

## **TRABAJO ESPECIAL DE GRADO**

**“APLICACIÓN DE UN ACCESO REMOTO DESDE CUALQUIER PC CON ACCESO A INTERNET, AL TERMINAL DE DISTRIBUCIÓN ÓPTICO (ODF), UBICADO EN EL CNT DE CANTV, PARA MEJORAR LOS TIEMPOS DE RESPUESTA DEL SISTEMA DE DETECCIÓN DE FALLAS EN LA RED DE FIBRA ÓPTICA DE LA REGIÓN CAPITAL”.**

Presentado ante la ilustre  
Universidad Central de Venezuela  
Por el Br. Suárez M., Gabriel A.  
Para optar al título de  
Ingeniero Electricista

Caracas, 2008

## **TRABAJO ESPECIAL DE GRADO**

**“APLICACIÓN DE UN ACCESO REMOTO DESDE CUALQUIER PC CON ACCESO A INTERNET, AL TERMINAL DE DISTRIBUCIÓN ÓPTICO (ODF), UBICADO EN EL CNT DE CANTV, PARA MEJORAR LOS TIEMPOS DE RESPUESTA DEL SISTEMA DE DETECCIÓN DE FALLAS EN LA RED DE FIBRA ÓPTICA DE LA REGIÓN CAPITAL”.**

Prof. Guía: Ing. Carolina Regoli  
Tutor Industrial: Ing. Robin Alonzo

Presentado ante la ilustre  
Universidad Central de Venezuela  
Por el Br. Suárez M., Gabriel A.  
Para optar al título de  
Ingeniero Electricista

Caracas, 2008



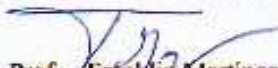
### CONSTANCIA DE APROBACIÓN


Caracas, 10 de junio de 2008


Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Gabriel Suárez, titulado:

**“APLICACIÓN DE UN ACCESO REMOTO DESDE CUALQUIER PC CON ACCESO A INTERNET, AL TERMINAL DE DISTRIBUCIÓN ÓPTICO (ODF) UBICADO EN EL CNT DE CANTV, PARA MEJORAR LOS TIEMPOS DE RESPUESTA DEL SISTEMA DE DETECCIÓN DE FALLAS EN LA RED DE FIBRA ÓPTICA DE LA REGIÓN CAPITAL”**

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

  
Prof. Franklin Martínez  
Jurado

  
Prof. Zeldivar Bruzual  
Jurado

  
Prof. Carolina Regoli  
Prof. Guin



## **DEDICATORIA**

A Dios, por estar presente en cada momento de mi vida y bendecir cada uno de mis logros.

A mi madre, por haberme regalado el don de la vida, por su sencillez, honradez y trabajo, quien me ha guiado desde mis primeros pasos a lo largo de mi formación personal y profesional. A mi familia en especial a mis tías Narcisa, Rita, Doris e Irene por su ayuda incondicional.

Gabriel A. Suárez.

## **RECONOCIMIENTOS Y AGRADECIMIENTOS**

A la **UNIVERSIDAD CENTRAL DE VENEZUELA**, por ser mi casa de estudios y a todos los profesores por su apoyo incondicional y toda la orientación prestada.

A mi tutora Profesora **CAROLINA REGOLI**, por todo su tiempo e interés y asesoría en la realización de este trabajo de grado.

A la empresa CANTV por darme la oportunidad de hacer mis pasantías, gracias por toda la colaboración prestada.

A mis compañeros de estudio, quienes de alguna manera u otra siempre estuvieron dispuestos a prestar su colaboración.

Y por último pero no menos importante, a **IYIRUBA ANCELMO**, por su paciencia, cariño, sabiduría y amor.

**Suárez M., Gabriel A.**

**APLICACIÓN DE UN ACCESO REMOTO DESDE CUALQUIER PC CON ACCESO A INTERNET, AL TERMINAL DE DISTRIBUCIÓN ÓPTICO (ODF), UBICADO EN EL CNT DE CANTV, PARA MEJORAR LOS TIEMPOS DE RESPUESTA DEL SISTEMA DE DETECCIÓN DE FALLAS EN LA RED DE FIBRA ÓPTICA DE LA REGIÓN CAPITAL.**

**Profesor Guía: Carolina Regoli. Tutor Industrial: Robin Alonzo. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: Compañía Anónima Nacional Teléfonos de Venezuela. Trabajo de Grado. 2008. 82 hojas + anexos**

**Palabras Claves:** Fibra óptica, Acceso Remoto, Servidor Web, Página Web, Red LAN, Seguridad de Redes.

**Resumen.** Se realizó este proyecto con el fin de el monitorear de las fibras ópticas interurbanas de la empresa CANTV de forma remota para determinar el lugar geográfico de la falla en caso de corte en las fibras, para ello se debe controlar el analizador de fibras (OTDR) desde un computador servidor que pueda ser accedido remotamente desde cualquier otra computadora que se encuentre en la red LAN de la empresa. Se hicieron las configuraciones al servidor, además se efectuaron pruebas de conectividad correspondientes, también se efectuaron los análisis correspondientes a la seguridad en la red y se determinó la forma más segura para acceder al servidor con las pruebas y ataques para encontrar vulnerabilidades en la red y en el servidor y corregir las fallas. Se diseñó la interfaz que controla el *switch* mecánico que se encarga de seleccionar el recorrido de fibra a ser analizado. Adicionalmente se migró la base de datos existente de los recorridos digitalizados de las fibras de Microsoft Access a MySQL. Por último se diseñó e implementó la interfaz amigable entre el usuario y el servidor para controlar remotamente de forma sencilla al analizador de fibra. El resultado obtenido es una página Web capaz de mostrar en un mapa de la región capital el lugar geográfico donde se encontraría cortada la fibra óptica seleccionada para el análisis. El servidor se configuró de forma que sea muy complicado para cualquier atacante infiltrarse y obtener de forma ilegal información tan delicada como las rutas digitalizadas de fibras interurbanas de la empresa CANTV

## INDICE GENERAL

CONSTANCIA DE APROBACION.....	ii
DEDICATORIA.....	iii
RECONOCIMIENTOS Y AGRADECIMIENTOS.....	iv
RESUMEN.....	v
INDICE GENERAL.....	vi
INDICE DE FIGURAS.....	ix
INDICES DE TABLAS.....	x
LISTA DE ACRONIMOS.....	xi
<b>INTRODUCCIÓN.....</b>	<b>xiii</b>
<b>CAPÍTULO I</b>	
<b>RESEÑA DEL PROYECTO.....</b>	<b>1</b>
1.1 Planteamiento del Problema.....	1
1.2 Antecedentes y Justificación.....	1
1.3 Objetivo General.....	2
1.4 Objetivos Específicos.....	3
1.5 Metodología.....	4
<b>CAPÍTULO II</b>	
<b>MARCO TEORICO.....</b>	<b>6</b>
2.1 Definición de fibra óptica.....	6
2.1.1 Características.....	6
2.1.2 Principio de funcionamiento.....	7
2.1.3. Tipos de fibra.....	7
2.1.3.1 Fibras multimodo.....	7

2.1.3.2 Fibra monomodo.....	8
2.1.4 Aplicaciones.....	8
2.1.4.1 Internet.....	8
2.1.4.2 Redes.....	9
2.1.4.3 Telefonía.....	11
2.2 Reflectómetro (OTDR).....	11
2.3 Sistema de Transmisión de Fibra Óptica de CANTV.....	12
2.4 Tipo de red.....	13
2.4.1 Redes punto a punto.....	13
2.4.2 Redes basadas en servidor.....	14
2.4.2.1 Clasificación de las redes cliente servidor.....	14
2.4.2.1.1 Redes de datos.....	14
2.4.3 Red de telefonía.....	17
2.5 Expansión y modernización de las redes de CANTV.....	17
2.5.1 Segmento de dispersión módulos.....	17
2.6 Protocolo modelo TCP-IP.....	19
2.6.1 El nivel físico.....	20
2.6.2 El nivel de enlace de datos.....	20
2.6.3 El nivel de Internet.....	20
2.6.4 El nivel de transporte.....	21
2.7 Protocolo de Red ETHERNET.....	21
2.7.1 CSMA/CD (Carrier Sense Multiple Access).....	21
2.8 Virtual Private Network (VPN).....	22
2.8.1 VPN de acceso remoto.....	22
2.9 Escritorio remoto de Windows.....	22
2.10 Página Web.....	22
2.10.1 Comportamiento dinámico.....	23
2.10.2 Visualización.....	23
2.11 Protocolo RS-232.....	25



2.12 Protocolo del puerto paralelo.....	27
2.12.1 Puerto de datos (Pin 2 al 9).....	27
2.12.2 Puerto de estado (Pin 15, 13, 12, 10 y 11).....	27
2.12.3 Puerto de control (Pin 1, 14, 16 y 17).....	28
2.13 Protocolo Frame Relay.....	28
2.13.1 Características.....	28

### **CAPITULO III**

<b>SOLUCIÓN PARA MEDICIÓN REMOTA DELAS FIBRAS ÓPTICAS.....</b>	<b>30</b>
3.1 Análisis de la red de acceso.....	30
3.1.1 Área <i>Backbone</i> (WAN).....	30
3.1.2 Área de Acceso (LAN).....	32
3.2 Búsqueda y levantamiento de información del OTDR.....	33
3.2.1 Características del OTDR.....	33
3.2.2 Parámetros de medición.....	34
3.3 Conexión a través del programa <i>hiperterminal</i> de Windows.....	35
3.3.1 Protocolo de conexión usado.....	35
3.3.2 Secuencia de transmisión del método directo.....	36
3.4 Conexión con el OTDR a través del programa PHP.....	37
3.5 Conexión remota al OTDR y seguridad del servidor.....	38
3.5.1 Conexión a través del escritorio remoto.....	38
3.5.2 Solución final crear una página Web.....	41
3.5.2.1. El fichero archivo httpd.conf. estructura del fichero principal de configuración del Apache.....	42
3.5.2.1.2 Proceso de autenticación.....	46
3.5.3 Configuración segura de puertos.....	48
3.6 Diseño del <i>switch</i> mecánico.....	51
3.6.1 Diseño de la parte mecánica del <i>switch</i> .....	52
3.6.2 Diseño del software de control del <i>switch</i> .....	54

3.6.3 Diseño del driver del <i>switch</i> .....	54
3.7 Diseño de la interfaz gráfica amigable.....	56
3.7.1 Introducción de las interfaces gráficas.....	56
3.7.2 Implementación de interfaz gráfica.....	57
<b>CAPITULO IV</b>	
<b>LEVANTAMIENTO Y PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA</b> .....	62
4.1 Conectividad del OTDR con el computador servidor.....	62
4.2 Conexión remota al OTDR.....	64
4.3 Conexión con el puerto serial a través del programa PHP.....	65
4.4 Pruebas de conectividad del servidor.....	68
4.5 Ataques al servidor para comprobar su seguridad.....	71
4.5.1 Determinación de sistemas vivos y escucha de puertos abiertos.....	71
4.5.2 Identificación de los servicios TCP y UDP que estén en ejecución.. ..	73
4.5.3 Ataques de enumeración.....	74
4.5.3.1 Contramedidas para ataques de enumeración.....	76
<b>CONCLUSIONES</b> .....	78
<b>RECOMENDACIONES</b> .....	80
<b>REFERENCIAS BIBLIOGRAFICAS</b> .....	81
<b>BIBLIOGRAFIA</b> .....	82
<b>ANEXOS</b> .....	83

## INDICE DE FIGURAS

Figura 2.1. Corte Transversal de la Fibra Óptica .....	7
Figura 2.2. Esquema de Transmisión con Fibra Óptica.....	13
Figura 2.3: Diagrama Esquemático de Red Telefónica Básica Fija.....	19
Figura 2.4: Esquema de los Pines del Puerto Paralelo.....	28
Figura 3.1: Interconexión de una LAN a la Red de <i>Switches</i> Frame Relay.....	31
Figura 3.2: Ejemplo de un Paquete Recorriendo la LAN de CANTV.....	32
Figura 3.3: (OTDR) Ejemplo de una reflectometría realizada.....	34
Figura 3.4: Formato del Mensaje Cuando se Usa el Método directo.....	36
Figura 3.5: Secuencia de Comunicación Entre el OTDR y la PC.....	36
Figura 3.6: Esquema de Atención de Peticiones del Servidor Apache.....	43
Figura 3.7: <i>Switch</i> Mecánico.....	52
Figura 3.8: Diagrama del Selenoide.....	53
Figura 3.9: Esquema del <i>Buffer</i> .....	54
Figura 3.10: Salida del <i>Buffer</i> .....	55
Figura 3.11: Salida del <i>Buffer</i> .....	55
Figura 3.12: Esquema del <i>buffer</i> .....	56
Figura 3.13: Esquema del Programa.....	58
Figura 3.14: Página de Inicio.....	59
Figura 3.15: Página de Transición.....	59
Figura 3.16: Página de Transición.....	60
Figura 3.17: Página que Muestra el Mapa Donde se Encuentra la Falla.....	60
Figura 4.1. Parámetros de Conexión del Puerto Serial.....	62
Figura 4.2: Configuración ASCII.....	63

Figura 4.3: Demostración con Hyperterminal de la Conexión con el OTDR.....	64
Figura 4.4: Ejemplo de Conexión con el Servidor.....	69
Figura 4.5: Página que Indica la Configuración por Defecto del Servidor.....	70
Figura 4.6: Página que Indica que No Se Realizo la Conexión con el Servidor...	71
Figura 4.7: Resultado del Comando Tracert.....	72
Figura 4.8: Resultado que Indica que el Sistema a Atacar Esta “Vivo”.....	72
Figura 4.9: Resultado del Comando Ping.....	73
Figura 4.10: Ejemplo de Sesión Nula.....	75
Figura 4.11: Resultado del Ataque de Enumeración.....	76
Figura 4.12: Resultado del Comando Netstat que Indica las Conexiones Activas del Servidor con Otras Maquinas.....	77

## INDICE DE TABLAS

Tabla 2.1 Características de los Pines del Puerto RS-232.....	25
Tabla 3.1: Secuencia para Mover el Motor a la Izquierda.....	52
Tabla 3.2: Secuencia para Mover el Motor a la Derecha.....	53

## LISTA DE ACRÓNIMOS

APD	Avalanche Photo Diode
BIGFON	Breitbandiges Integriertes Glasfaser-Fernmelde-Ortsnetz
ASP	Active Server Pages
LAN	(Local Area Network
CANTV	Compañía Anónima de Teléfonos de Venezuela
IP	Internet Protocol
WAN	Wide Area Network
VoIP	Voice over Internet Protocol
IPTV	Internet Protocol Televisión
CNT	Centro Nacional de Telecomunicaciones
OTDR	Optical Time Domain Reflectometer
ODF	Distribuidor de Fibra Óptica
PC	Personal Computer
VPN	Virtual Private Network
TCP	Transfer Control Protocolo
SQL	Structured Query Language
LED	Light-emitting diode
PBX	Private Branch Exchange
IBFN	Integriertes BreitbandFernmeldeNetz
E/O	Electro-Óptico
O/E	Óptico-Eléctrico
PAN	Personal Area Network
CAN	Campus Area Network
MAN	Metropolitan Area Network

DQDB	Distributed Queue Dual Bus
TDMA	Time Division Multiple Access
ATM	Asynchronous Transfer mode
SDH	Synchronous Digital Hierarchy
SLIP	Serial Line Internet Protocol
PPP	Point-to-Point Protocol
HDLC	High-Level Data Link Control
SDLC	Synchronous Data Link Controller
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
HTML	HyperText Markup Language
WWW	World Wide Web
HTTP	Hypertext Transfer Protocol
JSP	JavaServer Pages
IRQ	IRQ Interrupt ReQuest
RTS/CTS	Request to Send / Clear to Send
BIT	Bynary Digit
MBPS	Mega Bits Per Second
OSI	Open System Interconnection
RDSI	Red Digital de Servicios Integrados
DTE	Data Terminal Equipment
DCE	Data Communication Equipment
ICA	<i>- Independent Computing Arquitectura</i>
RDP	<i>Remote Desktop Protocol</i>
AIP	<i>Adaptive Internet Protocol</i>
VNC	<i>Virtual Network Computing</i>
DSL	Digital Subscriber Line

DoS	Denial of Service
IPsec	<i>Internet Protocol Security</i>
URL	Uniform Resource Locator
MD5	Message-Digest Algorithm 5
UDP	User Datagram Protocol
SMB	<i>(Server Message Block).</i>



## INTRODUCCIÓN

CANTV se inició como una empresa proveedora de servicios de Telecomunicaciones en Venezuela y, siendo pionera en este ámbito es, actualmente, la más grande en su ramo.

En sus inicios la telefonía básica fue su función primordial. Hoy en día la red de CANTV pone a disposición de los usuarios voz y datos a gran velocidad, en tanto que las empresas de televisión han aprovechado dicha tecnología para obtener señales de video en sitios remotos del país.

Vale decir que, si dicha red no tuviese un *backbone* y equipos que soporten gran ancho de banda, estos servicios serían imposibles. En tal sentido, la red de fibra óptica es imprescindible para el sistema de telecomunicaciones de Venezuela. Es de hacer notar que su mantenimiento y monitoreo constante revisten especial importancia, sobre todo en lo que se refiere a una rápida respuesta en el caso de una falla.

Por otra parte, la red de CANTV se basa principalmente en la conmutación entre centrales para llevar la información (voz, datos y video) al sitio que la requiera. Esta conmutación no podría efectuarse sin un sistema que soporte un gran ancho de banda, tanto en la capa de enlace, como en la capa física.

Asimismo, con el auge del protocolo IP (que actúa en la capa de red), los *routers* deben disponer de gran capacidad de procesamiento, para atender la creciente demanda por información del mercado venezolano.

Es así como, en un mayor nivel de detalle, se observa que la capa física, encargada de hacer la conexión a nivel troncal entre las centrales, constituye la fibra óptica en casi el 100 % de todo el territorio nacional. En ella hay cobre, pero éste ya está siendo reemplazando por dicha fibra. El motivo es que este medio guiado no presenta limitaciones teóricas en el ancho de banda, permitiendo mayor cantidad de

canales de voz y ancho de banda para las WAN y LAN.

Además de lo mencionado, se puede ofrecer gran cantidad de servicios como: educación a distancia, tele-conferencias, telefonía IP (VoIP), video a través de Internet (IPTV), etc., esto nos da una idea de la importancia de la capa física y de la fibra óptica en la red de CANTV

El propósito de este proyecto es disminuir los tiempos de respuesta del sistema de detección de fallas al mínimo. Para ello, se evita que los empleados encargados del mantenimiento de la fibra óptica realicen las mediciones pertinentes en el CNT (Centro Nacional de Telecomunicaciones), para luego dirigirse al sitio de la falla. Esto se logra cuando, desde el computador más cercano con acceso a Internet, se localizan las fallas que permiten ir de inmediato al sitio (lugar geográfico), sin tener que ir al CNT. Esto **ahorrará valioso tiempo en la reparación de los cortes en la fibra**, y traerá un gran beneficio para los usuarios en lugares donde no se disponga de respaldo de otras rutas entre centrales.

# **CAPITULO I**

## **Reseña del proyecto**

### **1.1 Planteamiento del Problema.**

CANTV es la principal y más grande empresa de telecomunicaciones de Venezuela, por sus redes de transporte transita toda la información del país, dichas redes utilizan la fibra óptica como *backbone* entre centrales para garantizar la prestación de todos los servicios a sus clientes, tanto empresas como a usuarios (vos, dato y video).

Al no disponer de un sistema REMOTO de MEDICIÓN en caso de corte en la fibra óptica, los tiempos de respuesta a este problema son demasiados extensos para ser tolerados por la empresa CANTV, porque en el peor de los casos hay que suspenderles el servicio a los usuarios.

### **1.2 Antecedentes y Justificación**

El presente proyecto se viene llevando a cabo en todo el mundo. Tener un sistema remoto de medición de fallas en la fibra óptica es necesario para reducir los tiempos de respuesta de la reparación y evitar pérdidas cuantiosas a raíz del reporte de una eventual caída del servicio. Este tipo de eventualidades genera impactos negativos en los ingresos (\$376'000.000 por 24 horas de falla en el servicio, i.e.) para las empresas, por demoras en la restauración del servicio de comunicación. Esto hace necesario disponer de herramientas que permitan la detección de fallas y revisión constante del enlace óptico.

Como ejemplo, considérese la empresa norteamericana *fiberzone Network*, una compañía que ofrece servicio de mantenimiento en las redes de fibra óptica ya instaladas en las premisas del usuario, por lo que debe disponer de un servicio capaz de responder rápidamente a las fallas en la fibra. Esta empresa dispone de un servicio

de monitoreo y medición remota en las fibras que componen esta red entre otros.

Actualmente, el personal encargado del mantenimiento y monitoreo de la red de fibra óptica de CANTV debe estar presente en la sala de transmisión del CNT, para realizar mediciones en la fibra, conectando manualmente el aparato medidor u OTDR (*Optical Time Domain Reflectometer*) al ODF (Terminal de Distribución Óptico), obtener los datos del OTDR (vía *disket*), ingresarlos a la computadora y, por último, estos datos son procesados por un software desarrollado en CANTV, llamado WHERE, que ubica el lugar de la falla en un mapa de Caracas .

El propósito de este proyecto es mejorar este sistema, dotando a los empleados de un mecanismo remoto que permita obtener la información de la falla desde cualquier computador que tenga acceso a Internet. Esto se logra siguiendo los siguientes pasos o fases de los que consta este trabajo:

- Desarrollar una interfaz entre el OTDR y el ODF que permita seleccionar el puerto que se requiera para la medición con el OTDR (proveyendo de un mecanismo del cual no se disponía anteriormente, y que, a la vez sea más económico que la solución tradicional: un *switch* óptico)
- Desarrollar una interfaz gráfica que permita controlar el OTDR con el PC-servidor ubicado en la sala de transmisión
- Encontrar una forma de controlar el PC- servidor desde cualquier computador que tenga acceso a Internet.

### **1.3 Objetivo General**

Implementar un acceso remoto desde cualquier PC con acceso a Internet, al Terminal de Distribución Óptico (ODF), ubicado en el CNT de CANTV, para mejorar los tiempos de respuesta del sistema de detección de fallas en la red de fibra óptica de la región capital.

#### **1.4 Objetivos Específicos**

**Recopilar información de todos los elementos del proyecto**, al hacer estudio previo de los siguientes tópicos:

- La estructura de la red de acceso de la empresa,
- Posibles ataques a dicha red y estudiar los protocolos de seguridad pertinentes en la capa de red,
- Seguridad en las redes, para implementar servidores de seguridad en la capa de aplicación
- Configurar servidores con el programa Apache, en donde se alojara el programa Where.
- Los diversos métodos de conexión remota,
- Información del protocolo de comunicación RS-232c para comunicación con el puerto serial
- Documentación sobre el lenguaje PHP con el cual se realizará la interfaz amigable entre usuario y PC (programa Where).

**Interconectar el OTDR al PC servidor**, analizando los protocolos de comunicación del OTDR Anritsu 9760, para realizar la conexión al PC servidor

**Analizar la red de acceso al PC servidor**, estudiando la estructura de la red de acceso LAN y WAN, para implementar protocolos de acceso y seguridad adecuados en la capa de red.

**Analizar e implementar el método de acceso remoto**, al hacer un estudio para escoger entre diversos métodos de conexión remota (red privada virtual (VPN), a través de una página Web, escritorio remoto) e implementarlo.

**Desarrollar una interfaz amigable entre el usuario y la PC**, al migrar el programa WHERE de visual Basic a PHP.

**Diseñar la interfaz entre el OTDR y el ODF**, al diseñar el controlador de un *switch* mecánico, utilizado para seleccionar el recorrido de fibra óptica a ser medido

## **1.5 Metodología**

### **Fase 1**

**Estudios previos.** Se obtuvo información de los protocolos de comunicación RS-232c, TCP-IP, protocolos de seguridad en la red; configuración de servidores, dominio en Windows, teoría sobre fibra óptica, programación en PHP y en lenguaje C++.

### **Fase 2**

**Análisis de tecnología y protocolos asociados.** Se realizó un asentamiento de la información obtenida, basándose en los requerimientos, las especificaciones técnicas y funcionales asociados a los elementos del proyecto.

### **Fase 3**

**Desarrollo e implementación del proyecto.** Se Interconectó el OTDR con la computadora servidor. Se realizó mediante el conocimiento del protocolo RS-232, luego se probó la conexión del el equipo medidor de fibra óptica con el Hyperterminal de Windows XP; al haber establecido la conexión con estos dos equipos se procedió a interconectarlo con un lenguaje de bajo nivel. (PHP y C++)

Se configuró el computador servidor para alojar el programa: luego de recopilar información del programa Apache, se procedió a configurar el servidor con dicho programa para empezar a hacer las pruebas con la red interna de CANTV y se comprobó que se tiene acceso al servidor desde otro computador.

Se migró la base de datos existente del programa Where de Visual Basic a MySQL: Se migró la Base de Datos a MySQL para hacerla compatible con el programa Apache.

Al hacer estos pasos, se recopiló información del lenguaje PHP y C++, para realizar el programa que controle el OTDR desde el servidor.

Para la realización del programa se siguieron los siguientes pasos.

**Análisis de los requerimientos:** Conectar el puerto serial del computador con el OTDR, acceso a la base de datos en MySQL, funcionamiento del programa como página Web.

**Desarrollo del programa:** una vez delimitados los requerimientos se procede al desarrollo con los lenguajes PHP y C++.

## **CAPITULO II**

### **Marco Teórico**

- **2.1 Definición de fibra óptica.**

La fibra óptica es un conductor de ondas en forma de filamento, generalmente de vidrio, aunque también puede ser de materiales plásticos. La fibra óptica es capaz de dirigir la luz a lo largo de su longitud usando la reflexión total interna. Normalmente la luz es emitida por un láser o un LED [1].

Las fibras son ampliamente utilizadas en telecomunicaciones, ya que permiten enviar gran cantidad de datos a gran velocidad, mayor que las comunicaciones de radio y cable. También se utilizan para redes locales. Son el medio de transmisión inmune a las interferencias por excelencia [1].

#### **2.1.1 Características**

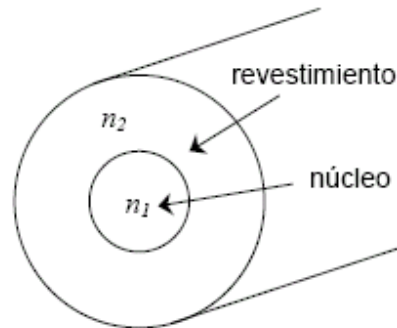
La fibra óptica es una guía de ondas dieléctrica que opera a frecuencias ópticas.

Cada filamento consta de un núcleo central de plástico o cristal (óxido de silicio y germanio) con un alto índice de refracción, rodeado de una capa de un material similar con un índice de refracción ligeramente menor. Cuando la luz llega a una superficie que limita con un índice de refracción menor, se refleja en gran parte, cuanto mayor sea la diferencia de índices y mayor el ángulo de incidencia, se habla entonces de reflexión interna total [1].

Así, en el interior de una fibra óptica, la luz se va reflejando contra las paredes en ángulos muy abiertos, de tal forma que prácticamente avanza por su centro. De este modo, se pueden guiar las señales luminosas sin pérdidas por largas distancias.



La figura 2.1 muestra un corte transversal de una fibra óptica.



**Figura 2.1. Corte transversal de la fibra óptica**

### **2.1.2 Principio de funcionamiento.**

Los principios básicos de funcionamiento se justifican aplicando las leyes de la óptica geométrica, principalmente, la ley de la refracción (principio de reflexión interna total) y la Ley De Snell [1].

Su funcionamiento se basa en transmitir por el núcleo de la fibra un haz de luz, tal que éste no atraviese el núcleo, sino que se refleje y se siga propagando. Esto se consigue si el índice de refracción del núcleo es mayor al índice de refracción del revestimiento, y también si el ángulo de incidencia es superior al ángulo límite [1].

**2.1.3 Tipos de Fibra:** Las diferentes trayectorias que puede seguir un haz de luz en el interior de una fibra se denominan modos de propagación, y según el modo de propagación tendremos dos tipos de fibra óptica: multimodo y monomodo [1].

#### **2.1.3.1 Fibra multimodo**

Una fibra multimodo es aquella que puede propagar más de un modo de luz. Puede tener más de mil modos de propagación de luz. Las fibras multimodo se usan comúnmente en aplicaciones de corta distancia, menores a 1 Km.; es simple de diseñar y económico. Su distancia máxima es de 2 Km. y usa cañón láser de baja intensidad [1].

El núcleo de una fibra multimodo tiene un índice de refracción superior, pero del mismo orden de magnitud, que el revestimiento. Debido al gran tamaño del núcleo de una fibra multimodo, es más fácil de conectar y tiene una mayor tolerancia a componentes de menor precisión [1].

Dependiendo el tipo de índice de refracción del núcleo, tenemos dos tipos de fibra multimodo:

- Índice escalonado: En este tipo de fibra, el núcleo tiene un índice de refracción constante en toda la sección cilíndrica, tiene alta dispersión modal.

- Índice gradual: Mientras en este tipo, el índice de refracción no es constante, tiene menor dispersión modal y el núcleo se constituye de distintos materiales.

### **2.1.3.2 Fibra monomodo**

Una fibra monomodo es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación, su transmisión es en línea recta. Su distancia va desde 2.3 Km. a 100 Km. máximo y usa un *hub* con cañón láser de alta intensidad. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias y transmitir elevadas tasas de bit.

Las diferentes trayectorias que puede seguir un haz de luz en el interior de una fibra se denominan modos de propagación. Y según el modo de propagación tendremos dos tipos de fibra óptica: multimodo y monomodo.

## **2.1.4 Aplicaciones**

### **2.1.4.1 Internet**

El servicio de conexión a Internet por fibra óptica, derriba la mayor limitación del ciberespacio: su exasperante lentitud.

Para navegar por la red mundial de redes, Internet, no sólo se necesitan un computador, un módem y algunos programas, sino también una gran dosis de

paciencia. El ciberespacio es un mundo lento. Un usuario puede pasar varios minutos esperando a que se cargue una página o varias horas tratando de bajar un programa de la Red a su PC.

Esto se debe a que las líneas telefónicas, el medio que utiliza la mayoría de los 50 millones de usuarios para conectarse a Internet, no fueron creadas para transportar videos, gráficas, textos y todos los demás elementos que viajan de un lado a otro en la Red.

Pero las líneas telefónicas no son la única vía hacia el ciberespacio. Recientemente un servicio permite conectarse a Internet a través de la fibra óptica.

La fibra óptica hace posible navegar por Internet a una velocidad de dos millones de bps, impensable en el sistema convencional, en el que la mayoría de usuarios se conecta a 28.000 o 33.600 bps.

#### **2.1.4.2 Redes**

La fibra óptica se emplea cada vez más en la comunicación, debido a que las ondas de luz tienen una frecuencia alta y la capacidad de una señal para transportar información aumenta con la frecuencia. En las redes de comunicaciones se emplean sistemas de láser con fibra óptica. Hoy funcionan muchas redes de fibra para comunicación a larga distancia, que proporcionan conexiones transcontinentales y transoceánicas. Una ventaja de los sistemas de fibra óptica es la gran distancia que puede recorrer una señal antes de necesitar un repetidor para recuperar su intensidad. En la actualidad, los repetidores de fibra óptica están separados entre sí unos 100 Km., frente a aproximadamente 1,5 Km. en los sistemas eléctricos. Los amplificadores de fibra óptica recientemente desarrollados pueden aumentar todavía más esta distancia [1].

Otra aplicación cada vez más extendida de la fibra óptica son las redes de área local. Al contrario que las comunicaciones de larga distancia, estos sistemas conectan a una serie de abonados locales con equipos centralizados como computadoras o impresoras. Este sistema aumenta el rendimiento de los equipos y permite

fácilmente la incorporación a la red de nuevos usuarios. El desarrollo de nuevos componentes electroópticos y de óptica integrada aumentará aún más la capacidad de los sistemas de fibra [1].

Una red de área local o LAN, es un conjunto de computadores que pueden compartir datos, aplicaciones y recursos (por ejemplo impresoras). Las computadoras de una red de área local (LAN, *Local Area Network*) están separadas por distancias de hasta unos pocos kilómetros, y suelen usarse en oficinas o campus universitarios. Una LAN permite la transferencia rápida y eficaz de información en el seno de un grupo de usuarios y reduce los costes de explotación [1].

Otros recursos informáticos conectados son las redes de área amplia (WAN, *Wide Area Network*) o las centrales privadas (PBX). Las WAN son similares a las LAN, pero conectan entre sí computadores separados por distancias mayores, situados en distintos lugares de un país o en diferentes países; emplean equipo físico especializado y costoso y arriendan los servicios de comunicaciones. Las PBX proporcionan conexiones informáticas continuas para la transferencia de datos especializados como transmisiones telefónicas, pero no resultan adecuadas para emitir y recibir los picos de datos de corta duración empleados por la mayoría de las aplicaciones informáticas [1].

Las redes de comunicación públicas están divididas en diferentes niveles; conforme al funcionamiento, a la capacidad de transmisión y al alcance que definen. Por ejemplo, si está aproximándose desde el exterior hacia el interior de una gran ciudad, se tiene primeramente la red interurbana y red provisional, a continuación las líneas prolongadas a portadoras de tráfico de más baja capacidad procedente de áreas alejadas (red rural), hacia el centro la red urbana y finalmente las líneas de abonado. Los parámetros dictados por la práctica son el tramo de transmisión que es posible cubrir y la velocidad binaria específica así como el tipo de fibra óptica apropiado, es decir, cables con fibras monomodo o multimodo [1].

### 2.1.4.3 Telefonía

Con motivo de la normalización de interfaces existentes, se dispone de los sistemas de transmisión por fibra óptica para los niveles de la red de telecomunicaciones públicas en una amplia aplicación, contrariamente para sistemas de la red de abonado (línea de abonado), hay ante todo una serie de consideraciones.

Para la conexión de un teléfono es suficiente con los conductores de cobre existentes. Precisamente con la implantación de los servicios en banda ancha como la videoconferencia, la videotelefonía, etc, la fibra óptica se hará imprescindible para el abonado. Con el BIGFON (red urbana integrada de telecomunicaciones en banda ancha por fibra óptica) se han recopilado amplias experiencias en este aspecto. Según la estrategia elaborada, los servicios de banda ancha posteriormente se ampliarán con los servicios de distribución de radio y de televisión en una red de telecomunicaciones integrada en banda ancha (IBFN) [1].

- **2.2 Definición de Reflectómetro (OTDR):**

En telecomunicaciones, un **OTDR** (del inglés: *Optical Time Domain Reflectometer*) es un instrumento óptico-electrónico usado para caracterizar una fibra óptica.

Un OTDR inyecta en la fibra bajo análisis una serie de pulsos ópticos. También extrae, del mismo extremo de la fibra, luz que ha sido dispersada y reflejada de vuelta desde puntos de la fibra con un cambio en el índice de refracción.

Este dispositivo es el equivalente en óptica al Reflectómetro en el Dominio del Tiempo (TDR), que mide los cambios producidos en la impedancia de un cable. La intensidad del pulso devuelto, es integrada como una función del tiempo, y representada en función de la longitud de la fibra.

Un OTDR puede ser utilizado para estimar la longitud de la fibra, y su atenuación, incluyendo pérdidas por empalmes y conectores. También puede ser utilizado para detectar fallos, tales como roturas de la fibra.

Los parámetros que se varían para hacer mediciones son:

- Ancho del pulso.
- Distancia.
- Longitud de onda.
- *Averaging* (número de muestras por segundo).

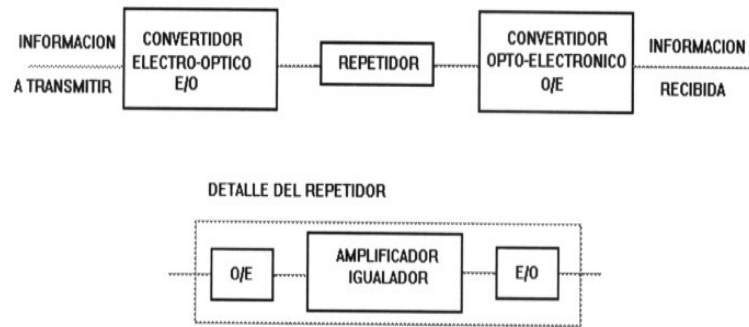
- **2.3 Sistema de transmisión de fibra Óptica de CANTV :**

Estos sistemas están compuestos por un transmisor, cuya misión es la de convertir la señal eléctrica en señal óptica susceptible de ser enviada a través de una fibra óptica. En el extremo opuesto de la fibra óptica se encuentra el receptor, cuya misión es la de convertir la señal óptica en señal eléctrica nuevamente. La figura 2 muestra el proceso de bloques del sistema de transmisión [2].

El transmisor puede emplear un LED o un diodo láser como elemento de salida. A estos elementos se los denomina conversores electro-ópticos (E/O).

El receptor consiste en un diodo PIN o un APD, que se acopla a la fibra óptica. Se le denomina convertidor opto-electrónico (O/E) [2].

El tipo de modulación utilizado es el de amplitud, modulando la intensidad de luz generada por el emisor. Las no linealidades de los emisores y receptores al convertir las señales eléctricas a ópticas y viceversa, así como las fuentes de ruido que se superponen a la señal en los sistemas típicos de fibra óptica hacen que este sistema sea especialmente apropiado para la transmisión de señales digitales, que corresponde a los estados de encendido-apagado del emisor. No obstante también es posible transmitir señales analógicas. La figura 2.2 muestra un esquema del sistema [2].



**Figura 2.2. Esquema de transmisión con fibra óptica**

Otros tipos de modulación, como modulación en frecuencia y demás sistemas coherentes están en fase de desarrollo, debido a la dificultad de obtener señales luminosas espectralmente puras y que al mismo tiempo puedan ser moduladas en frecuencia [2].

La señal óptica que se propaga a través de la fibra óptica se degrada por la atenuación y restricción al ancho de banda de la fibra, y entonces, es preciso regenerar la señal transmitida. El mejor método es tratar la señal en forma eléctrica. Por lo tanto, los conversores E/O y O/E son componentes indispensables en un repetidor óptico. El amplificador e igualador de la señal eléctrica son similares a los de los sistemas de transmisión convencionales [2].

- **2.4 Tipos de red**

- **2.4.1 Redes punto a Punto.**

En una red punto a punto cada computadora puede actuar como cliente y como servidor. Las redes punto a punto hacen que compartir datos y periféricos sea fácil para un pequeño grupo de gente. En un ambiente punto a punto, la seguridad es difícil, porque la administración no es centralizada.

## **2.4.2 Redes Basadas en servidor.**

Las redes basadas en servidor son mejores para compartir gran cantidad de recursos y datos. Un administrador supervisa la operación de la red, y vela que la seguridad sea mantenida. Este tipo de red puede tener uno o más servidores, dependiendo del volumen de tráfico, número de periféricos etc. Por ejemplo, puede haber un servidor de impresión, un servidor de comunicaciones, y un servidor de base de datos, todos en una misma red.

Como es sabido, las redes basadas en servidores son más eficientes para manejar redes grandes por ende este estudio se basará en éstas.

### **2.4.2.1 Clasificación de las Redes Cliente servidor.**

Existen varios tipos de redes, los cuales se clasifican de acuerdo a su tamaño y distribución lógica. CANTV maneja dos tipos de redes: datos y telefonía, y se clasifican de la siguiente forma.

#### **2.4.2.1.1 Redes de datos.**

**a) PAN (red de administración personal)** son redes pequeñas, las cuales están conformadas por no más de 8 equipos, por ejemplo: Los cibercafés.

**b) CAN: Campus Area Network, Red de Area Campus.** Una CAN es una colección de LANs dispersadas geográficamente dentro de un campus (universitario, oficinas de gobierno, maquilas o industrias) pertenecientes a una misma entidad en una área delimitada en kilómetros. Una CAN utiliza comúnmente tecnologías tales como FDDI y Gigabit Ethernet para conectividad a través de medios de comunicación tales como fibra óptica y espectro expandido.

**c) LAN (Local Area Network, redes de área local)** son las redes que todos conocemos, es decir, aquellas que se utilizan en nuestra empresa. Son redes pequeñas, entendiendo como pequeñas las redes de una oficina, de un edificio. Debido a sus limitadas dimensiones, son redes muy rápidas en las cuales cada estación se puede comunicar con el resto. Están restringidas en tamaño, lo cual significa que el tiempo



de transmisión, en el peor de los casos, se conoce. Además, simplifica la administración de la red.

Suelen emplear tecnología de difusión mediante un cable sencillo (coaxial o UTP) al que están conectadas todas las máquinas. Operan a velocidades entre 10 y 100 Mbps.

Características preponderantes:

- Los canales son propios de los usuarios o empresas.
- Los enlaces son líneas de alta velocidad.
- Las estaciones están cercas entre sí.
- Incrementan la eficiencia y productividad de los trabajos de oficinas al poder compartir información.
- Las tasas de error son menores que en las redes WAN.
- La arquitectura permite compartir recursos.

Las LAN muchas veces usan una tecnología de transmisión, dada por un simple cable, donde todas las computadoras están conectadas.

**d) WAN (Wide Area Network**, redes de área extensa) son redes punto a punto que interconectan países y continentes. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos. El alcance es una gran área geográfica, como por ejemplo: una ciudad o un continente. Está formada por una vasta cantidad de computadoras interconectadas (llamadas hosts), por medio de subredes de comunicación o subredes pequeñas, con el fin de ejecutar aplicaciones, programas, etc.

Una red de área extensa WAN es un sistema de interconexión de equipos informáticos geográficamente dispersos, incluso en continentes distintos. Las líneas utilizadas para realizar esta interconexión suelen ser parte de las redes públicas de transmisión de datos.

Las redes LAN comúnmente se conectan a redes WAN, con el objetivo de

tener acceso a mejores servicios, como por ejemplo a Internet. Las redes WAN son mucho más complejas, porque deben enrutar correctamente toda la información proveniente de las redes conectadas a ésta.

**MAN (Metropolitan Area Network,** redes de área metropolitana), comprenden una ubicación geográfica determinada "ciudad, municipio", y su distancia de cobertura es mayor de 4 km. Son redes con dos buses unidireccionales, cada uno de ellos es independiente del otro en cuanto a la transferencia de datos. Es básicamente una gran versión de LAN y usa una tecnología similar. Puede cubrir un grupo de oficinas de una misma corporación o ciudad, ésta puede ser pública o privada. El mecanismo para la resolución de conflictos en la transmisión de datos que usan las MANs, es DQDB (**Distributed queue dual bus**).

DQDB consiste en dos buses unidireccionales, en los cuales todas las estaciones están conectadas, cada bus tiene una cabecera y un fin. Cuando una computadora quiere transmitir a otra, si ésta está ubicada a la izquierda usa el bus de arriba, caso contrario el de abajo.

#### **2.4.2.1.2 Elementos de una red.**

**a) Líneas de transmisión:** Son las encargadas de llevar los bits entre los hosts.

**b) Elementos interruptores (routers):** Son computadoras especializadas usadas por dos o más líneas de transmisión. Para que un paquete llegue de un router a otro, generalmente debe pasar por routers intermedios, cada uno de estos lo recibe por una línea de entrada, lo almacena y cuando una línea de salida está libre, lo retransmite.

**c) INTERNET WORKS:** Es una colección de redes interconectadas, cada una de ellas puede estar desarrollada sobre diferentes software y hardware. Una forma típica de Internet Works es un grupo de redes LANs conectadas con WANs. Si a una subred le sumamos los *host* obtenemos una red. El conjunto de redes mundiales es lo

que conocemos como Internet.

**2.4.3 Red de telefonía:** La red de telefonía es digital entre las centrales, utiliza tecnología TDMA para enviar las tramas a través de E1, desde las centrales hasta el abonado la red sigue siendo analógica.

- **2.5 Expansión y Modernización de las Redes de CANTV.**

Durante los primeros seis años como empresa privada, se emprende la expansión y modernización de las redes de voz y datos, fijas y móviles; gracias a la mayor inversión de capital que una empresa privada haya realizado en el país: más de 3.000 millones de dólares. Esta novedosa plataforma tecnológica, que cubre todo el territorio nacional, permite atender la creciente demanda de telecomunicaciones de los venezolanos, gracias a su actualización permanente, como ocurrió posteriormente con la red de Movilnet [3].

En efecto, se construyen 1.981 kilómetros del más importante proyecto de CANTV para este período: el sistema de fibra óptica interurbana, el cual permitiría la interconexión de las principales ciudades del país a la plataforma de telecomunicaciones más avanzada y confiable existente en Latinoamérica [3].

Se pone en servicio la primera fase de la red ATM/Frame Relay para la transmisión de datos y video a gran velocidad, y se inicia la conversión de la plataforma en red inteligente. Actualmente, el 99 por ciento de las centrales están interconectadas a través de fibra óptica [3].

**2.5.1 Segmento de Dispersión de Módulos.**

- Módulo de Acceso
- Módulo de Conmutación
- Módulo Troncal

El Módulo de Acceso está integrado por segmentos de red en cable de cobre o de fibra óptica:

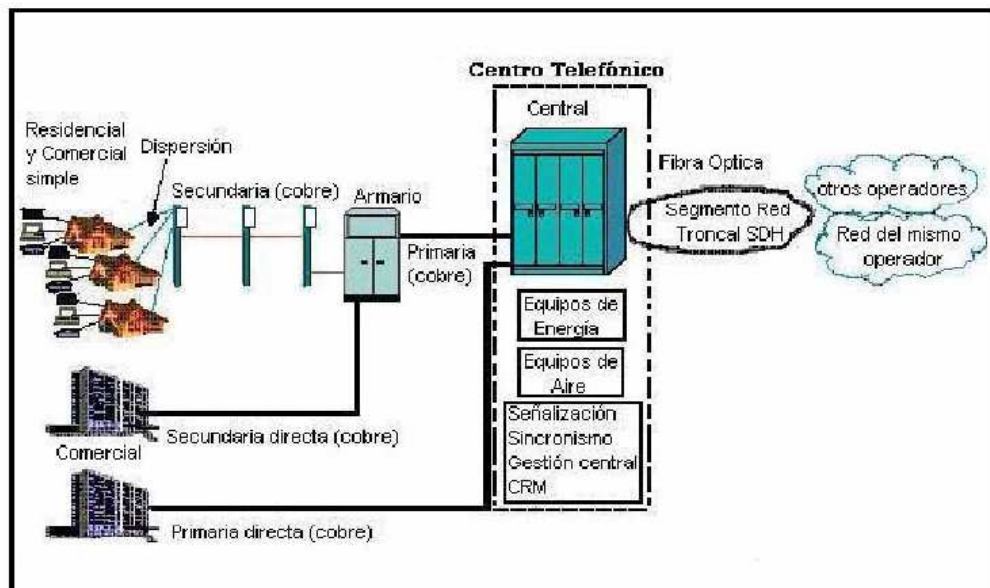
- Segmento de Red Primaria
- Segmento de Red Secundaria

El Módulo de Conmutación puede estar integrado por una sola central telefónica de conmutación o por más de una. La configuración mínima de red permite la interconexión con las demás redes telefónicas adyacentes y/o complementarias.

Este módulo está integrado por:

- Etapa de abonado.
- Matriz de Conmutación.
- Etapa Troncal.
- Procesamiento y control.
- Señalización.
- Sincronismo.
- Gestión.

Al Módulo Troncal pertenecen todos los equipos e infraestructura necesarios para la conexión entre las diferentes centrales telefónicas de conmutación, cuando hay más de una central en la red, y para la interconexión de la red con las demás redes telefónicas adyacentes y/o complementarias, mediante fibra óptica con tecnología SDH.



**Figura 2.3: Diagrama Esquemático de Red Telefónica Básica Fija. [3]**

- **2.6 Protocolo° Modelo TCP-IP**

Para conseguir un intercambio fiable de datos entre dos computadoras, se deben llevar a cabo muchos procedimientos separados.

El resultado es que el software de comunicaciones es complejo. Con un modelo en capas o niveles resulta más sencillo agrupar funciones relacionadas e implementar el software de comunicaciones modular.

Las capas están jerarquizadas. Cada capa se construye sobre su predecesora. El número de capas y, en cada una de ellas, sus servicios y funciones son variables con cada tipo de red. Sin embargo, en cualquier red, la misión de cada capa es proveer servicios a las capas superiores haciéndoles transparentes el modo en que esos servicios se llevan a cabo.

De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior, a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados.

### **2.6.1 El nivel Físico:**

El nivel físico describe las características físicas de la comunicación, como las convenciones sobre la naturaleza del medio usado para la comunicación (por ejemplo las comunicaciones por cable, fibra óptica o radio), y todo lo relativo a los detalles como los conectores, código de canales y modulación, potencias de señal, longitudes de onda, sincronización y temporización y distancias máximas [4].

### **2.6.2 El nivel de Enlace de datos:**

El nivel de enlace de datos especifica cómo son transportados los paquetes sobre el nivel físico, incluyendo los delimitadores (patrones de bits concretos que marcan el comienzo y el fin de cada trama). Ethernet, por ejemplo, incluye campos en la cabecera de la trama que especifican qué máquina o máquinas de la red son las destinatarias de la trama. Ejemplos de protocolos de nivel de enlace de datos son Ethernet, Wireless Ethernet, SLIP, Token Ring y ATM [4].

PPP (Point-to-Point Protocol) es un poco más complejo y originalmente fue diseñado como un protocolo separado que funcionaba sobre otro nivel de enlace, HDLC/SDLC [4].

Este nivel es a veces subdividido en Control de enlace lógico (*Logical Link Control*) y Control de acceso al medio (*Media Access Control*) [4].

### **2.6.3 El nivel de Internet**

Con la llegada del concepto de Internet, nuevas funcionalidades fueron añadidas a este nivel, basadas en el intercambio de datos entre una red origen y una red destino. Generalmente esto incluye un enrutamiento de paquetes a través de una red de redes, conocida como Internet [4].

En la familia de protocolos de Internet, IP realiza las tareas básicas para conseguir transportar datos desde un origen a un destino. IP puede pasar los datos a una serie de protocolos superiores; cada uno de esos protocolos es identificado con un único "Número de protocolo IP". ICMP y IGMP son los protocolos 1 y 2,

respectivamente.

#### **2.6.4 El nivel de Transporte**

Los protocolos del nivel de transporte pueden solucionar problemas como la fiabilidad ("¿alcanzan los datos su destino?") y la seguridad de que los datos llegan en el orden correcto. En el conjunto de protocolos TCP/IP, los protocolos de transporte también determinan a qué aplicación van destinados los datos [4].

- **2.7 Protocolo de Red ETHERNET**

Ethernet se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD, aunque actualmente se llama Ethernet a todas las redes cableadas que usen el formato de trama descrito más abajo, aunque no tenga CSMA/CD como método de acceso al medio.

##### **2.7.1 CSMA/CD (Carrier Sense Multiple Access)**

Acceso múltiple con detector de portadora de portadora significa que se utiliza un medio de acceso múltiple y que la estación que desea emitir previamente escucha el canal antes de emitir. Lo cual es el protocolo de señal eléctrica que se usa. En función de como actúe la estación, el método **CSMA/CD** se puede clasificar en:

- **CSMA no-persistente**

Si el canal está ocupado espera un tiempo aleatorio y vuelve a escuchar. Si detecta libre el canal, emite inmediatamente[5]

- **CSMA 1-persistente**

Con el canal ocupado, la estación pasa a escuchar constantemente el canal, sin esperar tiempo alguno. En cuanto lo detecta libre, emite. Puede ocurrir que, si durante un retardo de propagación o latencia de la red posterior a la emisión de la trama emitiera otra estación, se produciría una colisión (probabilidad 1) [5].

## **- CSMA p-persistente**

Después de encontrar el canal ocupado, y quedarse escuchando hasta encontrarlo libre, la estación decide si emite. Para ello ejecuta un algoritmo o programa que dará orden de transmitir con una probabilidad  $p$ , o de permanecer a la espera (probabilidad  $(1-p)$ ). Si no transmitiera, en la siguiente ranura o división de tiempo volvería a ejecutar el mismo algoritmo. Así hasta transmitir. De esta forma se reduce el número de colisiones (compárese con CSMA 1-persistente, donde  $p=1$ ) [5].

- **2.8 Virtual Private Network (VPN):**

- 2.8.1 VPN de acceso remoto**

Éste es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hotel, aviones (preparadas), etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura 'dial-up' (módems y líneas telefónicas), aunque por razones de contingencia todavía conservan sus viejos modems [6].

- **2.9 Escritorio Remoto de Windows.**

Esta técnica se utiliza para acceder a un computador o servidor remoto desde cualquier computador autorizado, funciona exactamente igual a estar sentado delante de la computadora a la que se accede, al dejar este puerto abierto se presentan diversos problemas de vulnerabilidad del sistema.

- **2.10 Página Web.**

Es una fuente de información adaptada para la World Wide Web (WWW) y accesible mediante un navegador de Internet. Esta información se presenta



generalmente en formato HTML y puede contener hiperenlaces a otras páginas Web, constituyendo la *red* enlazada de la World Wide Web [7].

Las páginas Web pueden ser cargadas de un computador local o remoto, llamado Servidor Web, el cual servirá de *host*. El servidor Web puede restringir las páginas a una red privada, por ejemplo, una intranet, o puede publicar las páginas en el World Wide Web. Las páginas Web son solicitadas y transferidas de los servidores usando el Protocolo de Transferencia de Hipertexto (HTTP - Hypertext Transfer Protocol). La acción del Servidor *host* de guardar la página Web, se denomina "HOSTING" [7].

Las páginas Web pueden consistir en archivos de texto estático, o se pueden leer una serie de archivos con código que instruya al servidor cómo construir el HTML para cada página que es solicitada, a esto se le conoce como Página Web Dinámica [7].

### **2.10.1 Comportamiento dinámico**

Los códigos del lado del cliente como JavaScript o AJAX pueden incluirse adjuntos al HTML o por separado, ligados con el código específico en el HTML. Este tipo de código necesita correr en la computadora cliente, si el usuario lo permite, y puede proveer de un alto grado de interactividad entre el usuario y la página Web [7].

Las páginas Web dinámicas son aquellas que pueden acceder a bases de datos para extraer información que pueda ser presentada al visitante dependiendo de ciertos criterios. Ejemplo de esto son páginas que tienen sistemas de administración de contenido o CMS. Estos sistemas permiten cambiar el contenido de la página Web sin tener que utilizar un programa de FTP para subir los cambios [7].

Existen diversos lenguajes de programación que permiten agregar dinamismo a una página Web tal es el caso de ASP, PHP, JSP y varios más.

### **2.10.2 Visualización:**

Las páginas Web generalmente requieren más espacio del que está disponible

en pantalla. La mayoría de los navegadores mostrarán barras de desplazamiento (*scrollbars*) en la ventana que permitan visualizar todo el contenido. La barra horizontal es menos común que la vertical, no sólo porque las páginas horizontales no se imprimen correctamente, también acarrearán más inconvenientes para el usuario [7].

Una página Web puede ser un sólo HTML o puede estar constituido por varios formando un arreglo de marcos (*frames*). Se ha demostrado que los marcos causan problemas en la navegación e impresión, sin embargo, estos problemas generalmente ocurren en navegadores antiguos [7].

Su uso principal es permitir que cierto contenido, que generalmente está planeado para que sea estático (como una página de navegación o encabezados), permanezcan en un sitio definido mientras que el contenido principal puede ser visualizado y desplazado si es necesario. Otra característica de los marcos es que sólo el contenido en el marco principal es actualizado [7].

Cuando las páginas Web son almacenadas en un directorio común de un servidor Web, se convierten en un *website*. El *website* generalmente contiene un grupo de páginas Web que están ligadas entre sí. La página más importante que hay que almacenar en el servidor es la página de índice (*index*). Cuando un navegador visita la página de inicio (*homepage*) de un *website* o algún URL apunta a un directorio en vez de a un archivo específico, el servidor Web mostrará la página de índice [7].

Cuando se crea una página Web, es importante asegurarse que cumple con los estándares del Consorcio World Wide Web (W3C) para el HTML, CSS, XML, etc. Los estándares aseguran que todos los navegadores mostrarán información idéntica sin ninguna consideración especial. Una página propiamente codificada será accesible para diferentes navegadores, ya sean nuevos o antiguos, resoluciones, así como para usuarios con incapacidades auditivas y visuales.

- **2.11 Protocolo RS-232:**

Este puerto, existente en todos los computadores, es aún el sistema más común para la transmisión de datos entre computadores. Todos los computadores como mínimo poseen uno (módem, ratón, etc.) [8].

El RS-232 es un estándar de comunicaciones propuesto por la Asociación de Industrias Electrónicas (EIA) y es la última de varias versiones anteriores. Antiguamente se utilizaba para conectar terminales a un computador Host. Se envían datos de 7, 8 o 9 bits. La velocidad se mide en baudios (bits/segundo) y sólo son necesarios dos cables, uno de transmisión y otro de recepción.

Lo más importante del estándar de comunicaciones es la función específica de cada pin de entrada y salida de datos porque nos encontramos básicamente con dos tipos de conectores los de 25 pines y los de 9 pines, es probable que se encuentre más la versión de 9 pines aunque la versión de 25 permite muchas más información en la transferencia de datos.

Las señales con la que actúa el puerto son digitales (0 - 1) y la tensión a la que trabaja es de 12 Voltios, resumiendo:

- 12 V. = Lógica "0".
- -12 V = Lógica "1".

Las características de los pines y su nombre típico son:

- TXD Transmitir Datos Señal de salida.
- RXD Recibir Datos Señal de entrada.
- RTS Solicitud de envío Señal de salida.
- DTR Terminal de datos listo Señal de salida.
- CTS Libre para envío Señal de entrada.
- DSR Equipo de datos listo Señal de entrada.
- DCD Detección de portadora Señal de entrada.
- SG Tierra Referencia para señales.
- RI Indicador de llamada Señal de entrada. La tabla 2.1 muestra la característica de los pines.

25 pines	9 pines	Nombre	Descripción
1	1	-	Masa chasis
2	3	TxD	Transmit Data
3	2	RxD	Receive Data
4	7	RTS	Request to send
5	8	CTS	Clear to send
6	6	DSR	Data Set Ready
7	5	SG	Signal Ground
8	1	DCD	Data Carrier Detect
15	-	TxC	Transmit Clock
17	-	RxC	Receive Clock
20	4	DTR	Data Terminal Ready
22	9	RI	Ring Indicator
24	-	RTxC	Transmin/Receive Clock

**Tabla 2.1: Características de los pines del puerto RS-232**

Para controlar al puerto serie, la CPU emplea direcciones de puertos de E/S y líneas de interrupción (IRQ). En el AT-286 se eligieron las direcciones 3F8h (o 0x3f8) e IRQ 4 para el COM1, y 2F8h e IRQ 3 para el COM2. El estándar del computador llega hasta aquí, por lo que al añadir posteriormente otros puertos serie, se eligieron las direcciones 3E8 y 2E8 para COM3-COM4, pero las IRQ no están especificadas.

Cada usuario debe elegir las IRQ de acuerdo a las que tenga libres o el uso que vaya a hacer de los puertos serie (por ejemplo, no importa compartir una misma IRQ en dos puertos siempre que no se usen conjuntamente, ya que en caso contrario puede haber problemas).

Antes de iniciar cualquier comunicación con el puerto RS-232 se debe de determinar el protocolo a seguir dado que el estándar del protocolo no permite indicar

en qué modo se está trabajando, es la persona que utiliza el protocolo la que debe decidir y configurar ambas partes antes de iniciar la transmisión de datos, siendo los parámetros a configurar los siguientes:

- Protocolo serie (número bits-paridad-bits stop)
- Velocidad de puerto
- Protocolo de control de flujo (RTS/CTS o XON/XOFF).

- **2.12 Protocolo del Puerto Paralelo.**

Se denomina puerto de impresora a un tipo de puerto paralelo original de los computadores usados, entre otras cosas, para imprimir [9].

Consta de un conector tipo "D" de 25 pines en donde los datos tienden a ir en un sólo sentido. En dicho puerto se emplean 8 bits de datos y 4 de control en la salida y otros 4 bits para la entrada. El resto de pines corresponden a "masa" y quedan intercaladas entre las pines de datos para evitar interferencias [9].

El método de transmisión es unidireccional (en una sola dirección) y muy sencillo. Un *latch* presenta en la salida el byte a imprimir. Inmediatamente la señal *strobe* se activa indicando que hay dato válido y al cabo de un tiempo se desactiva, para continuar con el siguiente byte [9].

La principal ventaja del puerto paralelo de impresora es la sencillez del manejo e implementación, los voltajes son compatibles con TTL y al operar en banda base carece de circuitos de traducción y adaptación de señales. Simplemente con un decodificador de direcciones y uno o dos *latches* se puede implementar un puerto paralelo. Este puerto dispone de tres registros de 8 bit cada uno (un byte).

**2.12.1 Puerto de datos (Pin 2 al 9):** Es el PORT 888 y es de sólo escritura, por este registro se enviarán los datos al exterior de la computadora.

**2.12.2 Puerto de estado (Pin 15, 13, 12, 10 y 11):** Es el PORT 889 y es de sólo lectura, por aquí se enviarán señales eléctricas al computador, de este registro

sólo se utilizan los cinco bits de más peso, que son el bit 7, 6, 5, 4 y 3 teniendo en cuenta que el BIT 7 funciona en modo invertido.

**2.12.3 Puerto de control (Pin 1, 14, 16 y 17):** Es el correspondiente al PORT 890, y es de lectura/escritura, es decir, se podrán enviar o recibir señales eléctricas. De los 8 bits de este registro sólo se utilizan los cuatro de menor peso o sea el 0, 1, 2 y 3, con un pequeño detalle, los bits 0, 1, y 3 están invertidos.

En esta imagen se pueden ver los tres registros, sus bits y los pines asignados a cada uno de ellos. La imagen corresponde a un conector DB-25 (Hembra).

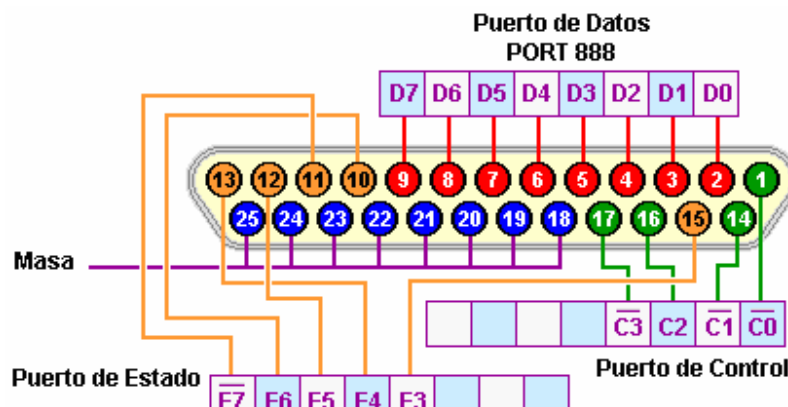


Figura 2.4: Esquema de los pines del puerto paralelo. [9]

- **2.13 Protocolo Frame Relay**

Es un protocolo de enlace, que se define como un servicio portador RDSI, de banda estrecha en modo de paquetes para el intercambio de datos y voz a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un costo menor, y que trabaja solamente en los dos primeros niveles del modelo OSI, y ha sido específicamente adaptado para velocidades de hasta 2.048 Mbps, aunque nada le impide separarlas [10].

### **2.13.1 Características**

- Es un Protocolo de Enlace mediante circuito virtual permanente muy usado para dar conexión directa a Internet.
- El sistema y tecnología de transmisión de datos consiste en la conmutación de unidades de datos de tamaño variable, denominada Tramas.
- Trabaja solamente con los dos primeros niveles OSI (Organización de Estándares Internacionales), nivel físico - nivel de enlace.
- Es un protocolo que se emplea en determinadas oportunidades como proveedor de enlaces digitales de alta velocidad a Internet.
- La información transmitida en una trama Frame Relay puede oscilar entre 1 y 8.250 bytes, aunque por defecto es 1.600 bytes.
- Demuestra un alto grado de interoperabilidad entre diferentes fabricantes de equipos y redes.
- Proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuito punto a punto.
- Las tramas y cabeceras pueden tener diferentes longitudes ya que hay una gran variedad de opciones disponibles en la implementación conocidos como anexos, a las del estándar básico.

## CAPÍTULO III

### Solución para Medición Remota de las Fibras Ópticas

El presente capítulo expone los dos métodos utilizados para el desarrollo del proyecto que son la Conexión de la computadora servidor con el OTDR por consola a través de *Hyperterminal* y a través del lenguaje PHP para desarrollar una interfaz gráfica amigable entre computadora y usuario, asimismo se hace un análisis superficial de la red de datos de CANTV para tener una comprensión más precisa del problema.

- **3.1 Análisis de la red de acceso**

La red de datos de CANTV básicamente se compone de dos fases:

- **3.1.1 Área *Backbone* (WAN)**

En el contexto de las telecomunicaciones el *backbone* es el troncal por el cual circula gran cantidad de información de diversos clientes a la misma vez, Los dispositivos conectados a una WAN Frame Relay caen dentro de una de dos categorías generales:

- DTE (Equipo Terminal de Datos): Los DTE, en general, se consideran equipo de terminal par una red específica y, por lo general, se localizan en las instalaciones de un cliente, de hecho, pueden ser propiedad del cliente. Algunos ejemplos de los dispositivos DTE son las terminales, computadoras personales, *routers* y *switches*.

- DCE: son dispositivos de interconectividad de redes propiedad de la compañía de larga distancia. El propósito del equipo DCE es proporcionar los servicios de temporización y conmutación en una red, que son en realidad los dispositivos que transmiten datos a través de la WAN. En la mayoría de los casos,

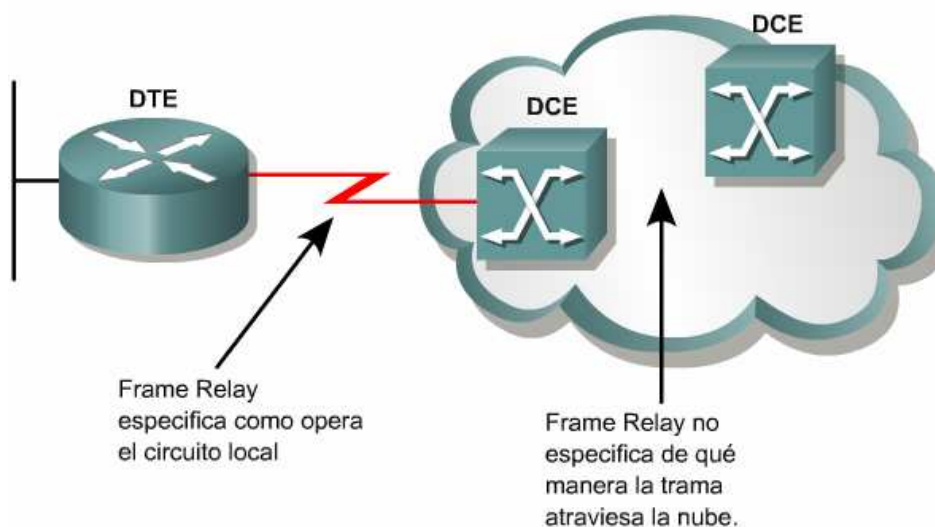


éstos son switches de paquetes.

La conexión entre un dispositivo DTE y un DCE consta de un componente de la capa física y otro de la capa de enlace de datos. El componente físico define las especificaciones mecánicas, eléctricas y de procedimiento para la conexión entre dispositivos. Una de las especificaciones de interfaz de la capa física que más se utiliza es la especificación del RS-232 (Estándar recomendado 232). El componente de la capa de enlace de datos define el protocolo que establece la conexión entre el dispositivo DTE, que puede ser un *router* y el dispositivo DCE, que puede ser un switch.

Como se puede observar en la figura, la WAN de *Frame Relay* de CANTV es una malla de *switches* interconectados. El DTE del cliente se conecta a los *switches* a través de líneas arrendadas.

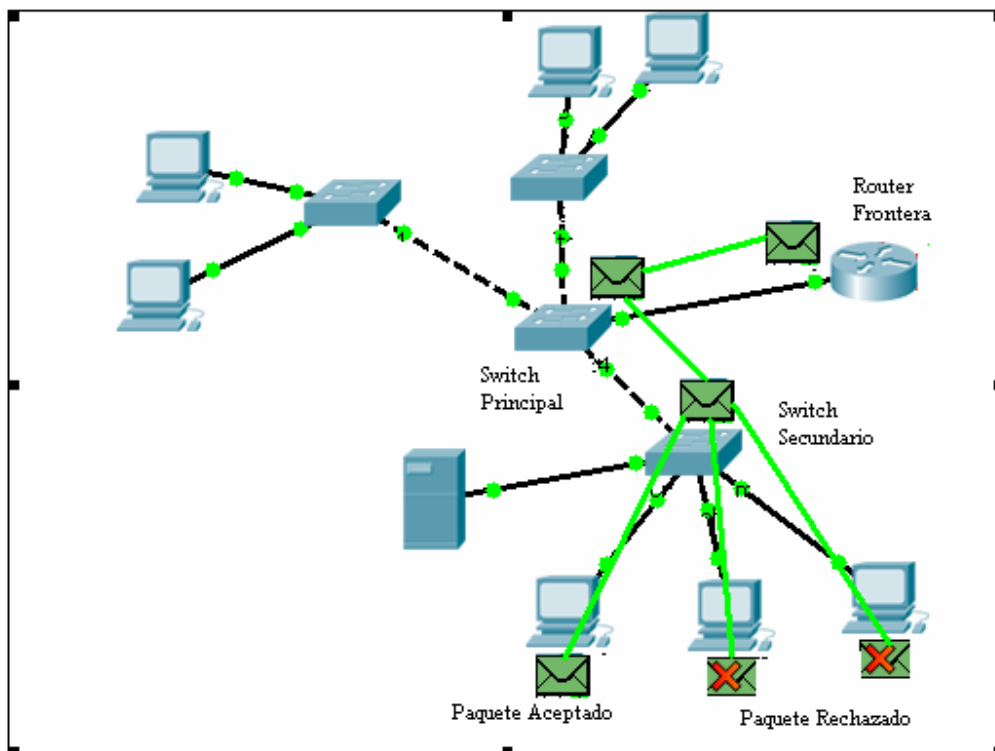
En el caso de la empresa CANTV, se usa *Frame Relay* para la interconexión de LAN. En estos casos, un router en cada una de las LAN será el DTE. Una conexión serial, como una línea arrendada T1/E1, conecta el router al switch *Frame Relay* de la compañía CANTV en su punto de presencia más cercano al router de la empresa solicitante del servicio. El *switch Frame Relay* es un dispositivo DCE. Las tramas se envían y entregan desde un DTE a otro DTE utilizando la red de *Frame Relay* creada por los DCE de CANTV la compañía de servicios.



**Figura 3.1: Interconexión de una LAN a la red de *switches* Frame Relay.**

### 3.1.2 Área de Acceso (LAN)

En esta área se utilizan los protocolos de capa 2 Ethernet y de capa 3 principalmente OSPF (también se pueden encontrar routers configurados con RIP, EIGRP, IGRP). Cuando un paquete entra a través del DTE, éste es desencapsulado, se remueven las cabeceras del protocolo *Frame Relay* y es entregado a la red LAN a través de los routers configurados con OSPF, los router se encargan de enviar el paquete al segmento de red correspondiente por el camino más corto, cuando llega al segmento de red de destino es entregado al switch principal de dicho segmento, si la dirección MAC no se encuentra en la tabla del *switch*, éste inunda los puertos con el paquete, el equipo terminal o computador destino del paquete envía al switch un acuse de recibo y se coloca en la tabla de puenteo del mismo, el resto de equipos terminales o computadoras desechan el paquete. La figura 3.2 ilustra el proceso.



**Figura 3.2: Ejemplo de un paquete recorriendo la LAN de CANTV**

- **3.2 Búsqueda y levantamiento de información del OTDR**

La parte más complicada del proyecto es la conexión de la computadora con el OTDR, ya que no se dispone de programas diseñados para esta tarea, no se sabe el protocolo de conexión con el puerto serial ni qué comandos se utilizarían para manejar el medidor de fibra óptica.

La primera medida a tomar es recopilar la mayor información del OTDR para saber su funcionamiento al medir las fibras, cómo interpreta los resultados, y lo más importante de todo cómo se conecta a la computadora.

- **3.2.1 Características del OTDR.**

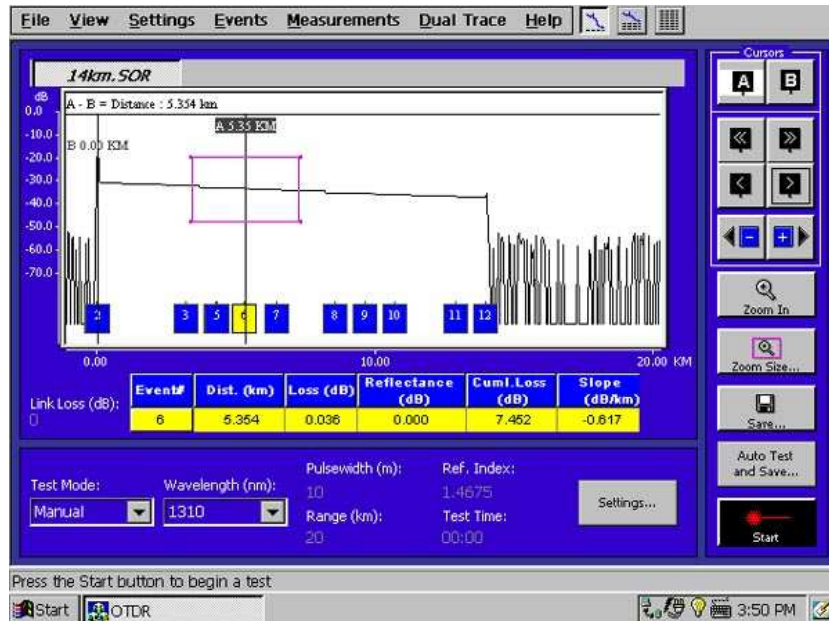
- Medida de pérdida óptica: El alto rango dinámico permite medidas precisas de pérdidas en la fibra y de distancia.

- Alto rango dinámico: Cuando se usa una longitud de onda de  $1.55 \mu\text{m}$  un punto ubicado a 190 km. puede ser medido.

Luego de ser promediadas las muestras tomadas, los resultados arrojados por el OTDR se grafican en una pantalla donde se muestra el nivel de señal en función de la distancia.

Adicionalmente se podrán medir atenuaciones de los diferentes tramos, atenuación de empalmes y conectores, atenuación entre dos puntos, etc.

También el OTDR se utiliza para medir la distancia a la que se produjo un corte, o la distancia total de un enlace, o para identificar una fibra dándole una curvatura para generar una fuga y observando en la pantalla del OTDR ver si la curva se “cae”, como lo muestra la figura 3.3.



**Figura 3.3: (OTDR) Ejemplo de una reflectometría realizada**

### 3.2.2 Parámetros de medición

- Índice de refracción
- Ancho de pulso
- Rango de medición en Km.
- $\lambda$  (longitud de onda)
- Cantidad de muestras
- Monomodo, multimodo, etc.

Luego de realizar los ajustes adecuados de los parámetros para la fibra a ser analizada se puede obtener la atenuación entre 2 puntos, pérdida en empalme, pérdida de retorno, atenuación por tramo, distancias a empalmes, cortes, tramos, etc.

Los parámetros de medición se varían por los siguientes motivos:

- Se varía el índice de refracción para ver mejor la traza, actúa como una especie de foco.
- El ancho del pulso se reduce para que llegue a una mayor distancia la

medición.

- La longitud de onda se aumenta para que alcance mayor distancia con mayor precisión. Se utiliza la longitud de 1550 nm para distancias mayores a 5 km, y 1310 para fibras inferiores a 5km, aunque se puede utilizar 1550nm para distancias cortas

- Cantidad de muestras (*averaging*): Parámetro que permite que el pulso recorra el tramo completo de fibra que se mida, si se escoge un *averaging* por debajo del necesario para una medición no se recorrerá la fibra completamente dando resultados poco precisos.

La utilidad que más interesa para este proyecto, es la capacidad del OTDR de conectarse con cualquier computador que posea por lo menos un puerto serial que utilice el protocolo de comunicaciones RS-232. EL medidor cuenta con un puerto serial RS-232 macho.

Adicionalmente, en la búsqueda de información sobre el manejo del OTDR, se encontró un manual con todos los comandos que controlan al medidor; ahora sólo se tiene que establecer la conexión entre el equipo medidor y la computadora.

- **3.3 Conexión a través del programa *Hyperterminal* de Windows**

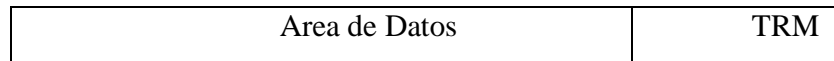
En principio, para realizar las pruebas, se utilizó el *Hyperterminal* de Windows, ya que es una herramienta sencilla que permite el control vía consola de cualquier dispositivo conectado a los puertos seriales del la computadora, tanto el OTDR como el puerto serial 2 o “COM 2” el cual establecerá la conexión entre ambos, tienen que ser configurados con el mismo protocolo de comunicación y con los mismos parámetros.

- 3.3.1 Protocolo de conexión usado.**

Se utilizó el método directo, cuya trama está descrita de la siguiente forma:

- Área de datos: Toda la información es transmitida de una sola vez en este método sin realizar la división en la transmisión, el valor máximo es de 220.000 bytes.

- Área TRM: Indica finalización de los datos transmitidos (\$oDoA), es un campo de datos binario de 2 Bytes.

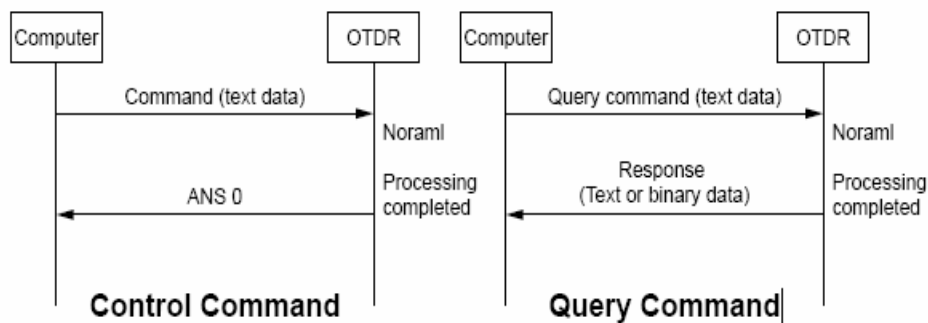


**Figura 3.4: Formato del mensaje cuando se usa el método directo**

### 3.3.2 Secuencia de transmisión del método directo

Cuando se envía un comando y la respuesta es positiva el OTDR envía nuevamente a la consola de control la respuesta “ANS0”.

Cuando se desee obtener información se envía un comando de requerimiento (*Query Command*). Por ejemplo cuando se desea saber el último evento donde termina la fibra se envía el comando AUT y se recibe la distancia y la pérdida de la fibra, como se indica en la figura 3.5.



**Figura 3.5: Secuencia de comunicaciones entre el OTDR y la PC**

Las pruebas que se describirán en el capítulo 4 demostraron que es posible la conexión con el OTDR y el control total del mismo por consola; pero, como se mostrará más adelante, es necesario un método automatizado para controlar al OTDR que no requiera introducir comandos a través del teclado sino a través del botón del ratón o *Mouse*, es por esto que se optó por utilizar el lenguaje PHP para ejecutar los comandos de una forma automatizada

- **3.4 Conexión con el OTDR a través del programa PHP**

Una vez realizada la conexión con el OTDR, se necesitaba automatizar el proceso, con *Hyperterminal* se tienen que introducir manualmente los datos a través del teclado, sólo queda el camino de la programación para establecer la comunicación entre el servidor y el dispositivo medidor.

PHP es un lenguaje de programación creado y diseñado en el ámbito de los sistemas libres, es usado normalmente para la creación de páginas Web dinámicas. PHP es un acrónimo recursivo que significa "PHP *Hypertext Pre-processor*" (inicialmente *PHP Tools*, o, *Personal Home Page Tools*), y se trata de un lenguaje interpretado, es muy versátil ya que trabaja tanto en alto como bajo nivel, es tan potente que es uno de los software más usados para la creación de páginas Web.

El gran parecido que posee PHP con los lenguajes más comunes de programación estructurada, como C y Perl, permiten a la mayoría de los programadores crear aplicaciones complejas con una curva de aprendizaje muy corta. También les permite involucrarse con aplicaciones de contenido dinámico sin tener que aprender todo un nuevo grupo de funciones. Este lenguaje se usó en conjunto con el Apache (también software libre) para establecer el servidor para el programa

La elección de estos programas viene influenciada por la nueva política de la empresa CANTV que en el afán de reducir costos para reducir las tarifas se requiere trabajar con software libre y gratuito. Las pruebas y la metodología se encuentran en el capítulo 4.

Las pruebas y métodos utilizados que se explicarán en el capítulo 4 demuestran claramente lo exitoso que fue utilizar PHP, se logró una conexión rápida y precisa con el OTDR, además de poder controlar por completo al mismo. Una vez logrado este objetivo, se procedió a controlar al OTDR desde otra computadora que estuviese conectada a la red LAN de CANTV con diversos métodos de conexión remota.

- **3.5 Conexión remota al OTDR y Seguridad del Servidor.**

- **3.5.1 Conexión a través de Escritorio Remoto.**

Se procedió a establecer la comunicación con la computadora servidor desde otra computadora ubicada en el CNT. Esta conexión se realizó estableciendo un escritorio remoto, esta utilidad facilita que un usuario pueda trabajar en una computadora, a través de su escritorio gráfico, desde otra computadora o terminal situado en otro lugar, gracias a una red de computadores. Esta técnica de conexión permite ver lo que se encuentra en el escritorio de la computadora servidor como si se estuviese sentado delante de ella.

La tecnología de escritorio remoto permite la centralización de aquellas aplicaciones que generalmente se ejecutan en entorno de usuario (por ejemplo, procesador de textos o navegador). De esta manera, dicho entorno de usuario se transforma en terminales de entrada/salida. Los eventos de pulsación de teclas y movimientos de ratón se transmiten a un servidor central donde la aplicación los procesa como si se tratase de eventos locales. La imagen en pantalla de dicha aplicación es retornada al terminal cliente cada cierto tiempo. De ahí la idea de “escritorio remoto”.

El elemento característico de cualquier implementación de escritorio remoto es su protocolo de comunicaciones:

- *Independent Computing Arquitectura (ICA)*, utilizado por *MetaFrame*.
- *Remote Desktop Protocol (RDP)*, utilizado por *Terminal Service*.
- *Adaptive Internet Protocol (AIP)*, utilizado por *Secure Global Desktop*.
- *Virtual Network Computing, (VNC)*, utilizado por el producto del mismo nombre.
- *X-11*, utilizado por *X-Window*.



El diseño de estos protocolos se basa en los siguientes principios:

- Latencia: El retardo de las comunicaciones es más importante que el ancho de banda.
- Balanceo de funcionalidad entre cliente y servidor.
- Tipo de primitivas de representación gráfica. Existen cuatro posibilidades: gráficos de alto nivel, gráficos de bajo nivel, primitivas de dibujo en 2D y píxel en bruto.
- Compresión de los datos relativos a las actualizaciones de la pantalla.
- Sincronismo de dichas actualizaciones. Definido por dos parámetros: la política de actualización de pantalla y la política de sincronización.

Como se está utilizando Windows 2000 para establecer la comunicación con el OTDR se utiliza el Protocolo de Escritorio Remoto (RDP), un protocolo de presentación que permite que un Terminal basado en Windows u otros clientes también bajo Windows, puedan comunicarse con un servidor Terminal Server.

RDP funciona a través de cualquier conexión TCP/IP, incluida una conexión de acceso telefónico, una red de área local (LAN), una red de área extensa (WAN), una Red digital de servicios integrados (ISDN), DSL o una Red privada virtual (VPN).

Una vez establecido el escritorio remoto, se inicia la sesión de *Hyperterminal* en el computador servidor con los parámetros establecidos anteriormente, se introducen exitosamente los comandos necesarios para realizar una medición en una fibra previamente conectada al ODF.

Para enviar el pulso que recorrerá la fibra hasta su fin, se tipea "STR 1", se pudo observar cómo el aparato medidor pasa de un estado pasivo a otro en el que empieza a realizar la medición. Estos comandos se obtuvieron en una búsqueda

intensiva en Internet hasta encontrar el manual de conexión remota del ANRITSU 9600 series.

Así como se puede enviar el pulso se puede variar a voluntad casi cualquier parámetro del OTDR, desde mandar el pulso, hasta guardar las trazas de las fibras en un archivo para su posterior análisis.

De esta forma se puede tomar control absoluto del OTDR desde cualquier computador que, previa autenticación, se encuentre conectado a Internet, pero, según se ha hecho público en algunos foros y sitios de seguridad, la vulnerabilidad detectada en el escritorio remoto, podría ser utilizada para realizar ataques de denegación de servicio (DoS), mediante peticiones creadas maliciosamente, y enviadas al protocolo RDP.

La explotación exitosa podría llegar a reiniciar el sistema, pero no sería posible la ejecución remota de código, lo que disminuye las posibilidades de que un atacante pueda tomar el control del equipo afectado.

Además, como este servicio no está activo por defecto (salvo en *Windows XP Media Center Edition*), la vulnerabilidad no afecta a todos los usuarios. Los sistemas afectados (si se activa el servicio), son los siguientes:

- *Microsoft Windows 2000 Service Pack 4.*
- *Microsoft Windows XP Service Pack 1.*
- *Microsoft Windows XP Service Pack 2.*
- *Microsoft Windows XP Professional x64 Edition.*
- *Microsoft Windows Server 2003.*
- *Microsoft Windows Server 2003 (Itanium-based Systems).*
- *Microsoft Windows Server 2003 Service Pack 1.*
- *Microsoft Windows Server 2003 SP1 (Itanium-based Systems).*
- *Microsoft Windows Server 2003 x64 Edition.*

*Windows XP Home Edition* no posee el servicio "Remote Desktop", aunque en cambio implementa la característica "*Remote Assistance*" (Asistencia remota), por lo que también es vulnerable si dicho servicio está habilitado.

Para mitigar un ataque que se aproveche de esta vulnerabilidad, y hasta que se publique un parche que la solucione, se recomienda utilizar cortafuegos, bloquear el puerto TCP/3389, desactivar si no son necesarios, los servicios "*Terminal Services*" o "*Remote Desktop*" (Escritorio remoto), o utilizar IPsec (*Internet Protocol Security*), o VPN (*Virtual Private Networks*), para las conexiones.

Asimismo, como se puede ver este ambiente no es muy amigable, ya que se tienen que realizar una serie de pasos, como iniciar el escritorio remoto e iniciar una sesión de *Hyperterminal* con los parámetros correctos para establecer la conexión con el OTDR, lo que complicaría el uso a los empleados que se encargan de reparar las fibras ópticas de CANTV, que serían los beneficiarios de este proyecto.

### **3.5.2 Solución Final. Crear una Página Web.**

Como se puede observar a menos que sea extremadamente necesario no se deberían tener abiertos los puertos de servicio remoto de la computadora, ya que esto presentaría un riesgo severo en la seguridad del servidor.

Es de hacer notar que tampoco se pudo realizar una página Web con una IP pública, ya que el servidor en el cual está alojado el programa se encuentra dentro de la red de CANTV, la cual no esta abierta al público, y hacer un "túnel" en la configuración de la red para que se pueda acceder a una dirección IP del servidor es un enorme riesgo para la seguridad.

Esto nos deja con la mejor salida que es utilizar una VPN y dentro de ella configurar un servidor para que aloje el programa *Where* como página Web por 2 motivos fundamentales:

- Mayor seguridad.
- Interfaz más sencilla y amigable para los usuarios finales.

Las VPN son una excelente opción frente a las líneas alquiladas debido al costo que puede significar el pagar una conexión de este tipo, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a

Internet o para hacer negocios con clientes frecuentes a través de la red.

En las VPN, los datos son codificados o cifrados y recién enviados a través de la conexión, para de esa manera asegurar la información y el *password* que se esté enviando.

Esta tecnología proporciona un medio para aprovechar un canal público de Internet como un canal privado o propio para comunicar datos que son privados. Más aún, con un método de codificación y encapsulamiento, una VPN básica, crea un camino privado a través de Internet. Esto reduce el trabajo y riesgo en una gestión de red.

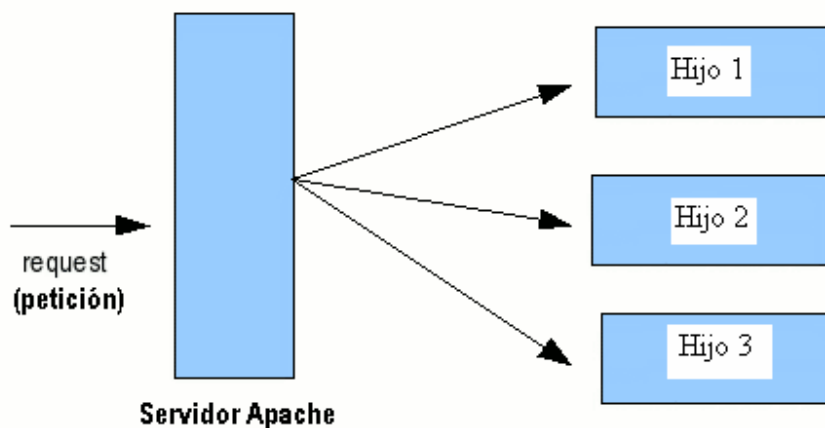
La tecnología de túneles está basada en estándares. Esta tecnología permite transmitir datos entre dos redes similares. A esto también se llama "encapsulación", es decir, a la tecnología que coloca algún tipo de paquetes dentro de otro protocolo (TCP). Aparte de todo esto, también se añade otra información necesaria para poder descifrar la información que se encuentra codificada. Estos paquetes llegan a su destino después de haber atravesado Internet, pero para verificar que ha llegado al destino correcto se realiza un proceso de autenticación.

#### **3.5.2.1 Configuración del servidor Apache.**

Para acceder al programa desde cualquier computadora es necesario configurar un computador para que actúe como servidor, para esta tarea se utilizó el software *Wampserver*, utilidad que posee el Apache que es el programa para configurar el servidor. EL PHP 5 forma parte de esta utilidad y está configurado de forma que sirva como un módulo del Apache, y MySQL que es el software para crear bases de datos, también como módulo del Apache.

El servidor Apache es un software que está estructurado en módulos. La configuración de cada módulo se hace mediante la configuración de las directivas que están contenidas dentro del módulo. Los módulos del Apache se pueden clasificar en tres categorías:

- **Módulos Base:** Módulo con las funciones básicas del Apache
- **Módulos Multiproceso:** son los responsables de la unión con los puertos de la máquina, aceptando las peticiones y enviando a los hijos a atender a las peticiones, como lo muestra la figura 3.6.



**Figura 3.6: Esquema de Atención de Peticiones del Servidor Apache**

- **Módulos Adicionales:** Cualquier otro módulo que le añada una funcionalidad al servidor.

El resto de funcionalidades del servidor se consiguen por medio de módulos adicionales que se pueden cargar. Para añadir un conjunto de utilidades al servidor, simplemente hay que añadirle un módulo, de forma que no es necesario volver a instalar el software. Para instalar el Apache se siguen los siguientes pasos:

**a) Descarga de Apache**

El servidor Web Apache se puede descargar en la página de la Fundación Apache, en Apache.org. En la URL <http://httpd.apache.org/> tienen una sección en particular para el servidor HTTP (Protocolo de transmisión utilizado en la Web), en la que se tiene que buscar el enlace para descarga.

Una vez en la página de descarga se debe buscar la última versión estable o la versión que recomendada. El servidor está disponible para sistemas Unix o Windows, por lo que se ofrecerán diversas opciones de descarga, incluso para obtener el código fuente del programa. Si se desea instalarlo en un sistema Windows, se necesita obtener el archivo *Win-32 Binary*, que es un instalador Windows.

### **b) Instalación**

Una vez descargado, se debe instalar en el sistema, ejecutando el archivo obtenido. Se dará paso a un asistente que guiará en el proceso de instalación del servidor. Durante el proceso preguntará el nombre del dominio y del servidor, que se puede rellenar con "*localhost*". Pedirá también una dirección de correo, que se puede rellenar con cualquiera que se desee. También se pregunta si se desea que el servidor responda en el puerto 80 para todos los usuarios o si se desea que sólo se active para el usuario actual en el puerto 8080, cuando se inicie manualmente. Lo normal es que lo active para todos los usuarios.

Con estos datos queda configurado el Apache inicialmente. En cualquier momento se puede editar al gusto o necesidad del usuario. Para ello se debe editar el fichero *httpd.conf*, que se encuentra en el directorio de instalación de Apache, que se ha indicado durante el proceso de instalación, más concretamente, en el subdirectorio *conf*.

Para comprobar que el servidor está activo y funciona correctamente se puede abrir un explorador y probar a acceder a la URL *http://localhost*, que es el propio servidor. Si todo ha ido bien se observará el mensaje de bienvenida del servidor con algo como "Funcionó! ¡El servidor Apache ha sido instalado en este equipo!"

#### **3.5.2.1.1 El fichero archivo *httpd.conf*. Estructura del fichero principal de configuración del Apache.**

El fichero *httpd.conf* es el fichero principal de configuración

del Apache, se encuentra dentro del directorio Conf, en el directorio de instalación del Apache.

En primer lugar hay que destacar que el fichero está dividido en tres grupos secciones:

1º Parámetros globales.

2º Directivas de Funcionamiento.

3º Host Virtuales.

En el fichero se encuentran todos los parámetros de funcionamiento del Apache. Algunos parámetros son generales para la instalación y funcionamiento del Apache. Muchos otros de los parámetros se pueden configurar independientes para un conjunto de directorios y/o ficheros . En estos casos los parámetros se encuentran ubicados dentro de secciones donde se indica el ámbito de aplicación del parámetro.

Las secciones más importantes son:

**<Directory>**: Los parámetros que se encuentran dentro de esta sección, sólo se aplicarán a el directorio especificado y a sus subdirectorios.

**<DirectoryMatch>**: Igual que Directory, pero acepta en el nombre del directorio expresiones regulares.

**<Files>**: Los parámetros de configuración proporcionan control de acceso de los ficheros por su nombre.

**<FilesMatch>**: Igual que Files, pero acepta expresiones regulares en el nombre del fichero.

**<Location>**: Proporciona un control de acceso de los ficheros por medio de la URL.

**<LocationMatch>**: Igual que

*Location*, pero acepta expresiones regulares en el nombre del fichero.

Algunas veces las directivas de funcionamiento de las secciones anteriores se pueden cruzar en cuyo caso tienen el siguiente orden de preferencia:

1. <Directory> y .htaccess (.htaccess prevalece frente a <Directory>).
2. <DirectoryMatch> y <Directory> .
3. <Files> y <FilesMatch> .
4. <Location> y <LocationMatch>.

También hay que destacar, que el fichero contiene una gran cantidad de comentarios para su correcta utilización, las líneas comentadas aparecen con el símbolo #.

#### **3.5.2.1.2 Proceso de Autenticación.**

Lo más importante que se realizó en el fichero httpd.conf es la autenticación de usuario. Como esta máquina se encuentra dentro de la VPN de CANTV, se asume que está a salvo de ataques fuera de esta red por lo que sólo nos enfocaremos en ataques que se puedan realizar dentro de la red.

La autenticación es el proceso por el cual se verifica que un usuario con una identidad conocida, tiene acceso al recurso solicitado. Para llevar a cabo esta acción, se suelen utilizar listas de permisos en las cuales se enumeran cada una de las acciones que puede realizar un usuario, o las que no puede hacer. Normalmente, para simplificar la gestión de estos ficheros, los usuarios se suelen unir en grupos proporcionando los permisos al grupo.

En Apache la autorización a recursos es gestionada mediante la directiva <directory> en el fichero principal de configuración, la forma de hacerlo es la



siguiente:

Se crea un archivo de base de datos donde se agregarán todos los usuarios permitidos, desde el *prompt* de la máquina se coloca `c:\wamp\Apache\bin\htdigest -c /alfonso cantv gabriel`, donde Htdigest es el comando para crear el archivo, /alfonso es el archivo sin extensión donde se crearán los usuarios permitidos, cantv es el dominio, gabriel es el usuario.

Luego de pulsar *enter*, el servidor requiere la clave y la confirmación, ya está creado el usuario gabriel en el dominio cantv con su respectiva clave. Cabe señalar que el cifrado de los datos se realiza con MD5 al usar autenticación *Digest*, un fuerte cifrado que se basa en un algoritmo virtualmente indescifrable. Luego se edita el archivo `httpd.conf` y se coloca la siguiente directiva

```
<Directory "C:/wamp/www">
```

```
Options Indexes FollowSymLinks
```

```
AllowOverride all
```

```
Order deny,allow
```

```
Allow from all
```

```
#Deny from all
```

```
AuthType digest
```

```
AuthName "cantv"
```

```
AuthuserFile /alfonso
```

```
Require user gabriel
```

</Directory>

Las directivas anteriores se explicarán a continuación.

*AllowOverride all*: Permite todas las directivas dentro del directorio `c:/wamp/www`.

*Order deny,allow*: Primero deniega el servicio a las direcciones IP no autorizadas y luego permite las autorizadas.

*Allow from*: Esta directiva indica las direcciones IP que pueden acceder al servidor, en este caso se puede colocar sólo la red vpn a la cual pertenece o se puede permitir cualquier dirección colocando “all”.

*AuthType*: Se coloca el tipo de autenticación, en este caso *digest*.

*AuthName*: Se coloca el dominio a la cual pertenecen los usuarios, en este caso “cantv”.

*AuthUserFile*: Se coloca el nombre del archivo donde se encuentran los usuarios y las claves. En este caso se encuentra en el directorio raíz y en el archivo alfonso (`c:\alfonso`), se coloca `/Alfonso`.

*Require user*: Se colocan los usuarios permitidos, en este caso gabriel.

Las pruebas de conectividad se explicarán en el capítulo posterior.

### **3.5.3 Configuración segura de puertos.**

Como se explicó anteriormente, la red VPN de la empresa CANTV es lo suficientemente segura para filtrar cualquier ataque *hacking* que provenga del exterior de la red, las listas de acceso de los routers frontera de la red se encargan de rechazar cualquier paquete red que no sea de la empresa haciendo virtualmente imposible acceder a los recursos si se encuentra en un computador con una dirección IP fuera de

la VPN, el mayor peligro se encuentra irónicamente dentro de la red.

Cualquier persona que tenga acceso a los recursos dentro de la empresa podría “hackear” sin mayor dificultad el servidor revelando las rutas de la fibra óptica lo que pondría en serio peligro la integridad de la red de fibra óptica, y por inducción todos los servicios de telefonía, voz datos y videos de todo el país.

Al ver lo importante de este servidor, no sólo basta con autenticar a los usuarios, se tiene que cerrar la puerta definitivamente a cualquier *hacker* que quiera acceder sin permiso. Por ende la única forma de bloquear la entrada a los intrusos es hacer un análisis exhaustivo de todas las técnicas de infiltración y aplicar las contramedidas, en este trabajo sólo se expondrán las más utilizadas y populares, no es objeto de esta tesis explicar todas y cada una de las técnicas y contramedidas *hackers*.

Para este estudio, se asume que los atacantes ya conocen la dirección IP de la máquina, por ende se intentarán determinar las rutas de acceso potenciales a la misma.

Antes de continuar se explicará el protocolo ICMP (*Internet Control Message Protocol*), que es de suma importancia en el tema de seguridad de redes. El ICMP es el subprotocolo de control y notificación de errores del protocolo IP. Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un *router* o *host* no puede ser localizado.

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta *Ping* y *traceroute*, que envían mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un *host* está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese *host* y cantidad de *hosts* por los que pasa.

Uno de los principales problemas de seguridad que nos encontramos con *Windows* es la facilidad para compartir archivos e impresoras. Si no se toman las debidas precauciones, esa facilidad para compartir, se puede convertir en un serio problema al estar conectados a Internet. Si se tiene abierto el puerto 139 que utiliza el

protocolo Netbios para compartir archivos con otras computadoras, cualquiera que descubra la dirección IP con la que estamos conectados (y sobre todo los que tienen conexión permanente con ADSL y dirección IP estática) podría acceder a nuestro sistema para realizar cualquier acción, desde acceder a los ficheros, pasando por introducir virus o troyanos, o usar nuestro servidor como plataforma para ataques a otros computadores.

Aunque la mayoría de los usuarios conoce los riesgos del puerto 139, usado por *Windows* para compartir archivos y carpetas, muchos ignoran que el puerto 445 en W2K, XP y Server 2003, permite prácticamente lo mismo que el anterior. En este caso, es usado por el SMB (*Server Message Block*).

El primer paso para proteger nuestro servidor es cerrar dichos puertos, para cerrar el puerto 139 se deben seguir los siguientes pasos:

1.- Ir primero a la carpeta Mi PC y hacer doble *click* sobre la carpeta Panel de Control.

2.- Pulsar sobre el icono de Red.

3.- Pulsar sobre la opción TCP/IP del Adaptador de Acceso Telefónico Internet) y a continuación pulsar sobre propiedades.

4.- En la pantalla que aparece hacer *click* sobre la pestaña enlaces. Se verán una serie de casilla. Luego hay que desmarcar la casilla de Compartir impresoras y archivos para redes Microsoft.

Una vez que se tiene desmarcada dicha casilla, pulsa aceptar y salir (hay que reiniciar para que la nueva configuración tenga efecto). Para cerrar el puerto 445 se siguen los siguientes pasos.

Desde Windows.

1.- Inicio -> Ejecutar -> regedit y pulsar aceptar.

2.- Una vez dentro del editor de registro se selecciona la carpeta HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters y se renombra la clave TransportBindName a TransportBindNameX.

Con esto se desactivan la interfaz Netbios por completo (puertos 137, 138,139) y la SMB (445).Esto es así porque para acceder a una sesión

Netbios en W2000- Win XP se puede acceder por el puerto 139 o por el puerto 445.

Una vez cerrados estos puertos se procede a la instalación de un firewall que asegure por completo al servidor, en este caso se decidió instalar la herramienta *ZoneAlarm*.

*ZoneAlarm* es un firewall por software producido por Check Point. Incluye un sistema de detección de intrusiones entrantes, al igual que la habilidad de controlar que programas pueden crear conexiones salientes.

En *ZoneAlarm*, el acceso del programa está controlado por las "zonas" en las cuales se dividen las conexiones de red del computador. La "zona de confianza" ("*trusted zone*") normalmente incluye la red de área local del usuario y puede compartir recursos tales como ficheros e impresoras, mientras que la "zona de Internet" ("*Internet zone*") incluye todo lo que no esté en la "zona de confianza".

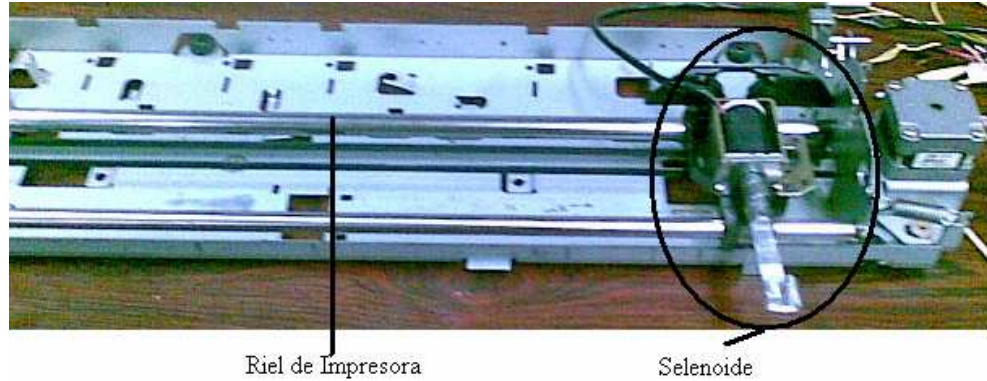
El usuario puede especificar que "permisos" (*trusted zone client, trusted zone server, Internet zone client, Internet zone server*) dar a un programa antes de que intente acceder a Internet (p.e. antes de ejecutarlo por primera vez) o, alternativamente, *ZoneAlarm* preguntará al usuario que permisos dar al programa en su primer intento de acceso. Las pruebas y ataques al servidor se explicarán en el capítulo posterior.

- **3.6 Diseño del *Switch* Mecánico.**

La empresa CANTV dispone de un gran número de fibras ópticas que recorren el territorio nacional en forma anular, y todas las fibras empiezan y terminan en el CNT, por este motivo tener un analizador de fibras en este punto es sumamente vital para tener centralizados los procesos de verificación y medición, pero resultaría sumamente costoso disponer de un OTDR por fibra, razón por la cual se necesita diseñar un dispositivo que actúe como *switch* o seleccionador de la ruta de fibra que se requiera.

### 3.6.1 Diseño de la parte mecánica del *switch*.

El *switch* mecánico que se diseñó consiste en un riel de impresora y sobre este un selenoide como lo ilustra la figura 12.



**Figura 3.7: *Switch* Mecánico**

El riel de impresora funciona principalmente con un motor paso a paso que mueve una correa giratoria, sobre la correa giratoria se encuentra embebida una plataforma en la cual descansa el selenoide.

El motor paso a paso tiene 6 pines o entradas, 2 de tierra (blanco y negro) y 4 para las entradas de datos (gris, carne, rojo y marrón), el motor se mueve a la izquierda cuando se colocan en nivel alto cada pin en secuencia, por ejemplo si se desea mover el motor cuatro pasos se colocan las siguientes entradas que indica la tabla 3.1.

Pin 0	Pin 1	Pin 2	Pin 3
Gris	Carne	Rojo	Marrón
1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1

**Tabla 3.1: Secuencia para mover el motor a la izquierda.**

Si se requieren más pasos, sólo se tiene que empezar la

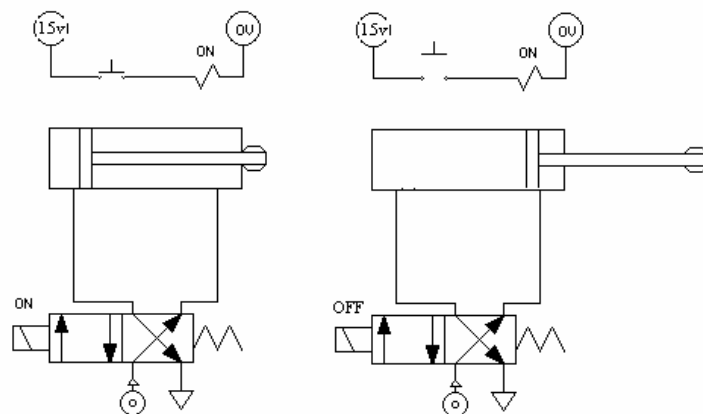
secuencia, para mover el motor a la derecha sólo se tiene que realizar la secuencia inversa, dependiendo de cuál fuese la última entrada, por ejemplo si la última entrada fue 0001, la secuencia para moverse a la derecha se indica en la tabla 3.2.

Pin 0	Pin 1	Pin 2	Pin 3
Gris	Carne	Rojo	Marrón
0	0	1	0
0	1	0	0
1	0	0	0
0	0	0	1

**Tabla 3.2: Secuencia para mover el motor a la derecha**

Las entradas del motor provienen del puerto paralelo de la computadora, manejar este puerto resulta más sencillo que el serial ya que no requiere sincronización ni configuración previa, sólo se envían los datos al puerto y éste a su vez al motor de modo que éste pueda seguir la secuencia y moverse.

El selenoide se activa cuando se colocan 15 voltios a su entrada, los campos magnéticos recogen el brazo, cuando se tiene un nivel bajo los campos magnéticos dejan de funcionar liberando el brazo, como se ilustra en la figura 13.



**Figura 3.8: Diagrama del Selenoide**

### 3.6.2 Diseño del software de control del *switch*

El programa que se utilizó para enviar datos al puerto paralelo fue el C++, lenguaje sumamente potente, que tiene la ventaja de crear archivos ejecutables, que pueden ser llamados desde PHP con el comando “exec” anteriormente explicado.

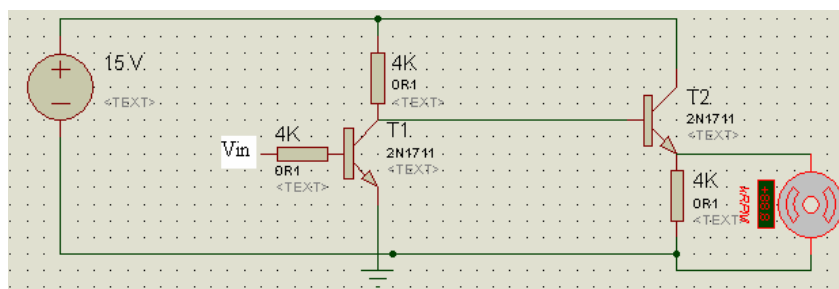
El comando `outport (888, N° decimal)` es el que realiza la conexión al puerto al colocar 888, el número decimal que se coloca luego de la coma es la salida que se requiera para el motor; por ejemplo si se requiere la entrada al motor 0001 se coloca `outport (888,1)`; el código fuente para controlar el *switch* se encuentra en los anexos.

### 3.6.3 Diseño del *driver* del *switch*.

Luego de automatizar el número de pasos requeridos para mover una distancia específica al selenoide, se encontró el problema de proporcionar el voltaje y la corriente necesaria para activar el motor y el selenoide, el puerto paralelo envía 2.5 voltios, que no son suficientes para activar ambos elementos, por esta razón fue necesario el diseño de un buffer o interfaz que proporcione el voltaje y la corriente necesaria. Los requerimientos de nuestro dispositivo son los siguientes:

- Voltaje de salida =15 V.
- Corriente de salida 70 mA.

Las pruebas determinaron que la impedancia de entrada del motor es de aproximadamente de 10 ohms por lo que el buffer debe tener una impedancia de salida si no inferior por lo menos igual. La topología se indica en la figura 14.

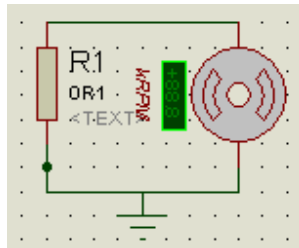


**Figura 3.9: Esquema del *Buffer*.**

El voltaje de salida del puerto paralelo es de 2.5 V y la corriente máxima es de 2.5 mA suficiente para saturar el transistor T1, cuando la  $V_{in}$  esta en alto, el  $V_a$  es de

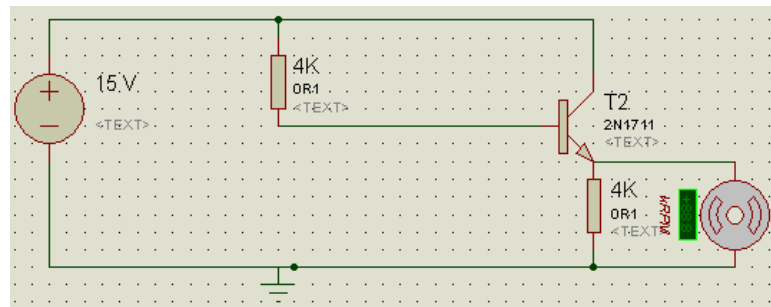


aproximadamente 0.2 V lo que hace que el transistor T2 se corte, por lo que el circuito quedaría como lo muestra la figura 15.



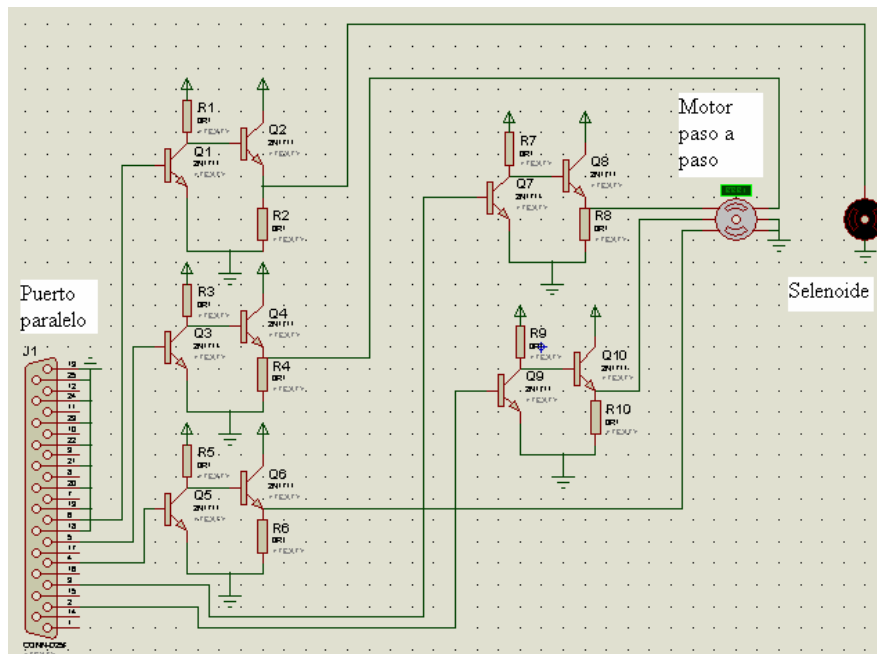
**Figura 3.10: Salida del Buffer**

Este circuito coloca en nivel bajo la salida, cabe destacar que el circuito actúa como inversor, si se quiere un nivel alto a la salida, se coloca un nivel bajo a la entrada lo que corta a T1 quedando el circuito como lo indica la figura 16:



**Figura 3.11: Salida del Buffer**

Como se puede notar, los niveles requeridos de corriente y voltaje los suministra la fuente y no el puerto paralelo, con esta configuración se aísla el motor del puerto, con lo cual se consigue proteger al puerto paralelo de posibles niveles inapropiados de tensión y corriente, los cuales podrían ser perjudiciales para el mismo. El montaje completo lo muestra la siguiente figura 17:



**Figura 3.12: Esquema del buffer.**

Al tener el dispositivo plenamente funcional, se procedió a utilizar al mismo para que funcionara como un switch mecánico para seleccionar la fibra que se quisiera analizar. El ODF (terminal óptico) se dispuso de tal forma que todas las fibras con sus conectores estuviesen alineados, la distancia entre cada conector es de 2,5 cm y desde el principio del carril hasta el primer conector es de 3 cm, como cada paso del motor se traducen en 0,1 mm para llegar a 3 cm se necesitan 300 pasos, luego para el siguiente conector se necesitarían 250 pasos, y así hasta llegar al conector que se necesita. El código para mover el motor en lenguaje C++ se encuentra en los anexos [A1].

- **3.7 Diseño de la Interfaz Gráfica Amigable**

- **3.7.1 Introducción a las Interfaces Gráficas**

La idea fundamental en el concepto de interfaz es el de mediación entre hombre y máquina. La interfaz es lo que "media", lo que facilita la comunicación, la interacción, entre dos sistemas de diferente naturaleza, típicamente el ser humano y una máquina como el computador.

Esto implica, además, que se trata de

un sistema de traducción, ya que los dos "hablan" lenguajes diferentes: verbo-icónico en el caso del hombre y binario en el caso del procesador electrónico.

De una manera más técnica se define la interfaz de usuario, como conjunto de componentes empleados por los usuarios para comunicarse con las computadoras. El usuario dirige el funcionamiento de la máquina mediante instrucciones, denominadas genéricamente entradas. Las entradas se introducen mediante diversos dispositivos, por ejemplo un teclado, entonces se convierten en señales electrónicas que pueden ser procesadas por la computadora.

Éstas señales se transmiten a través de circuitos conocidos como bus, son coordinadas y controladas por la unidad de proceso central y por un soporte lógico conocido como sistema operativo. Una vez que la UPC ha ejecutado las instrucciones indicadas por el usuario, puede comunicar los resultados mediante señales electrónicas, o salidas, que se transmiten por el bus a uno o más dispositivos de salida, por ejemplo una impresora o un monitor.

Resumiendo se puede decir que una interfaz de software es la parte de una aplicación que el usuario ve y con la cual interactúa. Está relacionada con la subyacente estructura, la arquitectura, y el código que hace el trabajo del software, pero no se confunde con ellos. La interfaz incluye las pantallas, ventanas, controles, menús, la ayuda en línea, la documentación y el entrenamiento.

Cualquier cosa que el usuario ve y con lo cual interactúa es parte de la interfaz. Una interfaz inteligente es fácil de aprender y usar. Permite a los usuarios hacer su trabajo o desempeñar una tarea en la manera más intuitiva y sencilla para ellos, en vez de tener que ajustarse al software. Una interfaz inteligente se diseña específicamente para la gente que la usará.

### **3.7.2 Implementación de la interfaz gráfica.**

Ahora que se tiene completamente funcional la máquina como servidor se precedió a desarrollar una interfaz gráfica que tenga 3 funciones básicas:

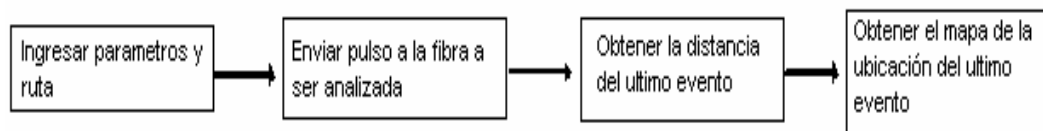
- Interacción con los programas desarrollados para controlar sendos puertos

paralelo y serial.

- Fácil manipulación por parte del personal que se encargará de manejarlo.
- Funcionamiento como página Web para ser accedido remotamente.

Para lograr este objetivo se utilizó una poderosa herramienta de diseño de página Web, Macromedia Dreamweaver, la ventaja de este programa es que los cambios que se hagan a la página son visualizados inmediatamente sin necesidad de ejecutar la página, recurso muy valioso cuando se están agregando gráficos.

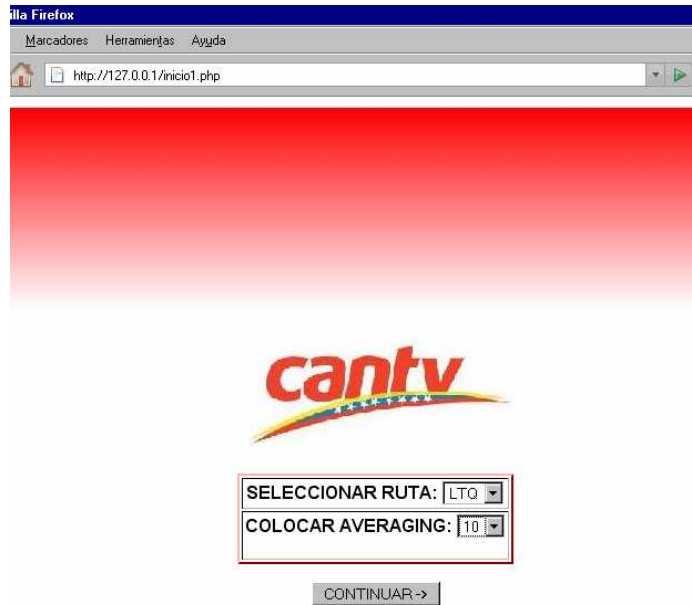
El programa se diseñó pensando en el usuario, de interfaz muy sencilla y que pueda ser trabajada paso a paso, el esquema del programa se hizo con diferentes páginas Web que procesen la información paso a paso como lo indica la figura 18.



**Figura 3.13: Esquema del programa.**

Las páginas se diseñaron para ser manejadas paso a paso de la siguiente manera:

- 1.- Página donde se ingrese el AVERAGING y la ruta a ser medida. (inicio1.php)



**Figura 3.14: Página de Inicio**

2.- Página de transición donde se envía el comando al OTDR para que envíe el pulso a la fibra. (prueba1.php)



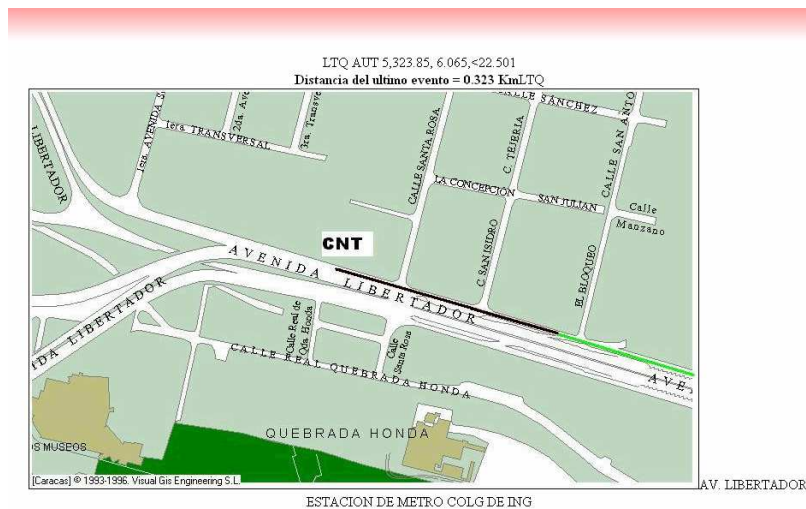
**Figura 3.15: Página de Transición.**

3.- Página de transición donde se envía el comando al OTDR para obtener el evento final de la fibra (gabriel1.php).



**Figura 3.16: Página de Transición**

4.- Página donde se visualiza el mapa con la sección de la ruta que indica el último evento de la fibra (generadoreventos.php).



**Figura 3.17: Página que Muestra el Mapa Donde se Encuentra la Falla.**

La última página se encarga de procesar los datos recogidos, la variable “ruta” se encarga de ubicar en la base de datos correspondiente a la ruta a ser analizada y la distancia obtenida por el OTDR ubica el mapa que será mostrado en pantalla.

Los mapas de las rutas digitalizadas se encontraban inicialmente en el formato de Microsoft Access, para poder accederlas a través del programa PHP se migró dicha base de datos a MySQL, con un software especializado llamado *MySQL Migration Toolkit*.

Para poder acceder al programa sólo se tienen que colocar las páginas Web diseñadas dentro de la carpeta predeterminada en el archivo de configuración `httpd.conf` como raíz, en este caso particular se definió que dicha carpeta se encuentre en `c:\wamp\www`, cuando se coloca desde el URL de cualquier navegador la dirección IP del servidor lo primero que hay que hacer es autenticarse como usuario autorizado, luego aparece la página definida como `index.php`, en este caso la página denominada anteriormente como `inicio1.php` se renombra a `index.php` para que ésta sea la primera página que observe el usuario cuando ingrese al servidor y así inicie el proceso de medición.

Como es evidente, esta interfaz paso a paso puede ser manejada por cualquier persona, los únicos conocimientos necesarios son saber qué significa el *averaging* y cuánto colocarle dependiendo del largo de la fibra, el personal de CANTV está plenamente calificado para manejar este programa, ya que sólo es una extensión del OTDR que ellos manejan a plenitud.

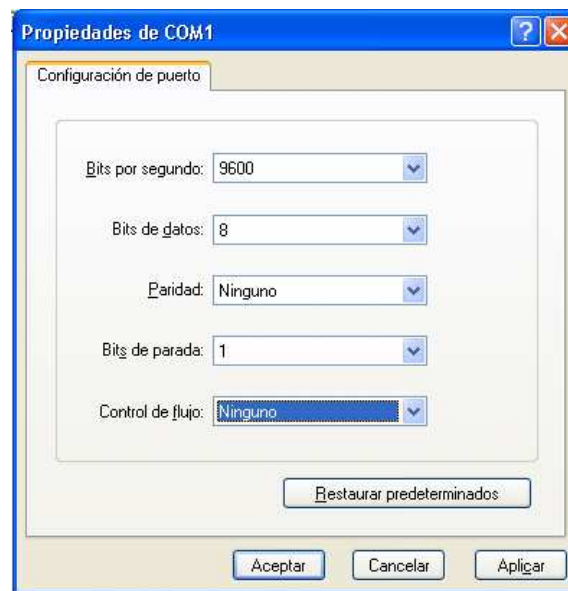
## CAPÍTULO IV

### Levantamiento y Pruebas del Funcionamiento del Sistema

El siguiente capítulo es una recopilación de todas las pruebas que se realizaron para el correcto funcionamiento del proyecto, por ende se procedió a ejecutar y a validar las aplicaciones instaladas, su acoplamiento e interoperabilidad.

- **4.1 Conectividad del OTDR con el computador servidor**

En principio tanto la computadora como el OTDR se tienen que configurar para que se establezca la conexión, el puerto serial de la computadora se configuró con el *Hyperterminal* con los parámetros que se muestran en la figura 4.1. El OTDR se configura con las mismas características.



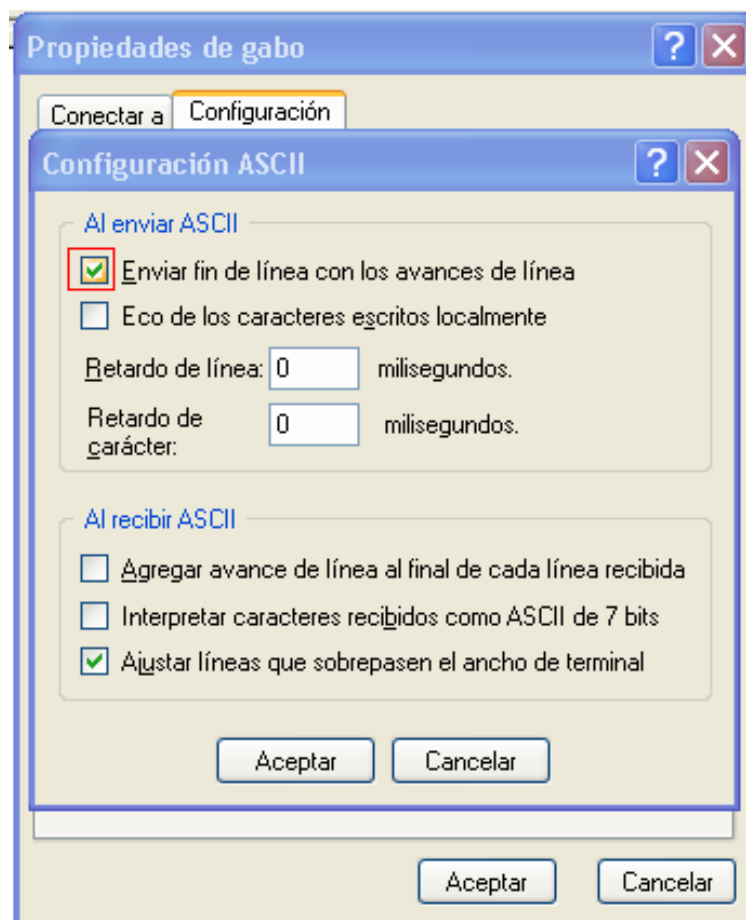
**Figura 4.1. Parámetros de conexión del puerto serial**

:

Cuando se empezaron la pruebas con el OTDR, las fallas que se presentaban



eran de conexión porque el equipo no reconocía la trama enviada por la computadora, a pesar que ambos equipos tenían la misma configuración, lo que no se estaba tomando en cuenta es que la computadora tiene que traducir los comandos que se introducen por la consola a código ASCII y enviar el fin de línea con las avances de línea. La figura 4.2 indica en un recuadro rojo la casilla que debe seleccionarse.

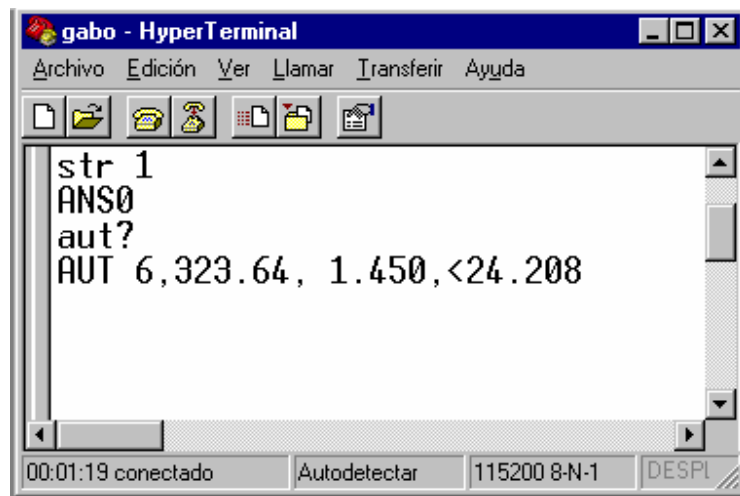


**Figura 4.2: Configuración ASCII.**

Al hacer estos cambios a la sesión de *Hyperterminal*, la conexión con el OTDR estuvo completa y funcionando como lo muestran las pruebas realizadas.

- **4.2 Conexión remota al OTDR**

En el momento en que se inicia la sesión de escritorio remoto, se toma control total de la computadora servidor y se puede tomar control de las unidades de disco de los archivos de configuración, etc. Incluso se pueden observar los iconos, en este punto se inicia la sesión de *Hyperterminal* en el computador servidor con los parámetros establecidos anteriormente, al introducir los comandos se obtuvieron los resultados esperados como se muestra en la figura 4.3.



**Figura 4.3: Demostración con *Hyperterminal* de la conexión con el OTDR**

Para enviar el pulso que recorrerá la fibra, se tipea “STR 1”, se pudo observar cómo el aparato medidor pasa de un estado pasivo a otro en el que empieza a realizar la medición. Estos comandos se obtuvieron en una búsqueda intensiva en Internet hasta encontrar el manual de conexión remota del ANRITSU 9600 series.

Así como se puede enviar el pulso se puede variar a voluntad casi cualquier parámetro del OTDR, desde mandar el pulso, hasta guardar las trazas de las fibras en un archivo para su posterior análisis.

Este método demuestra que se puede tener control remoto del OTDR desde cualquier computador que se encuentre en la red de CANTV, pero no es un método sencillo por todo los conocimientos previos en computación que se requieren, la interfaz con el usuario se quiere lo más sencilla posible es por eso que se intentaron

otros métodos descritos posteriormente.

- **4.3 Conexión con el puerto serial a través del programa PHP**

El primer problema que se plantea es enviar datos al OTDR y luego leer los datos del mismo de alguna forma, al probar con el *Hyperterminal* de Windows es notorio el hecho que el OTDR responde con una cadena de caracteres o *strings*, al ser así se puede capturar esta información en una variable para su posterior uso. El Lenguaje PHP tiene comandos de lectura, escritura y apertura de puertos.

Para estos comandos primero se tiene que inicializar el puerto serial, esto se logra con el programa bajado de Internet llamado serproxy. Este programa se encarga de abrir el puerto, y editando el archivo serproxy.cfg se pueden variar los bits por segundo, la paridad, número de bits, etc., simplemente se descarga el programe desde el link <http://www.lspace.nildram.co.uk/files/serproxy-0.1.2.zip>, se descomprime en la carpeta seleccionada, se edita el archivo serproxy.cfg con el editor de texto deseado y el programa se inicializa al ejecutar el archivo serproxy.exe.

Una vez inicializado el puerto serial se procede a inicializar la conexión con el comando *fsocketopen*, que inicia una conexión a través de *sockets* con el recurso especificado por *nombre\_host*. El *fwrite* que envía la información como cadena de caracteres al puerto, y el *fread* que lee la información del puerto. La sintaxis para abrir y escribir en el puerto serial 2 o COM 2 es:

```
$var = fsocketopen (localhost, 5332, 0,0 , 30));
```

Esta nomenclatura indica que \$var será un puntero en donde llegará la información del puerto, *localhost* es el nombre de la máquina a la que se quiere abrir el puerto, 5332 indica el puerto serial 2, y 30 indica el tiempo máximo para esperar la conexión.

La siguiente línea de comandos muestra la escritura en el puerto cadena de caracteres.

```
fwrite ($var , "str 1 $xD");
```

\$var es el indicador o puntero a donde se tiene que enviar la cadena de caracteres, "STR 1 \$xD"; los caracteres STR 1 indican el comando que se quiere introducir y el los caracteres \$xD son de suma importancia ya que éstos son el campo TRM de la trama que indica la finalización de ésta, como lo indica el protocolo de comunicaciones Método Directo explicado anteriormente.

Para leer la cadena de caracteres que envía el OTDR se coloca la siguiente línea en el programa:

```
$var1=fread ($var , 30);
```

La única diferencia con el comando fwrite es que se debe asignar lo que se obtenga en la lectura a una variable, en este caso \$var1, y el número "30" es la cantidad de caracteres que se deben leer, en este caso un máximo de 30.

Este método funcionó perfectamente, la conexión se estableció y los comandos enviados por el puerto serial al OTDR manejaron el dispositivo correctamente, el único inconveniente que se presentó fue que el tiempo total entre la conexión y el envío de datos es de 30 segundos, si se quisieran mandar muchos comandos para establecer diferentes parámetros, el tiempo de medición se tornaría intolerable para el usuario final.

El proceso total para determinar una falla podría tomar más de 3 minutos, este retardo en la conexión con el dispositivo parece independiente al lenguaje que se utilice, ya que se intentó hacer lo mismo con un programa de lenguaje C pero los resultados fueron los mismos; además, si se hubiese realizado con lenguaje C, la variable de interés es la del último evento quedaría en este lenguaje y todavía no se conoce ningún software que cambie una variable de un lenguaje a otro, por esta razón se prefirió hacer todo el programa con PHP.

Para superar el inconveniente del retardo, se investigaron diversas alternativas, como utilizar en C y C++ para compilar los programas que se encargarían de hacer la conexión con el puerto serial. Al investigar en el libro superutilidades hacker, que se consultaba para estudiar la seguridad

en el servidor y en la red, una utilidad en especial salta a la vista para el propósito del proyecto, el Netcat.

Por tanto este programa es el más versátil utilizado por los administradores de redes y por supuesto de los mismos hackers, ya que tiene infinidad de utilidades, la primordial para el proyecto: es capaz de enviar cadenas de texto a cualquier puerto de la computadora. Accediendo al *prompt* del sistema, se accede al directorio donde se encuentra el programa Netcat y se introduce el siguiente comando: `c:\netcat>nc 127.0.0.1 5332`, se establece una conexión con la misma computadora al introducir `127.0.0.1` (dirección de *loopback*) y con el puerto serial 2 con el número de puerto `5332`.

Al colocar este comando se estableció la conexión con el puerto serial, haciendo la salvedad que el programa *serproxy* tiene que estar activado para inicializar el puerto . Al colocar este comando el equipo queda a la escucha y se prepara para recibir la cadena de caracteres. Luego, simplemente se tipea el comando, por ejemplo `STR 1`, se tecléa un espacio con la barra y se presiona la tecla *enter*.

Con esta operación, se puede observar como el OTDR realizaba la medición en la fibra óptica, sin ningún retardo, haciéndola casi inmediatamente después de apretar la tecla *enter*, ahora sólo se tiene que automatizar este proceso; es decir, simplemente con hacer doble clic a un ejecutable en la pantalla se ejecute toda la medición en la fibra sin necesidad de tipear el comando.

Para automatizar este proceso se debe colocar en el *prompt* del sistema la siguiente línea de comandos:

```
C:\netcat>echo str 1 | nc 127.0.0.1 5332
```

Al colocar este comando la medición se realiza automáticamente sin necesidad de tipear posteriormente el comando requerido.

Esta operación garantiza la automatización de los procesos, ya que todos los lenguajes de programación tienen llamadas a programas externos o archivos, bien

sean ejecutables o no, el programa PHP utiliza el comando “exec” para hacer éstas llamadas.

La forma de enviar automáticamente el comando para que el OTDR realice la medición desde PHP es la siguiente:

```
exec (echo str 1 | nc 127.0.0.1 5332);
```

Con este comando se envía el pulso desde el programa PHP simplemente haciendo una llamada al ejecutable echo.com y nc.exe como se observa en el ejemplo anterior, la respuesta del programa es inmediata, haciendo posible utilizar una mayor gama de comandos para programar el OTDR, dependiendo de las necesidades de los encargados de las mediciones en la fibra óptica.

Por último, también se puede leer variables producidas por el Netcat, siendo de suma utilidad para leer el último evento de la fibra óptica. Para realizar este proceso (donde se presume que está el corte o el fin de la fibra) se coloca en el programa la siguiente línea:

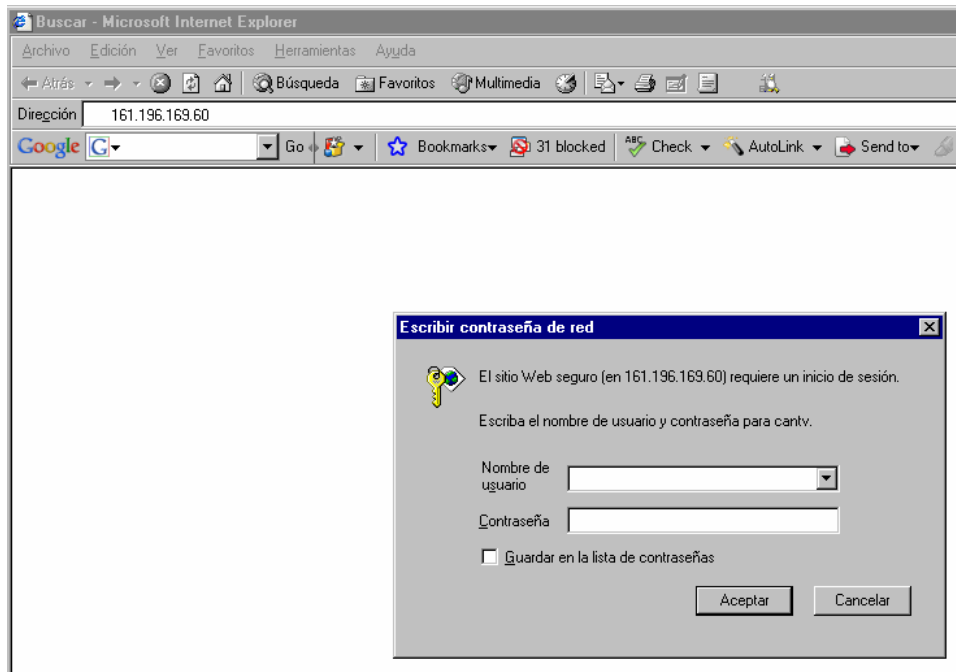
```
$var = echo exec (echo str 1 | nc 127.0.0.1 5332);
```

La variable \$var contiene una cadena de caracteres, como dato más relevante se encuentra la distancia del último evento, cabe destacar que esta medición se hace inmediatamente y no como se realizaba anteriormente en 30 segundos.

#### • **4.4 Pruebas de Conectividad del Servidor**

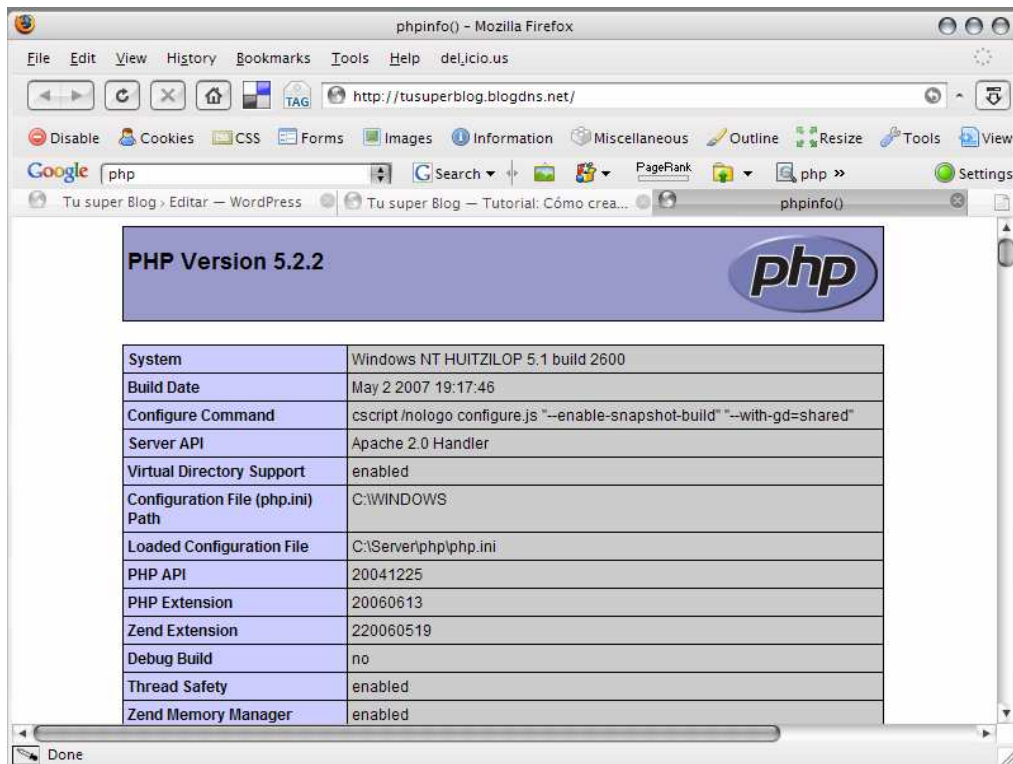
Al tener ya configurado el servidor se hacen las pruebas de conectividad dentro de la red. Lo que se quiere es acceder al servidor desde cualquier máquina dentro de la VPN. La dirección IP del servidor ya configurado es 161.196.169.60. Como se colocó en la configuración que se permitiera cualquier dirección, simplemente, desde otra computadora se abre el navegador Explorer o Mozilla y se coloca la dirección IP antes mostrada en el URL. Lo primero que se muestra es un menú en donde se tiene que

tiene suficiente seguridad para ataques internos dentro de la red, como se muestra en la figura.



**Figura 4.4: Ejemplo de conexión con el servidor**

Después de colocar el usuario y la clave se puede acceder al servidor, nos muestra es la página index.php como lo muestra la figura 4.5, que se coloca por defecto, en este punto ya se realizó la conexión con el servidor. Más adelante cuando se depure el programa esta página index será reemplazada por el programa.



**Figura 4.5: Página que indica la configuración por defecto del servidor**

Por último se verifica que nadie fuera de la VPN tenga acceso a la página, desde cualquier computadora que no esté dentro de dicha red se coloca en la URL del navegador el dirección IP del servidor obteniendo los resultados esperados, como lo muestra la figura 4.6.





**Figura 4.6: Página que indica que no se realizó la conexión con el servidor.**

Este resultado es el correcto ya que el *router* frontera de CANTV lee la dirección IP de la máquina desde la que se está intentando acceder y chequea con su lista de acceso programada por los administradores de la red LAN de CANTV, al no estar dentro de la red impide el acceso.

## • 4.5 Ataques al Servidor Para Comprobar su Seguridad

### 4.5.1 Determinación de sistemas vivos y escucha de puertos abiertos

Los ataques que se realizaron al servidor se hicieron en un ambiente seguro, es decir, se realizó desde una de las computadoras dentro de la red privada que se encuentra en el mismo departamento en el que se ubica el servidor, la cual está bajo nuestro total dominio.

El primer paso para comprometer un sistema basado en Windows es utilizar los comandos `Tracert` desde la *shell* de Windows; este comando envía paquetes ICMP a la computadora víctima, si recibe respuesta es porque el sistema

se encuentra activo, si no, puede ser que algún servidor de seguridad a algún router estén bloqueando los paquetes ICMP. Este comando tiene la particularidad de mostrar los routers por los que pasan los paquetes ICMP, cuando se intenta utilizar este comando desde fuera de la VPN se observaría lo que muestra la figura 4.7.

```

1 router7301 (201.219.64.1) 0.623 ms 0.557 ms 0.617 ms
2 201.219.64.254 (201.219.64.254) 1.364 ms 0.963 ms 1.356 ms
3 200.3.91.153 (200.3.91.153) 5.875 ms 6.473 ms 6.597 ms
4 mun01rt-pos1-5-2.tasf.telecom.net.ar (200.3.32.65) 134.427 ms 132.873 ms 134.266 ms
5 host86.200-3-81.telecom.net.ar (200.3.81.86) 147.632 ms 147.512 ms 147.145 ms
6 mia7-telecom-argentina-2-ar.mia.seabone.net (195.22.199.113) 142.061 ms 142.510 ms 142.481 ms
7 * * *
8 cha-00-vlan5.gw.cantv.net (200.44.43.202) 247.909 ms 247.696 ms 247.483 ms
9 cnt-00-ge7-0-0.gcore.cantv.net (200.44.43.26) 241.558 ms 241.205 ms 242.216 ms
10 * * *
11 * * *
12 * * *

```

**Figura 4.7: Resultado del Comando Tracert.**

En las líneas 10 a la 12 se observa que el router con la interfaz 200.44.43.23, la cual da acceso a la red interna, bloquea los paquetes ICMP impidiendo que un atacante externo pueda saber que hosts están “vivos”. Pero si se intenta desde la red interna se puede saber si el sistema esta vivo como lo muestra la figura 4.8.

```

C:\>tracert 161.196.169.60

Trazo a la dirección 78DHFRR.cantv.com.ve [161.196.169.60]
sobre un máximo de 30 saltos:

 1 <10 ms <10 ms <10 ms 78DHFRR.cantv.com.ve [161.196.169.60]

Trazo completa.

```

**Figura 4.8: Resultado que indica que el sistema a atacar esta “vivo”.**

Como se puede observar, si se realiza esta clase de ataque dentro de la red desde cualquier computador se sabe que el *host* con la dirección IP 161.196.169.60 está “vivo”; es decir la computadora está encendida y conectada a la red.

También se usa el comando Ping para realizar esta clase de ataque

obteniéndose la siguiente que se observa en la figura 4.9.

```
C:\>ping 161.196.169.60

Haciendo ping a 161.196.169.60 con 32 bytes de datos:

Respuesta desde 161.196.169.60: bytes=32 tiempo<10ms TTL=128
Respuesta desde 161.196.169.60: bytes=32 tiempo<10ms TTL=128
Respuesta desde 161.196.169.60: bytes=32 tiempo<10ms TTL=128
Respuesta desde 161.196.169.60: bytes=32 tiempo<10ms TTL=128

Estadísticas de ping para 161.196.169.60:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),
    Tiempos aproximados de recorrido redondo en milisegundos:
        mínimo = 0ms, máximo = 0ms, promedio = 0ms
```

### Figura 4.9: Resultado del comando Ping.

Se enviaron 4 paquetes ICMP ECHO REQUEST y se recibieron 4, esto indica claramente que el sistema se encuentra activo.

Para evitar estos ataques, desde el punto de vista del host, existen varias utilidades que pueden detectar y registrar estos ataques, si comienza a ver un patrón de paquetes ICMP ECHO enviados desde un sistema o red determinados, es posible que alguien esté realizando un reconocimiento de red del sitio. La herramienta utilizada para detectar los barridos Ping y Tracert es SNORT.

Si se detecta que el sistema está vivo, se procedería a detectar qué servicios se encuentran a la escucha.

#### 4.5.2 Identificación de los servicios TCP y UDP que estén en ejecución.

Utilizar una buena herramienta de exploración de puertos resulta crítica durante el proceso de rastreo. Aunque hay muchos exploradores de puertos disponibles tanto para el entorno Unix como Windows NT, se limitará el análisis a uno sólo de ellos: El Netcat, herramienta antes descrita.

Los principales objetivos son los puertos TCP 111, 139, 179, 445, 524, 1434, 2049 y UDP 513, 1434, 2049 y 32771, ya que a través de éstos se pueden realizar ataques de enumeración que serán explicados posteriormente en este capítulo.

Para detectar los puertos que se encuentran abiertos a la escucha, sólo se tiene que tener Netcat instalado, luego desde la *shell* de Windows colocar:

```
C:\netcat\nc -z -v -w2 161.196.169.60 111-2049
```

La opción `-v` proporciona salidas detalladas, la opción `-z`

genera Entrada/salida en modo cero y se utiliza para la exploración de puertos y la opción `-w2` proporciona un valor de tiempo de espera máximo para cada conexión. De forma predeterminada Netcat escuchará en los puertos TCP, si se quiere explorar los puertos UDP sólo se agrega coloca la opción `-u`.

```
C:\netcat\nc -u-z -v -w2 161.196.169.60 513-32771
```

Cabe destacar que algunas veces cuando se colocaban rangos de exploración de puertos superior a 100 el programa no se ejecutaba, es preferible explorar estos puertos individualmente.

Al realizar las pruebas en el servidor, se pudo notar que los puertos 137, 139 y 445 estaban abiertos.

Este resultado es sumamente importante, ya que si se dejan abiertos, darán pie a ataques de enumeración, proceso que consiste en analizar en mayor profundidad los servicios identificados en busca de debilidades conocidas.

#### **4.5.3 Ataques de enumeración**

La principal diferencia existente entre las técnicas de recopilación y las de enumeración es el grado de intrusión; la enumeración implica la conexión activa a los sistemas y la realización de consultas dirigidas. Como consecuencia, estas operaciones pueden ser registradas o, al menos detectadas.

En general, los atacantes intentarán encontrar, utilizando técnicas de enumeración, la siguiente información: nombres de cuentas de usuario para realizar ataques posteriores de adivinación de contraseñas, recursos compartidos mal configurados y versiones antiguas de software con conocidas vulnerabilidades de seguridad.

Una vez que el intruso conozca uno de estos datos sólo será cuestión de tiempo para que el mismo llegue a comprometer el sistema hasta cierto punto, si no completamente. Al ver todo lo que puede lograr un atacante si descubre uno de estos puntos débiles en el sistema, lo mejor es cerrar estos agujeros de seguridad para eliminar los principales puntos de apoyo del hacker.

Para realizar estos ataques de enumeración se debe realizar una sesión nula que consiste en una conexión de tipo "sesión nula", también conocida

como "entrada anónima al sistema", la cual es un mecanismo que permite a un usuario anónimo obtener información (como nombres de usuario y recursos compartidos) a través de la red, o conectarse sin autenticarse contra el sistema.

Este mecanismo es usado por aplicaciones como "explorer.exe" para enumerar los recursos compartidos en sistemas remotos. En Windows NT y Windows 2000 muchos servicios locales se ejecutan sobre la cuenta del sistema (SYSTEM), conocida como LocalSystem en Windows 2000. La cuenta SYSTEM se usa para diversas tareas críticas para el sistema. Cuando una máquina necesita obtener datos de sistema de otra, la cuenta SYSTEM abrirá una sesión nula contra la otra máquina.

La cuenta SYSTEM tiene virtualmente privilegios ilimitados y no tiene contraseña, por lo que no es posible entrar en el sistema como usuario SYSTEM. SYSTEM necesita en ocasiones acceder a información tal como recursos compartidos disponibles, nombres de usuario, etc. en otras máquinas -- una funcionalidad del tipo "Entorno de Red". Dado que no es posible conectarse a otros sistemas utilizando un identificador de usuario y una contraseña, utiliza una "sesión nula" para obtener acceso. Desgraciadamente, un atacante también puede utilizar la "sesión nula" del mismo modo.

Para llevar a cabo este ataque desde una máquina remota se accede al *prompt* del sistema y se realizan las operaciones que se indican en la figura 4.10.

```
C:\Documents and Settings\Administrador>cd..
C:\Documents and Settings>cd..
C:\>net use \\161.196.168.115 /user: ""
Se ha completado el comando correctamente.

C:\>
```

**Figura 4.10: Ejemplo de Sesión Nula**

Al ejecutar este comando y obtener una respuesta satisfactoria se ha iniciado una sesión nula con la máquina a ser atacada. Para realizar ataques de enumeración se utiliza la herramienta Nete, se coloca la siguiente línea en el *prompt* del sistema desde el subdirectorio donde se encuentre el programa Nete y se coloca el comando que

indica la figura 4.11.

```
F:\herramientas hacker>nete /U \\161.196.168.113
NetE v1.0 Questions, comments, bitches and bugs to sirdystic@cultdeadcow.com

NetRemoteComputerSupports():
  Remote Admin Protocol
  Remote Procedure Protocol
  SAM Protocol
  Unicode

NetWkstaGetInfo() Level 102:
Error 5 getting workstation info: Acceso denegado.
NetWkstaGetInfo() Level 101:
Error 5 getting workstation info: Acceso denegado.
NetWkstaGetInfo() Level 100:
Computer name: 78CCLGC
Platform:      NT v5.0
Lan group:     CANTU

NetWkstaUserEnum() Level 1:
Username:      78CCLGC$
Logon server:
Logon domain:  CANTU
Other domains:

Username:      jhern4
Logon server:  ALPHA02
Logon domain:  CANTU
Other domains:
```

**Figura 4.11: Resultado del Ataque de Enumeración**

Como se puede observar, se ha obtenido información valiosa (y peligrosa): la plataforma usada por la máquina (Windows NT v 5.0), la red LAN a la que pertenece (CANTV) y algunas cuentas de usuario (78cclgc\$ y jhern4), esta información es la puerta de entrada para los atacantes, no es cuestión de si puede ser atacada es cuestión de cuándo.

#### **4.5.3.1 Contramedidas para ataques de enumeración**

Como se ha mencionado anteriormente, la puerta de entrada para los ataques de enumeración son los puertos TCP 139 y UDP 445, se deben seguir los siguientes pasos para cerrarlos:

Determinar si la máquina no comparte archivos ni impresoras, si es así lo mejor es cerrarlos, en este caso, la máquina de la empresa sólo funcionará como servidor para la aplicación desarrollada, así que sólo el puerto TCP 80 debe estar abierto.

Una vez determinado que se deben cerrar estos puertos, se debe pulsar inicio, ejecutar, y tipear regedit y pulsar enter, con esto se accede al registro de configuración de la computadora. Se busca el siguiente registro:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters y se renombra la clave TransportBindName a TransportBindNameX.

Luego desde el *prompt* del sistema se coloca el comando Netstat -an para verificar si se cerraron los puertos, como se muestra en la figura 4.12.

```
C:\>netstat -an
Conexiones activas

Proto  Dirección local          Dirección remota          Estado
TCP    0.0.0.0:80                0.0.0.0:0                 LISTENING
TCP    0.0.0.0:135               0.0.0.0:0                 LISTENING
TCP    0.0.0.0:1043              0.0.0.0:0                 LISTENING
TCP    0.0.0.0:2701              0.0.0.0:0                 LISTENING
TCP    0.0.0.0:2702              0.0.0.0:0                 LISTENING
TCP    0.0.0.0:4445              0.0.0.0:0                 LISTENING
TCP    0.0.0.0:6129              0.0.0.0:0                 LISTENING
TCP    0.0.0.0:9495              0.0.0.0:0                 LISTENING
TCP    0.0.0.0:45417             0.0.0.0:0                 LISTENING
TCP    127.0.0.1:1074            127.0.0.1:6139            ESTABLISHED
TCP    127.0.0.1:6139            0.0.0.0:0                 LISTENING
TCP    127.0.0.1:6139            127.0.0.1:1074            ESTABLISHED
TCP    127.0.0.1:62514           0.0.0.0:0                 LISTENING
UDP    0.0.0.0:161                ***
UDP    0.0.0.0:1027               ***
UDP    0.0.0.0:1050               ***
UDP    0.0.0.0:1055               ***
UDP    0.0.0.0:1097               ***
UDP    127.0.0.1:62514           ***
UDP    161.196.169.60:5000        ***
UDP    161.196.169.60:4500        ***

C:\>_
```

**Figura 4.12: Resultado del Comando Netstat que Indica las Conexiones Activas del Servidor con Otras Maquinas.**

Al observar la tabla, es notorio el hecho que ninguno de los puertos de riesgo está abierto. Por ende la computadora servidor está lista para trabajar.

## CONCLUSIONES

En el presente capítulo se ilustrarán las conclusiones a las que se pudo llegar al realizar el proyecto

Como se puede observar a menos que sea extremadamente necesario no se deberían tener abiertos los puertos de servicio remoto de la computadora, ya que esto presentaría un riesgo severo en la seguridad del servidor.

Configurar un servidor con todos los elementos de seguridad es lo más importante para el proyecto, ya que la información de los recorridos de fibra óptica es sumamente delicada y si cae en malas manos puede poner en peligro las comunicaciones de todo el país con todos los riesgos que esto conlleva.

Se pudo tomar control absoluto del OTDR desde cualquier computador que previa autenticación, se encuentre conectado a Internet; pero según se ha hecho público en algunos foros y sitios de seguridad, la vulnerabilidad detectada en el escritorio remoto podría ser utilizada para realizar ataques de denegación de servicio (DoS), mediante peticiones creadas maliciosamente.

A menos que sea extremadamente necesario no se deberían tener abiertos los puertos de servicio remoto de la computadora, ya que esto presentaría un riesgo severo en la seguridad del servidor, entonces para iniciar el escritorio remoto se tienen que abrir estos puertos. Por lo que no queda otra opción que prescindir de este método

Asimismo, como se puede ver este ambiente no es muy amigable, ya que se tienen que realizar una serie de pasos, como iniciar el escritorio remoto e iniciar una sesión de Hyperterminal con los parámetros correctos para establecer la conexión con el OTDR, lo que complicaría el uso a los empleados que se encargan de reparar las fibras ópticas de CANTV que serían los beneficiarios de este proyecto.



La mejor opción es utilizar una VPN y dentro de ella configurar un servidor para que aloje el programa Where como una página Web. Las VPN son una excelente opción para abaratar los costos que puede significar el pagar una conexión de alto coste, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red. Además, Una VPN básica, crea un camino privado a través de Internet. Esto reduce el trabajo y riesgo, impidiendo el acceso a usuarios no autorizados a la red.

El proceso de autenticación de usuario es crítico, ya que éste impide la entrada de usuarios no autorizados que se encuentren dentro de la red y permite un control centralizado y sencillo de los recursos a los cuales tienen acceso los usuarios.

Los ataques de enumeración son devastadores ya que dan información valiosa de cualquier computadora que no esté protegida, como son, nombres de usuario, sistema operativo y red LAN a la cual pertenece, por esta razón impedir estos ataques deben ser prioridad número uno cuando se monte un servidor. Por esto es imperativo cerrar los puertos antes mencionados si no se comparten archivos e impresoras como es el caso de nuestro servidor.

Gracias a este proyecto, es posible bajar los tiempos de respuesta en aproximadamente una hora o más, esto da como resultado que los tiempos en los que el servicio de telefonía o Internet estén caídos sean menores, haciendo que las molestias causadas por cortes en la fibra óptica sean mínimas.

Además la versatilidad de haber utilizado páginas Web y servidores, permite que se pueda implementar en todo el territorio nacional y ser monitoreado desde un punto central para mayor eficiencia, en este caso desde el CORE o núcleo de CANTV, simplemente instalando este sistema en todos los estados, lo único que se debe hacer adicionalmente es digitalizar las rutas y crear la base de datos, ya que la estructura del programa de forma modular permite el acceso a cualquier base de datos, siguiendo ciertos parámetros, según lo que se requiera en cada estado del país.

## RECOMENDACIONES

La página Web debería ser montada en un servidor con mayor capacidad, y que sea dedicado a este propósito ya que en la actualidad el servidor es una máquina muy lenta y es usada por el personal del departamento.

El servidor debería ser montado en un sistema LINUX ya que el programa Apache en su versión para Windows tiene muchas limitaciones con los comandos de configuración, de hecho el programa Apache originalmente fue diseñado para trabajar en dicho sistema operativo.

El *switch* mecánico permitió escoger diferentes rutas de fibra óptica, reduciendo el costo de tener un OTDR por fibra; sin embargo la mejor opción es colocar switch óptico ya que éste puede funcionar en diversos ODF sin necesidad de alinear las fibras, ya que actúa como un multiplexor donde todas las fibras se conectan a este a través de tantos cables conectores o *patch cord* como fibras existan y un sólo *patch cord* sale del switch al OTDR escogiendo la ruta deseada.

## REFERENCIAS BIBLIOGRAFICAS

- [1] Wikipedia. Fibra Óptica.- EN:  
[http://es.wikipedia.org/wiki/Cable\\_de\\_fibra\\_%C3%B3ptica](http://es.wikipedia.org/wiki/Cable_de_fibra_%C3%B3ptica).- Libro en línea, (2008).  
[Consulta: 2008, Febrero]
- [2]Platea. La fibra Óptica.- EN: <http://platea.pntic.mec.es/~lmarti2/fibra.htm>.-  
[Consulta:2007, Diciembre]
- [3] Wikipedia. Compañía Anónima Nacional Teléfonos de Venezuela.- EN:  
<http://es.wiki.wikipedia.org/wiki/CANTV>  
.- Libro en línea, (ultima revisión 2008). [Consulta: 2007, Octubre]
- [4] Wikipedia. TCP-IP.- EN:  
[http://es.wikipedia.org/wiki/Capas\\_o\\_niveles\\_del\\_TCP/IP](http://es.wikipedia.org/wiki/Capas_o_niveles_del_TCP/IP)  
.- Libro en línea, (ultima revisión 2008). [Consulta: 2007, Octubre]
- [5] Wikipedia. CSMA/CD.- EN: <http://es.wikipedia.org/wiki/CSMA/CD> .- Libro en línea, (ultima revisión 2008). [Consulta: 2008, Octubre]
- [6] Wikipedia. Red Privada Virtual.- EN:  
[http://es.wikipedia.org/wiki/Red\\_privada\\_virtual](http://es.wikipedia.org/wiki/Red_privada_virtual)  
.- Libro en línea, (ultima revisión 2008). [Consulta: 2007, Octubre]
- [7] Wikipedia. Página Web.- EN:  
[http://es.wikipedia.org/wiki/Dise%C3%B1o\\_de\\_p%C3%A1ginas\\_web](http://es.wikipedia.org/wiki/Dise%C3%B1o_de_p%C3%A1ginas_web)  
.- Libro en línea, (ultima revisión 2008). [Consulta: 2007, Octubre]
- [8]Depeca. Puerto Serial.- EN:  
<http://www.depeca.uah.es/alcabot/seminario2006/Trabajos/JoseManuelMurciaBarba.pdf>. [Consulta: 2007, Octubre]
- [9] Wikipedia. Puerto Paralelo.- EN:  
[http://es.wikipedia.org/wiki/Puerto\\_de\\_impresora](http://es.wikipedia.org/wiki/Puerto_de_impresora)  
.- Libro en línea, (ultima revisión 2008). [Consulta: 2007, Noviembre]
- [10]Nireblog. Frame Relay.- EN <http://frame-relay.nireblog.com/post/2006/10/17/frame-relay>.- Libro en línea, (2008). [Consulta:]

## BILIOGRAFÍA

\_\_\_\_\_ . **Authentication, Authorization and Access Control for Apache servers,**

<http://httpd.apache.org/docs/1.3/howto/auth.html#basicconfig> .

Jones Keith, Shema Mike y Johnson Bradley C.: (2003). **Superutilidades Hackers**. Barcelona, España: McGraw Hill / Interamericana de España S. A. U.

\_\_\_\_\_ . **Gobierno de España Ministerio de Educación.**

<http://platea.pntic.mec.es>

\_\_\_\_\_ . **Nireblog.**

<http://nireblog.com/es>

\_\_\_\_\_ . **PHP Garage, Port COM Access.**

[http://phpa-bender.phparch.com/discuss/index.php/m/2980/0/#msg\\_2980](http://phpa-bender.phparch.com/discuss/index.php/m/2980/0/#msg_2980) .

Rodríguez G., Abraham. (2005). **PHP5 a través de ejemplos**. Madrid, España. Alfaomega Grupo Editor.

\_\_\_\_\_ . **Seguridad en las Redes de Comunicaciones.**

<http://www.iec.csic.es/CRIPTonOMICon/seguridad/> .

Scambray, Joel. (2003): **Hackers 4**. Barcelona, España: McGraw Hill / Interamericana de España S. A. U.

Shema, Mike. (2004): **Claves Hackers de Sitios Web**. Barcelona, España: McGraw Hill / Interamericana de España S. A. U.

\_\_\_\_\_ . **Universidad de Alcalá Departamento de Electrónica.**

<http://www.depeca.uah.es>

\_\_\_\_\_ . **Wikipedia La Enciclopedia Libre.**

<http://es.wikipedia.org/wiki/Portada>

## ANEXOS

### A.1 Código para mover el motor a la izquierda en lenguaje C++

```
#include<time.h>

#include<stdio.h>

#include<CONIO.H>

int b[4];

void main ()

{      int a,i,j,n;

outport (888,15);

delay (1000);

        a=7;

        b[0]=14;

        b[1]=13;

        b[2]=11;

        b[3]=7;

        i=0;

        j=0;
```

```

        n=1000;
        do
            {
                if (i==4)
                    {
                        i=0;
                    }
                output (888,b[i]);
                delay (a);

                i=i+1;
                j=j+1;
            } while (j!=n);

    delay (500);
    output(888,79);
}

```

## A.2 Código para mover el motor a la derecha en lenguaje C++

```

#include<time.h>

#include<stdio.h>

#include<CONIO.H>

int b[4];

```

```
void main ()
{
    int a,i,j,n;

    outport (888,15);

    delay (500);

    a=7;

    b[0]=7;
    b[1]=11;
    b[2]=13;
    b[3]=14;
    i=0;
    j=0;
    n=1000;
    do
    {
        if (i==4)
        {
            i=0;
        }
        outport (888,b[i]);
    }
}
```

```
delay (a);
```

```
i=i+1;
```

```
j=j+1;
```

```
} while (j!=n);
```

```
outport (888,79);
```

```
}
```