos que garantizan la privacidad, autenticación, etc., con lo que se impide el acceso no autorizado desde Internet.                                                                                                                                                                                                                                                  |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Frame Relay</b> | <p>Sistema de transmisión basado en la conmutación de paquetes. Tecnología eficiente de conmutación de paquetes que permite la entrega confiable de paquetes sobre circuito virtual (VC). Mucha de la funcionalidad de la capa de red se manipula en la capa de Enlace. Algunos de los conceptos usados en Frame Relay han sido incorporados en ATM.</p> <p>Estándar de la industria, protocolo de capa de enlace de datos con conmutación que maneja múltiples circuitos virtuales mediante una forma de encapsulamiento HDLC entre dispositivos conectados. Frame Relay es más eficiente que X.25, el protocolo para el cual se le considera generalmente un reemplazo.</p> |
| <b>Frames</b>      | Tramas. Estructura utilizada para encapsular los paquetes IP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>FTP</b>         | FTP son las siglas de File Transfer Protocol, el nombre del protocolo estándar de transferencia de ficheros. Su misión es permitir a los usuarios recibir y enviar ficheros de todas las máquinas que sean servidores FTP.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Gateway</b>     | Pasarela, puerta de acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un host a una red.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Hacker</b>      | Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el Fin de obtener información secreta.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>HTTP</b>        | Hiper Text Transfer Protocol). Protocola de transferencia de HiperTexto. Es el protocolo de Internet que permite que los exploradores del WWW recuperen información de los servidores.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>ICMP</b>        | (Internet Control Message Protocol). Protocolo de control de mensajes de interred. Protocolo usado por el IP para informar de errores y excepciones. El ICMP también incluye mensajes informativos usados por algunos programas como ping.                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Interface</b> | Interfaz. Conexión e interacción entre hardware, software y el usuario. El diseño y construcción de interfaces constituye una parte principal del trabajo de los ingenieros, programadores y consultores. Los usuarios "conversan" con el software. El software "conversa" con el hardware y otro software. El hardware "conversa" con otro hardware. Todo este "diálogo" no es más que el uso de interfaces. Las interfaces deben diseñarse, desarrollarse, probarse y rediseñarse; y con cada encarnación nace una nueva especificación que puede convertirse en un estándar más, de hecho o regulado. |
| <b>IPSec</b>     | Internet Protocol Security. Seguridad de Protocolo de Internet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>L2TP</b>      | Layer-2 Tunneling Protocol                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>LAN</b>       | Local Area Network. Red de Area Local. Red de computadoras ubicadas en El mismo ambiente, piso o edificio.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>NAT</b>       | Network Address Traslation. La técnica basada en la traducción de direcciones de red o NAT, así como su variante que permite la traducción adicional de los puertos, PAT (Port Address Traslation). Estas técnicas permiten no conocer desde el exterior las direcciones IP reales empleadas en la red interna, mostrando una visión particular y concreta de los sistemas y servicios visibles desde el exterior (direcciones IP y puertos). Por tanto, dificultarán la identificación y obtención de información de técnicas como footprinting.                                                        |
| <b>Nodo</b>      | Es el punto en donde se producen dos o más conexiones en una red de comunicaciones. No se trata de un elemento estrictamente físico, sino de una unidad funcional que exige hardware y software. Un nodo puede incluir controladores de comunicaciones, clusters, servidores, repetidores, etc.                                                                                                                                                                                                                                                                                                          |
| <b>ONCOP</b>     | Oficina Nacional de Contabilidad Pública                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>OOCP</b>      | Organismos Ordenadores de Compromisos y Pagos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OSI</b>                 | Siglas que significan Open Systems Interconnection o Interconexión de Sistemas Abiertos. Es un modelo o referente creado por la ISO para la interconexión en un contexto de sistemas abiertos. Se trata de un modelo de comunicaciones estándar entre los diferentes terminales y host. Las comunicaciones siguen unas pautas de siete niveles preestablecidos que son Físico, Enlace, Red, Transporte, Sesión, Presentación y Aplicación. |
| <b>Ping</b>                | (Packet Internet Groper) Proceso de verificación de la operatividad de una computadora o del buen funcionamiento de sus conexiones de red. Se realiza introduciendo el comando Ping 127.0.0.1, para verificar el propio pc, o introduciendo la IP del ordenador cuya comprobación deseamos hacer.                                                                                                                                          |
| <b>PLATINO</b>             | Plataforma Nacional de Información del Estado Venezolano                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>PPTP</b>                | Point-to-Point Tunneling Protocol                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Protocolo</b>           | Conjunto de reglas que posibilitan la transferencia de datos entre dos o más computadores.                                                                                                                                                                                                                                                                                                                                                 |
| <b>PVCs</b>                | Circuitos Virtuales Permanentes                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Red</b>                 | Se tiene una red cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.                                                                                                                                                                                                                                                                                                                                  |
| <b>Servidor (Hardware)</b> | Equipos centralizadores y de enlaces para la constitución de redes, de diferentes magnitudes, en interacción con PCs, routers, hubs, proxys, etc.                                                                                                                                                                                                                                                                                          |
| <b>SIGECOF</b>             | Sistema Integrado de Gestión y Control de la Finanzas Públicas                                                                                                                                                                                                                                                                                                                                                                             |
| <b>SVCs</b>                | Circuitos Virtuales Conmutados                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>TCP/IP</b>              | (Transmission Control Protocol/Internet Protocol). Se trata de un estándar de comunicaciones muy extendido y de uso muy frecuente para software de red basado en Unix con protocolos Token-Ring y Ethernet, entre otros.                                                                                                                                                                                                                   |
| <b>Telecomunicaciones</b>  | Transferencia de información entre dos puntos a distancia, a través de un medio guiado o no guiado, cuya propagación se realiza a través de ondas electromagnéticas.                                                                                                                                                                                                                                                                       |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Traceroute</b> | Toda red está caracterizada por una topología o distribución, tanto física como lógica, concreta. Existe una herramienta que ayuda a la obtención de ésta: traceroute, creada originalmente para solucionar problemas en una red. Esta técnica permite saber todos los sistemas existentes en un camino entre dos equipos.                                                                                                                                                                             |
| <b>Túnel</b>      | La tecnología de tuneles -Tunneling- es un modo de transferir datos entre 2 redes similares sobre una red intermedia. También se llama "encapsulación", a la tecnología de tuneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de tuneles VPN, añade otra dimensión al proceso de tuneles antes nombrado -encapsulación-, ya que los paquetes están encriptados de forma de los datos son ilegibles para los extraños. |
| <b>URL</b>        | Uniform Resource Locator. Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el World Wide Web. El url está conformado por el servicio (ejemplo: http://) más el nombre de la computadora (ejemplo: www.google.com) más el directorio y el archivo referido.                                                                                                                                                                                                 |
| <b>Virus</b>      | Programas muy sofisticados dedicados generalmente a causar un daño en la información o programas contenidos en un ordenador.                                                                                                                                                                                                                                                                                                                                                                           |
| <b>VPN</b>        | Virtual Private Network. Red Privada Virtual.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>WAN</b>        | Wide Area Network. Redes de Área Amplia. Es una red de computadoras de gran tamaño, dispersa por un país o incluso por todo el planeta.                                                                                                                                                                                                                                                                                                                                                                |

---

## BIBLIOGRAFIA

- Tanenbaum, A., **“Redes de Computadoras”**. Prentice-Hall Hispanoamericana, S.A. México 1997.
- Shaughnessy, T., **“Manual de Cisco”**. Osborne Mc Graw-Hill. España 2001.
- Commer, D., **“Redes Globales de Información con Internet y TCP/IP”**, Prentice Hall, 1996.
- Karanjit, S., y Chris, H., **“Firewalls y La Seguridad en Internet”**, Prentice Hall, 1997.
- Mansfield Richard, **“Defensa contra hackers: Protección de Información Privada”**, Anaya Multimedia, 2001.
- Huidobro, J.M., **“Redes y Servicios de Telecomunicaciones”**, Editorial Paraninfo - Thomson Learning, tercera edición. México 2000.
- Steve McQuerry, **“Interconnecting Cisco Network Devices”**, Cisco Press, 2000.
- H. Kim Lew, y Kevin Downes, **“Interconectividad. Manual para Resolución de Problemas”**, Prentice Hall, 2000.
- VV. AA., **“Manual de Trabajos de Grado de Especialización, Maestría y Tesis Doctorales”**, UPEL. Caracas 1998.
- Hernández, R., Fernández, C., Baptista, P., **“Metodología de la Investigación”**, Mc Graw-Hill. México 2000.
- Cheswick William R., Bellovin Steven M., Rubin Aviel D., **“Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition”**, Published by Addison Wesley Professional, 2003.
- Cocho Julian Marcelo, **“Riesgo y Seguridad de los Sistemas Informáticos”**, Universidad Politécnica de Valencia, 2003.
- Goncalves Marcus, **“Manual de Firewalls”**, McGraw-Hill, 2002
- Zwicky Elizabeth D., Cooper Simon D. and Chapman Brent, Building Internet Firewalls, Second Edition, Published by O'Reilly & Associates, 2000.
- Mendillo, V., **Seguridad Informática y Comunicaciones**, UCV, 2003.
- WatchGuard Firebox System, **“User Guide”**, 2004
- WatchGuard Firebox System, **“VPN Guide”**, 2004

---

## FUENTES ELECTRONICAS

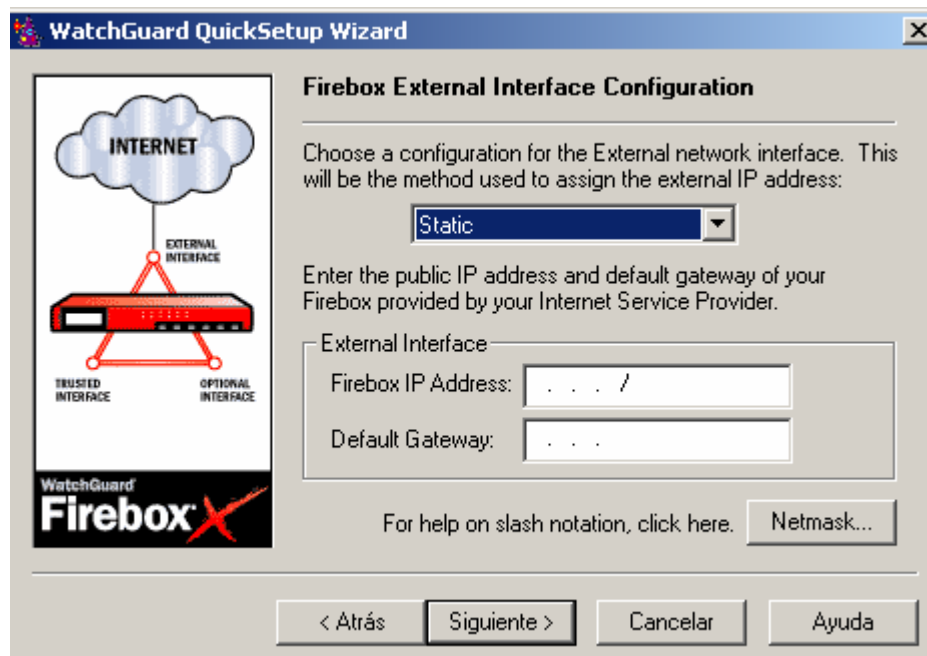
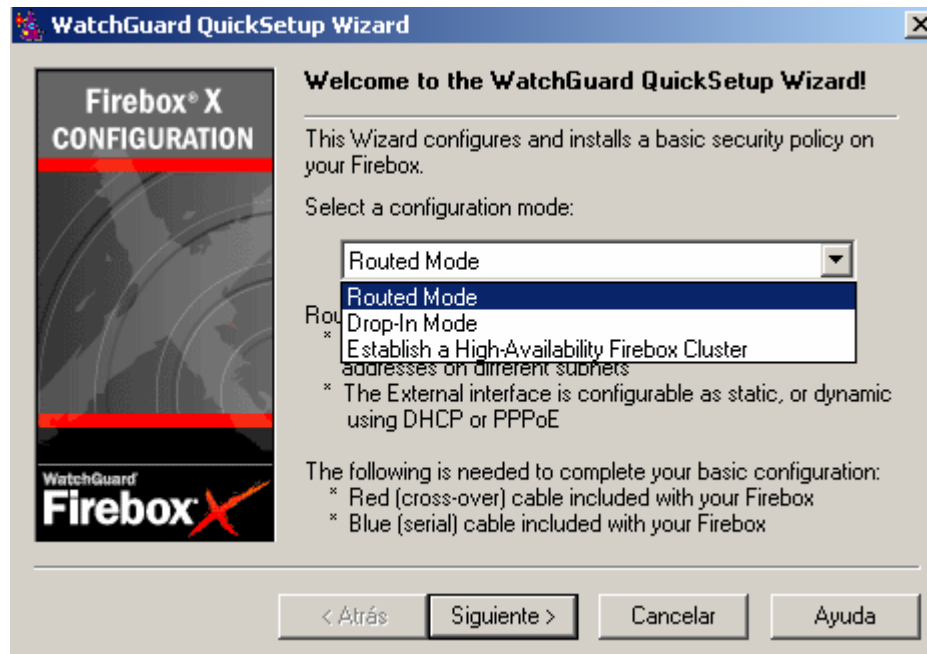
- <http://www.cisco.com/>
- <http://www.pc-news.com/>
- <http://www.firewall.com/>
- <http://www.redesafull.com.ar/>
- <http://www.watchguard.com/>
- <http://www.viared.cl/firewallwg.htm/>
- <http://www.ajoomal.com/>
- <http://www.g2security.com/>
- <http://www.eitd.net/>
- <http://www.monografias.com/>
- <http://www.ciac.org>
- <http://www.ibw.com.ni/~alanb/frame-relay/cfr3.htm>

---

## **ANEXOS**

## ANEXO 1: Configuración del Firewall WatchGuard

Muestra de algunas pantallas principales de la configuración del Firewall WatchGuard.



**WatchGuard QuickSetup Wizard**

### Firebox Internal Interface Configuration

Enter the IP addresses for the Firebox Trusted and Optional interfaces. These should be IP addresses on your internal private network and will act as the default gateway to computers behind the trusted and optional interfaces.

Trusted Interface:

Optional Interface:

☒ I have an additional private network behind my Firebox Trusted interface

Secondary Network:

For help on slash notation, click here [Netmask...](#)

< Atrás    Siguiente >    Cancelar    Ayuda

**WatchGuard QuickSetup Wizard**

### Configure Public Servers

Enter the IP address for each of your public servers. If you do not have any public servers, leave the checkboxes empty.

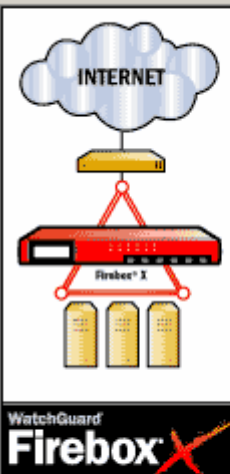
☐ I have an SMTP server behind my Firebox:

☐ I have an HTTP server on the Optional interface:

☐ I have an FTP server on the Optional interface:

< Atrás    Siguiente >    Cancelar    Ayuda

**WatchGuard QuickSetup Wizard**



**Create Firebox Access Passphrases**

The status passphrase is used to establish read-only connections to your Firebox.

Status Passphrase:

Retype Passphrase:

The configuration passphrase is used to establish read/write connections to your Firebox.

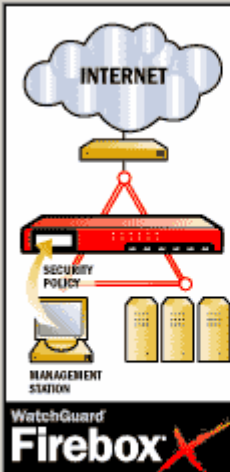
Configuration Passphrase:

Retype Passphrase:

\* Passphrases must be at least 7 characters long.

< Atrás    Siguiente >    Cancelar    Ayuda

**WatchGuard QuickSetup Wizard**



**Select Connection Method**

Firebox connection method:

Connect the red (cross-over) ethernet cable to this computer and the Trusted interface of your Firebox.

Connect the blue serial cable from this computer to the Firebox and select the appropriate serial port:

Enter an unused IP address on the same subnet as this computer. This will be temporarily assigned to the Firebox in order to upload your configuration.

Temporary IP Address:

After confirming your configuration, you will be prompted to turn on the power to your Firebox.

< Atrás    Siguiente >    Cancelar    Ayuda

**Configuring Firebox**

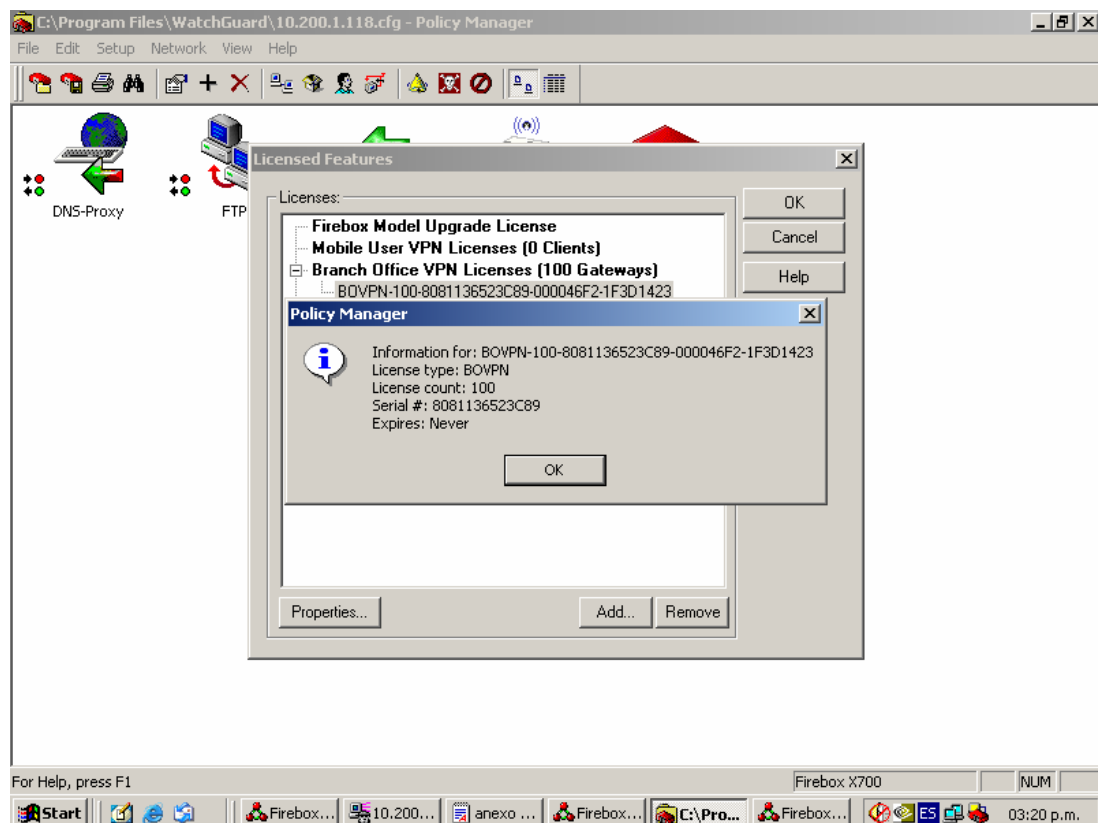
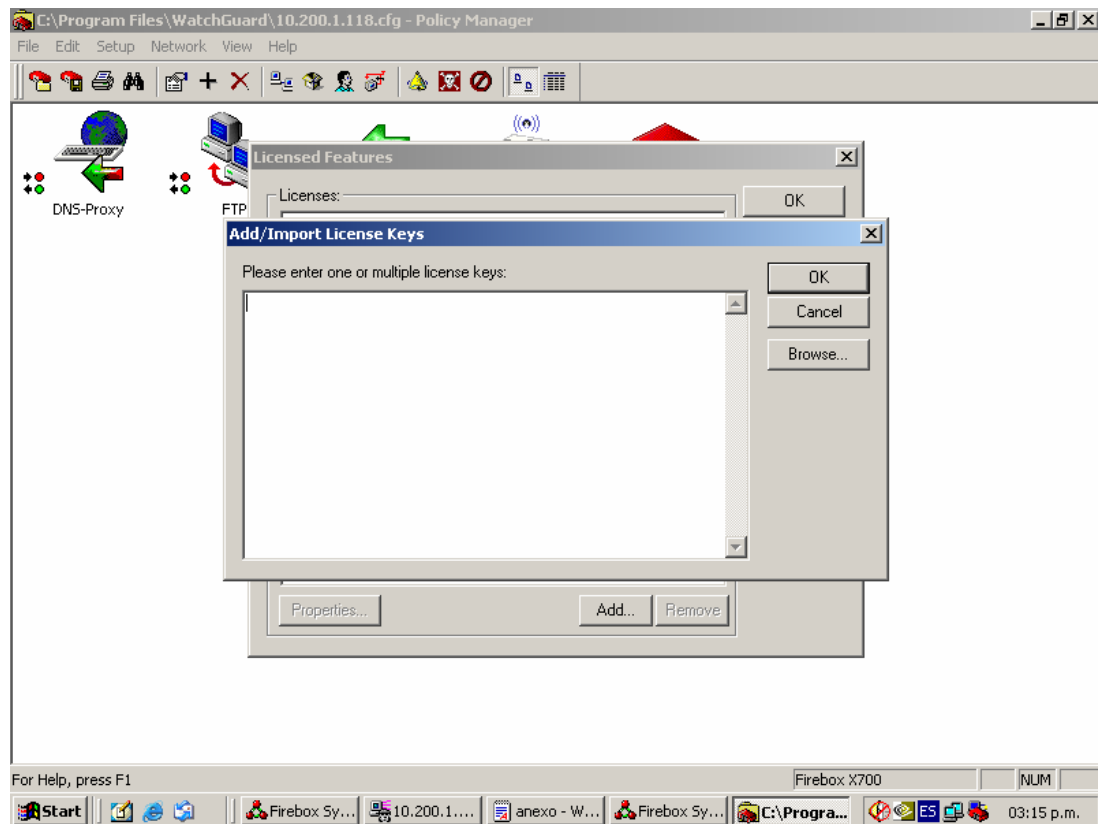


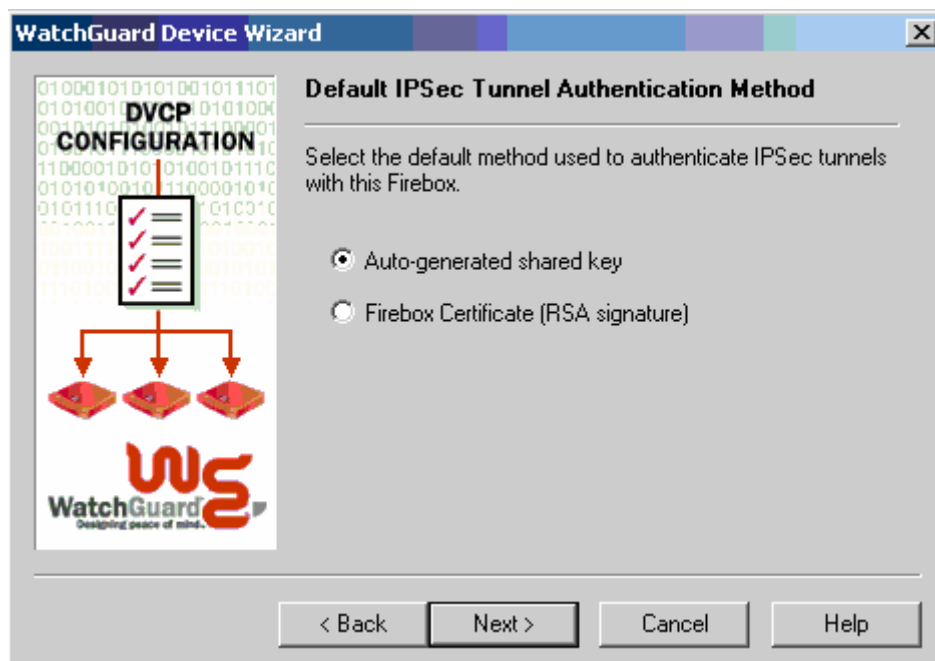
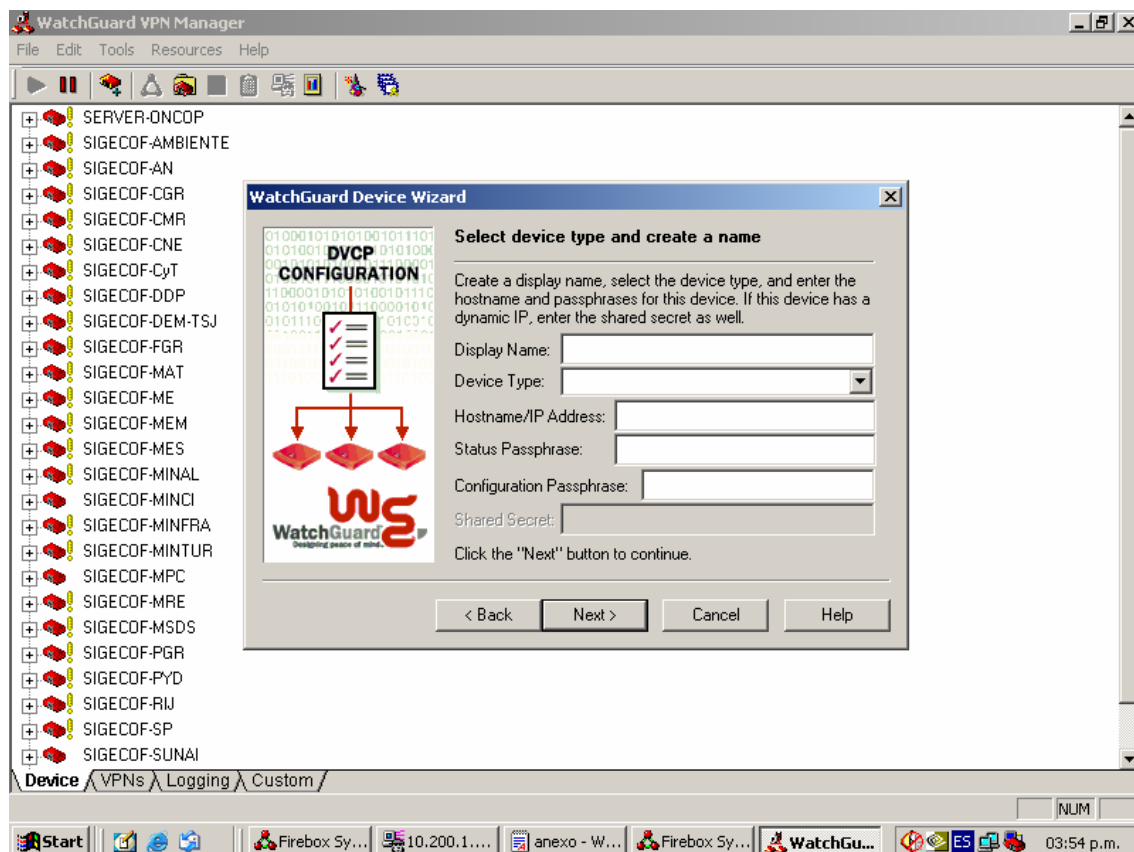
Status: Turn on your Firebox now. Waiting...

Cancel

## ANEXO 2: Pantallas Principales de Configuración de Túnel VPN

Muestra de algunas pantallas principales de la creación de los Túneles VPN en el Firewall WatchGuard.





**WatchGuard Device Wizard**



**DVCP CONFIGURATION**

### DNS and WINS settings for DHCP

This page allows you to specify DNS and WINS servers that you want remote tunnels to use when configuring their DHCP settings.

WINS (Windows Internet Name Service) Servers:

Primary:  Secondary:

DNS (Domain Name System) Servers:

Primary:  Secondary:

Domain Name:

Click the "Next" button to continue.

< Back   Next >   Cancel   Help

**WatchGuard Device Wizard**



**DVCP CONFIGURATION**

### Select Contact Information For This Device.

Select a contact information record from this list below for this device. If there aren't any records, you may add them here.

Fernando Zerpa

Add...   Edit...   Remove

Click the "Next" button to continue.

< Back   Next >   Cancel   Help



