Instituto Tecnológico de Costa Rica

Escuela de Ingeniería en Electrónica

Sistema de enlace hacia una red redundante entre las centrales telefónicas y el SICAT

Informe de Proyecto de Graduación para optar por el título de Ingeniero en Electrónica con el grado académico de Licenciatura

Carolina Arze Carrión

Cartago, Junio del 2008

INSTITUTO TECNOLOGICO DE COSTA RICA

ESCUELA DE INGENIERIA ELECTRONICA

PROYECTO DE GRADUACIÓN

TRIBUNAL EVALUADOR

Proyecto de Graduación defendido ante el presente Tribunal Evaluador como requisito para optar por el título de Ingeniero en Electrónica con el grado académico de Licenciatura, del Instituto Tecnológico de Costa Rica.

Miembros del Tribunal

Ing. José David Gómez Tames

Profesor lector

Ing. Julio Stradi Granados

Profesor lector

Ing. Eduardo Interiano Salguero

Profesor asesor

Los miembros de este Tribunal dan fe de que el presente trabajo de graduación ha sido aprobado y cumple con las normas establecidas por la Escuela de Ingeniería Electrónica

Escuela de Ing. Electrónica, *25/06/2008*

TEC
Instituto Tecnológico de Costa Rica
Escuela de Ingeniería Electrónica

Declaro que el presente Proyecto de Graduación ha sido realizado enteramente por mi persona, utilizando y aplicando literatura referente al tema e introduciendo conocimientos propios.

En los casos en que he utilizado bibliografía, he procedido a indicar las fuentes mediante las respectivas citas bibliográficas.

En consecuencia, asumo la responsabilidad total por el trabajo de graduación realizado y por el contenido del correspondiente informe final.

Instituto Costarricense de Electricidad (ICE), 25/06/2008

Firma del autor

Carolina Arze Carrión

Céd: *1-11640401*

Resumen:

El Instituto Costarricense de Electricidad (ICE) es la institución encargada de brindar los servicios de electricidad y telecomunicaciones a todo el país. Este se conforma por varias plataformas, cada una compuesta por múltiples divisiones.

Dentro de la Plataforma de Servicios, en la división de Redes y Sistemas se brindan servicios de mantenimiento y reparación de averías relacionadas con los servicios de telefonía fija. En la actualidad existe una gran problemática en cuanto a las averías en la red de las centrales de telefonía fija. Estas presentan tres tipos de averías: de red, de captura y de puerto.

Existe un sistema corporativo llamado SICAT, ubicado en un servidor en el ICE de San Pedro, por el cual se obtiene información necesaria de las centrales telefónicas así como por el cual se pueden enviar comandos para su configuración. Las transacciones que realiza el SICAT son enviadas por la red institucional hacia unas computadoras llamadas frontales ubicadas en cada central telefónica. El frontal contiene varias aplicaciones las cuales sirven de mediador entre el SICAT y la central telefónica.

Gran parte de las averías de captura y de puerto se deben a la existencia de un frontal o PC como mediador. Por ello se pretende centralizar la red de frontales mediante unos dispositivos llamados Terminal Servers (TS). Los frontales serán remplazados por TS los cuales enviarán la información a un único frontal que estará ubicado en el ICE de San Pedro.

Con esto se soluciona gran parte de las averías de captura y de puerto, mas no se presenta ninguna mejora para las averías de red. Actualmente existen grandes problemas con las averías de red, las cuales han llegado a durar más de un día.

Por este motivo, se pretende desarrollar un sistema de enlace de red redundante, por el cual sea factible tener comunicación alterna con las centrales telefónicas en caso de que ocurra una avería de red.

Palabras claves: Frontal, SICAT, avería, red, ICE, sistema corporativo, enlace redundante, central telefónica.

Abstract:

Costarrican Electricity Institute (ICE) is the national institute in charge of supplying telecommunications and electricity to Costa Rica. This Institute is organized in different platforms and each one in several divisions.

The network and systems division, in Service Platform has been given maintenance and repair of failures related with fixed telephony services. In these days there is an existing problem in the network of fixed telephony services centrals. There are three types of failures: network, capture and port failure.

There is a corporate system called SICAT, located in a ICEs server in San Pedro, Montes de Oca. This server gathers necessary information form telephonic central as well as send commands for its configuration. SICATs transactions are sent trough institutional network to computers called “frontales” located en each central. The frontal has many applications used as mediator between SICAT and the central telephony.

Great part of the port and capture failures are caused by the existence of a frontal or PC as mediator. That’s why this project pretends to centralize the frontal network using Terminal Servers (TS),

This will solve great part of the capture and port failures, mean while this won’t improve network failures. For this other problem will be developed a redundant network system, to have backup in case of a network failure.

Keywords: Frontal, SICAT, failure, network, ICE, corporate system, redundant network, telephony central.

Dedicatoria:

Dedico este proyecto a mi madre María del Carmen Carrión de Arze y a mi padre José Agustín Arze Borda.

Agradecimiento:

Agradezco el apoyo y ayuda durante la elaboración del proyecto a los ingenieros:

Ing. Luís Gonzalez Sandoval
Ing. David Alvarado Oviedo
Ing. Emmanuel Ramírez Segura
Ing. Guillermo Zuñiga Meléndez

INDICE GENERAL

Capitulo 1. Introducción 1
1.1 Problema existente e importancia de su solución 1
1.1.1 Entorno del proyecto 1
1.1.2 Definición del problema 3
1.1.3 Síntesis del problema 4
1.2 Solución seleccionada 4
Capítulo 2: Meta y objetivos 7
2.1 Meta 7
2.2 Objetivo general 7
2.3 Objetivos específicos 7
Capítulo 3: Marco teórico 8
3.1 Descripción del sistema o proceso a mejorar 8
3.1.1 Sistema actual de la red de frontales 8
3.1.2 Cambios que se realizarán al sistema actual de la red de frontales. 11
3.2 Antecedentes bibliográficos 13
3.2.1 Tecnología ISDN [20] 13
3.2.2 Protocolo Telnet y programa Expect de LINUX [17 y 18] 15
3.2.3 Enrutadores con LINUX [13 y 14] 15
3.2.4 Protocolo RIP [21] 16
3.3 Descripción de los principales principios matemáticos relacionados con la solución del problema 17
3.3.1 Confiabilidad de un sistema [19 y 16] 17
Capítulo 4: Procedimiento metodológico 19
4.1 Reconocimiento y definición del problema 19
4.2 Obtención y análisis de información 27
4.3 Evaluación de las alternativas y síntesis de una solución 28
4.4 Implementación de la solución 29
Capítulo 5: Descripción detallada de la solución (Explicación del diseño) 37
5.1 Análisis de soluciones y selección final 37
5.2 Descripción de software 40

Capítulo 6: Análisis de Resultados 47
6.1 Resultados 47
6.2 Cálculo del tiempo de ejecución del *script* 48
6.2 Cálculo de la confiabilidad del sistema 51
6.2 Análisis 53
Capítulo 7: Conclusiones y recomendaciones 57
7.1 Conclusiones 57
7.2 Recomendaciones: 58
Bibliografía 59
Apéndices 62
A.1 Glosario, abreviaturas y simbología 62
A.2 Información sobre la empresa/institución 64
Anexos 65

INDICE DE FIGURAS

Figura 1.1 Diagrama esquemático de la nueva topología para la conexión de una central telefónica el servidor SICAT ……..……...….6

Figura 3.1 Conexión del 81% de las centrales telefónicas……10

Figura 3.2 El restante 19% de los frontales se encuentra conectado de esta forma. Esto en lugares muy alejados donde no hay acceso a la red del ICE……..10

Figura 3.3 Diagrama esquemático del nuevo sistema de red

de frontales…….....12

Figura 3.4 Opciones de acceso ISDN……..14

Figura 4.1 Averías ocurridas desde febrero del 2007 hasta marzo del 2008…….……23

Figura 4.2 Duración de las averías de red ocurridas desde febrero del 2007 hasta marzo del 2008…….....24

Figura 4.3 Cantidad de averías de red por mes desde febrero del 2007 hasta marzo del 2008……...25

Figura 4.4 Cantidad de averías de red que ocurrieron simultáneamente desde febrero del 2007 hasta marzo del 2008……..26

Figura 4.5 Ejemplo del sistema de conexión entre módems propuesto inicialmente……..31

Figura 4.6 Ejemplo del sistema de conexión entre módems

propuesto finalmente……..…32

Figura 4.7 Topología de prototipo……....35

Figura 4.8 Topología final propuesta, con enlaces redundantes……36

Figura 5.1 Propuesta para la solución seleccionada…..……39

Figura 5.5 Diagrama de *script*……43

Figura 5.6 Diagrama de flujo del *script* principal……..46

Figura 6.1 Imagen de los resultados del *script* después de realizar la conexión del los módems y el enrutamiento de los paquetes……49

Figura 6.2 Módems ISDN conectados……50

INDICE DE TABLAS

Tabla 6.1 Tiempos de ejecución del *script* para la medición de la duración en conectar los módems y realizar el enrutamiento (conmutación) de los paquetes a la nueva ruta……47

Tabla 6.2 Tiempos de ejecución del *script* para la medición de la duración en desconectar los módems y realizar el enrutamiento (conmutación) de los paquetes a la ruta por defecto……48

Tabla 6.3 Tiempos de ejecución del *script* para la medición de la duración en agregar una dirección IP en la lista de Pendientes.txt……..……..……48

Capitulo 1. Introducción

1.1 Problema existente e importancia de su solución

1.1.1 Entorno del proyecto

El Instituto Costarricense de Electricidad (ICE), es una institución encargada de brindar servicios de energía y telecomunicaciones a todo el país. Éste consta de dos divisiones, la división Eléctrica y la de Telecomunicaciones. La división de Telecomunicaciones se compone de tres subdivisiones: Redes y Sistemas, Servicios y Servicios al Cliente. Estas subdivisiones se dividen en otras subcategorías llamadas procesos.

El proceso de Plataformas de Servicios de la Dirección Técnica de Operación y Mantenimiento, perteneciente a la División de Redes y Sistemas, se encarga principalmente de la intercomunicación y mantenimiento de redes entre las 67 centrales de telefonía fija del ICE, ubicadas en diversas regiones de todo el país. El presente proyecto se encuentra enfocado específicamente en ésta área.

Las centrales telefónicas se comunican con sistemas corporativos quienes se encargan de realizar gestiones de servicios como el aprovisionamiento, corte y reconexión de los servicios de telefonía fija.

La comunicación entre las centrales telefónicas y los sistemas corporativos se realiza mediante el "*Sistema de Categorización Automática*" (SICAT).

El SICAT es un *software* administrativo, que se encuentra en la intranet del ICE y una de sus funciones es servir como mediador para la comunicación entre las centrales telefónicas y los sistemas corporativos. Además, dicho sistema es utilizado por personal de agencias y servicio al cliente para aprovisionamiento de servicios telefónicos, cambios de categorías, casilleros de voz de telefonía fija y TDMA, también se utiliza para proporcionar información sobre ADSL en todas las tecnologías del ICE.

Actualmente, la comunicación entre la central telefónica y el servidor SICAT, se realiza mediante una computadora cliente llamada “frontal”, éste se comunica a la central telefónica por medio de un puerto serial (RS232) y recibe la información del SICAT a través de una conexión Ethernet, es decir por medio de Internet. El frontal cuenta con una aplicación que se encarga de convertir la información de la central telefónica para poder enviarla por Internet a la red del ICE o viceversa.

Cabe mencionar que todas las 67 centrales de telefonía fija del país son de diferentes marcas, como por ejemplo, SIEMENS, ERICCSON, ALCATEL, entre otras. Esta situación repercute en la programación de la aplicación del frontal ya que cada marca de cada central telefónica tiene su propio lenguaje. Por este motivo, si se presentan problemas con la aplicación del frontal, un técnico especializado en la aplicación específica de las 67 existentes debe trasladarse a la zona donde se encuentra la central telefónica para poder solucionar el problema. También, pueden ocurrir daños físicos en el frontal lo cual implica un desplazamiento por parte del equipo técnico para su reparación. Esto genera grandes pérdidas en costos de mantenimiento y reparación del los frontales además de los costos en capacitación de personal especializado.

De acuerdo a lo mencionado anteriormente, se pueden destacar los siguientes puntos conflictivos que presenta la red de frontales actual:

1. Computadoras con *software* diseñado específicamente para cada tipo de central telefónica. Esto debido a que cada central telefónica es de diferente marca, lo cual implica un lenguaje de programación distinto.
2. Equipo electrónico que requiere de un ambiente idóneo. Los frontales son equipos que deben de mantenerse en constante funcionamiento, durante las 24 horas del día, los 365 días del año, esto implica que se deben de tomar en cuenta aspectos como la climatización del lugar donde se encuentran los frontales, para evitar un sobrecalentamiento del equipo.

3. Seguridad requerida por los equipos, en cuanto a posibles daños físicos de los frontales por personas no habilitadas para su manejo.
4. Limitado número de personal capacitado a cargo de los equipos a nivel nacional, esto debido a la complejidad del equipo remoto (frontal).

Sin embargo, una de las ventajas que presenta la red de frontales actual es el almacenamiento de la información en caso de que la red del ICE se desconecte. Los datos de la central telefónica quedan almacenados en el disco duro de la computadora, por lo que nunca se presentan pérdidas de la información.

1.1.2 Definición del problema

Debido a la necesidad de que exista un frontal por cada central telefónica y los problemas que esto conlleva, se plantea centralizar la red de frontales para que de esta manera se puedan reducir las 67 computadoras a solamente una. Así se ahorrarían las pérdidas en reparación y mantenimiento de equipo y en capacitación de personal técnico.

La centralización consiste en tomar el frontal de cada central telefónica y sustituirlo por un dispositivo que comunique dicha central telefónica con el servidor del SICAT a través de la red del ICE. El inconveniente es que si la red del ICE falla, la información enviada se pierde. Por lo que el punto clave para que la centralización sea factible, es, realizar la centralización garantizando que la conexión entre la central telefónica y el SICAT casi nunca se pierda.

De esta forma si se logra una conectividad estable, no existirán problemas de pérdida de información por lo que no se requerirían sistemas de almacenamiento (computadoras) y con esto se evitan los gastos en mantenimiento y reparación de equipo.

1.1.3 Síntesis del problema

El problema radica básicamente en la inexistencia de un sistema que permita una conexión redundante de red entre las centrales telefónicas y el SICAT.

1.2 Solución seleccionada

Para solucionar el problema detallado con anterioridad, se pretende diseñar un sistema que sustituya los frontales actuales para lograr una centralización y que a su vez garantice la conectividad de la central telefónica con el SICAT. Con ello se pretende maximizar la disponibilidad de los frontales, minimizar la cantidad de equipos administrados y delegar a cada zona de mantenimiento un equipo más sencillo, fácil de diagnosticar y simple de mantener.

Una posible solución para garantizar una conectividad constante, es utilizar una red alterna. Entonces, cada vez que la red principal, que es la red del ICE, se desconecte, el sistema deberá conmutar a la otra red.
El ICE cuenta con una red privada llamada Red Digital de Servicios Integrados (RDSI), ésta puede ser utilizada como una red redundante. Además para que el sistema pueda realizar la conmutación, necesita detectar cuándo una red falla.
Este sistema deberá realizar una conversión de la información de una entrada serie a paquetes de información para poder ser enviadas por el protocolo 802.3 o Ethernet y viceversa, para ello se puede utilizar microprocesadores como el PIC Ethernet, Enrutadores y *Terminal Servers*.

La figura 1.1 muestra un diagrama del la solución propuesta, en ella se puede observar que el sistema diseñado para evitar la pérdida de comunicación entre la central telefónica y el SICAT debe colocarse después de la central telefónica y antes del servidor del SICAT, de esta forma se realizará una codificación de la información de la central telefónica a paquetes de

información y luego se decodificarán para poder ser leídas nuevamente por un puerto serie correspondiente al del servidor del SICAT.

Cabe destacar que en el Servidor del SICAT, debe de existir un sistema que detecte el destino de la información o bien la central telefónica de donde viene, ya que debido a que todas las centrales telefónicas trabajan con lenguajes diferentes, la aplicación que se programará en el único frontal debe ser compatible con todas las centrales telefónicas.

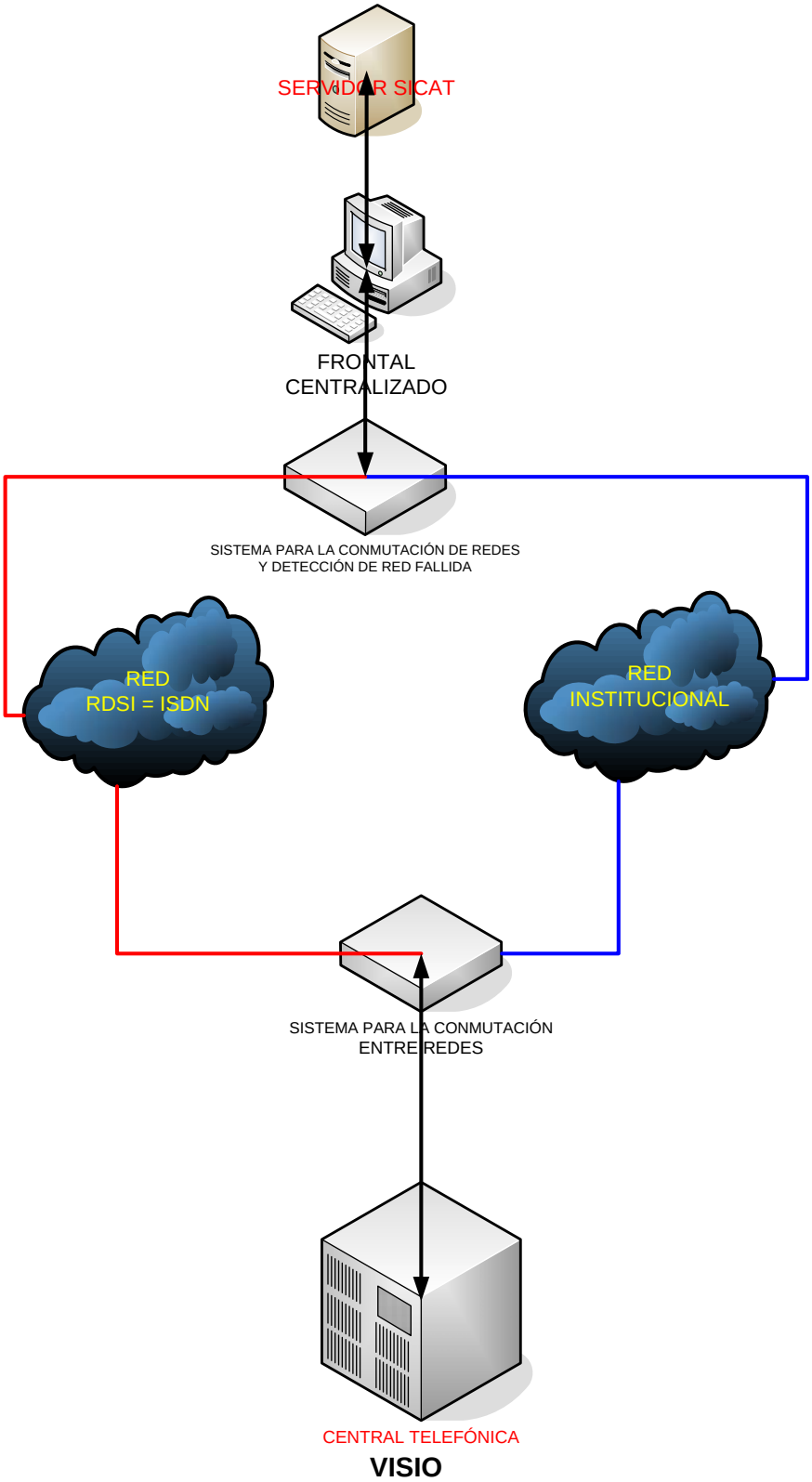


Figura 1.1 Diagrama esquemático de la nueva topología para la conexión de una central telefónica el servidor SICAT

Capítulo 2: Meta y objetivos

2.1 Meta

Reducir casi en su totalidad las averías de red.

Indicador: Reducir las averías de red en un 80 %.

2.2 Objetivo general

Desarrollar un sistema que garantice la comunicación entre la central telefónica y el SICAT.

Indicador: Garantizar el envío y recepción de paquetes en un 90%.

2.3 Objetivos específicos

- Desarrollar un sistema que detecte cuándo se pierde el enlace de red entre las centrales telefónicas y el SICAT.

  Indicador: Detectar la falla en un tiempo máximo de 5min.

- Desarrollar un sistema que permita realizar la conmutación entre redes del lado del servidor SICAT.

  Indicador: Garantizar un tiempo máximo de 30seg desde que se detecta la falla hasta que se establece el nuevo enlace.

- Desarrollar un sistema que permita realizar la conmutación entre redes del lado de la central telefónica.

  Indicador: Garantizar en un 99.5% la conmutación entre enlaces, desde que se detecta una falla en la conexión por la red institucional.

Capítulo 3: Marco teórico

3.1 Descripción del sistema o proceso a mejorar

3.1.1 Sistema actual de la red de frontales

El sistema actual de la red frontal se conforma de un frontal, conectado por RS-232, a cada central telefónica. Los frontales se comunican por medio de Ethernet a la red del ICE, en donde se encuentra el sistema corporativo SICAT.
En los frontales se encuentran dos tipos de aplicaciones:

- Aplicaciones que funcionan entre el SICAT y los frontales, como por ejemplo, una aplicación para la comprobación de la llegada de la información al frontal.
- Aplicaciones entre el frontal y la central telefónica, como por ejemplo, una aplicación que archiva todas las funciones que realiza la central telefónica, para llevar una bitácora de su funcionamiento.

El lenguaje de programación de las aplicaciones en los frontales difiere entre las marcas de las centrales telefónicas. Existen 5 marcas de centrales telefónicas: Ericsson, ALCATEL, SIMENS, NORTEL DMS - 10, NORTEL DMS - 100.

Actualmente existen tres tipos de aplicaciones:
SCAMONITOR (Operador Virtual): Esta es la aplicación más importante. Se encuentra en cada uno de los frontales y se encarga de traducir la información que llega del SICAT al lenguaje respectivo al tipo de central telefónica, además, divide la información en tramas para poder ser enviada a la central telefónica.

Calendario: Esta aplicación se encarga de mandar observaciones que se desean evaluar en la central telefónica, estas observaciones se envían desde el frontal directamente a la central telefónica.

Conteo: Esta aplicación detecta una avería en el frontal.

En la actualidad se presentan tres tipos de averías en la red de frontales, averías de red, de puerto y de captura. Las causas por las que estas averías pueden ocurrir son las siguientes:

Averías de Red: Pueden ser causadas por problemas en la red institucional en diferentes regiones del país.

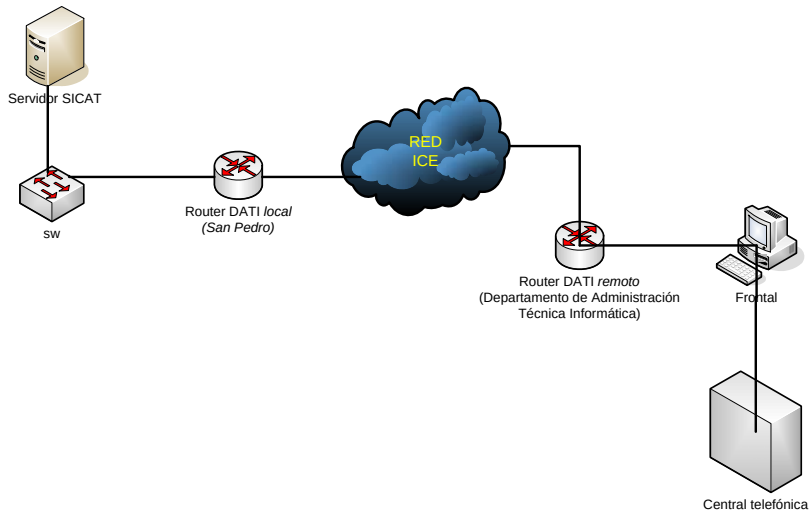
Averías de Captura y de Puerto:

Estas pueden ser originadas porque:

- La terminal de una central telefónica se encuentre fuera de servicio.
- Se envía información errónea de una central telefónica al frontal.
- Problemas de paridad y velocidad de la información enviada entre una centra y el frontal.
- Que el planificador de tareas (Cron) del frontal se encuentre retenido.
- Que el frontal presente procesos repetidos.
- Problemas de configuración en la terminal del frontal.
- Tiempos del sistema y del frontal dessincronizados.
- Velocidades entre puertos distintas.

Existen dos topologías para la comunicación entre los frontales y el SICAT ilustradas en las figuras 3.1 y 3.2:

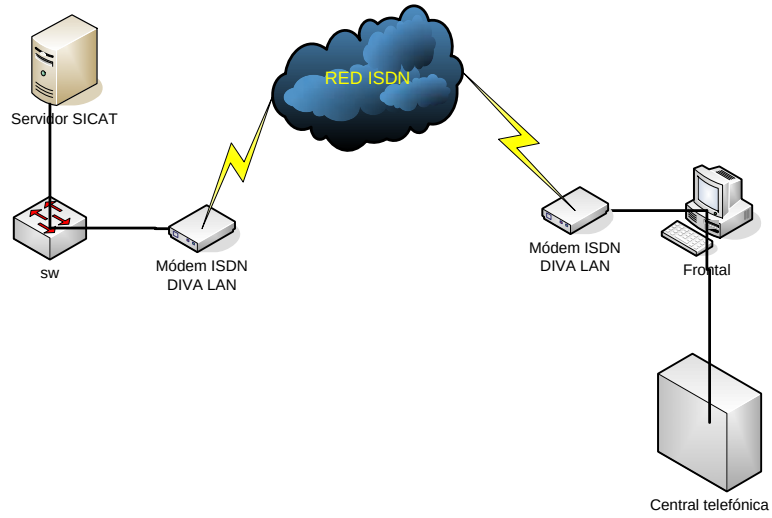
Forma 1: Por medio de la red institucional. (Conexión del 81% de las centrales telefónicas se encuentran conectadas de esta forma)



VISIO

Figura 3.1 Conexión del 81% de las centrales telefónicas

Forma 2: Por medio de la red telefónica ISDN o RDSI. (Conexión del 19% de las centrales telefónicas)



VISIO

Figura 3.2 El restante 19% de los frontales se encuentra conectado de esta forma. Esto en lugares muy alejados donde no hay acceso a la red del ICE.

3.1.2 Cambios que se realizarán al sistema actual de la red de frontales.

Para la centralización de la red de frontales se sustituirán todos los frontales por TS y existirá un frontal principal, el cual será el mediador entre el servidor del SICAT y todas las centrales telefónicas del país. En la figura 3.3 se demuestra un diagrama esquemático de cómo será la nueva red de frontales.

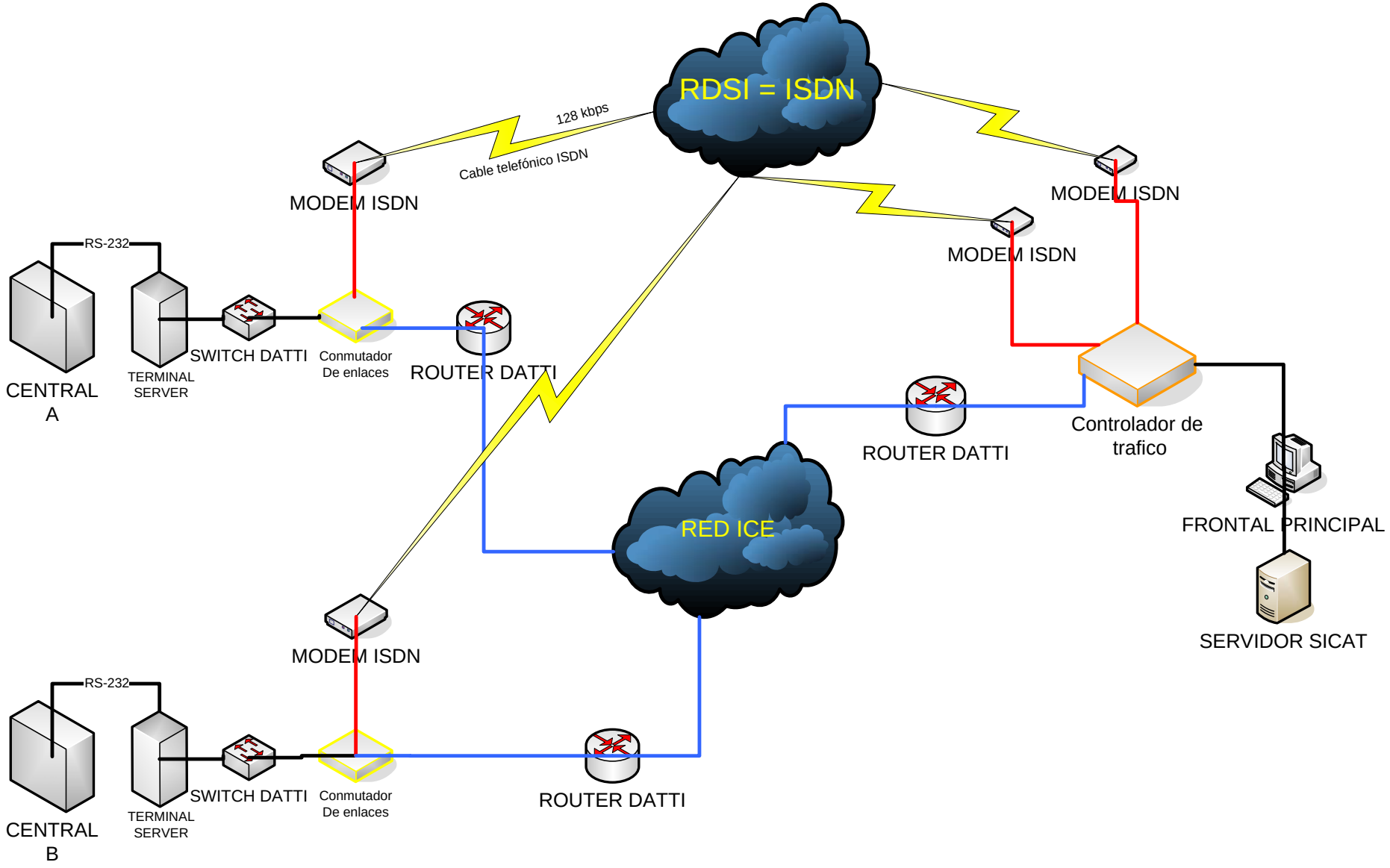
Con la centralización de los frontales se pretende reducir la gran mayoría de las averías de puerto y de captura que se dan actualmente con los frontales de cada central telefónica.

Este proyecto se centra en la reducción de las averías de red. Para esto existirá una ruta alterna de comunicación en caso de que la red institucional falle. Esta vía alterna de comunicación entre los frontales y el SICAT, se realizará por medio de un enlace ISDN o RDSI.

Para establecer la conexión, se colocarán módems ISDN en cada central telefónica y otros módems donde se encuentra el controlador de tráfico.

El controlador de tráfico, será un programa en Linux que detectará cuando una red falla y en caso de que falle, el sistema deberá determinar qué MODEM ISDN se encuentra desocupado y establecer una llamada al MODEM ISDN de la central telefónica donde la conexión de la red del ICE falló.

El motivo por el cual se realiza una conexión ISDN es que el ancho de banda (128 kbps) es mayor al del sistema telefónico analógico (52 kbps), además el tiempo para establecer la conexión es mucho menor a que si se usara una conexión por telefonía analógica.



VISIO

Figura 3.3 Diagrama esquemático del nuevo sistema de red de frontales

3.2 Antecedentes bibliográficos

3.2.1 Tecnología ISDN [20]

ISDN (Red Digital de Sevicios Integrados) es una de las tecnologías WAN creadas para brindar acceso a redes desde lugares remotos.

La tecnología ISDN permite el uso de datos digitales (voz, video y datos) a través de un mismo cable telefónico usado en las líneas telefónicas, esta fue creada para solucionar los problemas de ancho de banda que existían con los circuitos las centrales telefónicas analógicas.

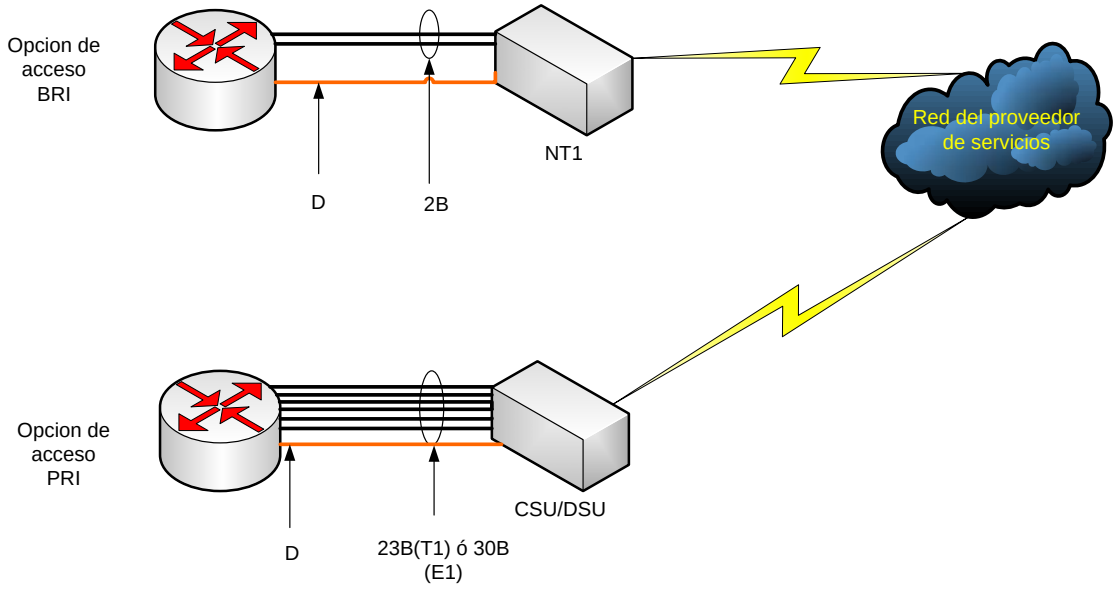
Algunos de los beneficios de las ISDN son [20]:

- Transportan varios tipos de información como datos, voz y video.
- Las llamadas se realizan más rápido que con conexiones de módem.
- La tasa de transferencia de los canales B es mayor que la de los módems.
- Los canales B son más apropiados para conexiones con el Protocolo de punto a punto (PPP) que con los módems.

Existen dos tipos de canales en las líneas ISDN, cada uno tiene una velocidad de transmisión distinta.
El primer canal es llamado canal B, transmite a una velocidad de 64kbps, en este canal se puede transmitir cualquier tipo de datos digitalizados en modo *full duplex*, como por ejemplo, voz, datos y video. En este canal la información se transporta en el formato de tramas mediante el control de enlace de datos de alto nivel (HDLC) o el protocolo PPP.

El segundo canal, es llamado el canal D, transporta la información de control para el canal B, como por ejemplo, mensajes de señalización tales como establecimiento y corte de llamada. Emplea el protocolo LAPD y transmite a una velocidad de 16Kbps para una interfaz de acceso básico (BRI) y 64Kbps para una interfaz de acceso principal (PRI).

La interfaz BRI utiliza dos canales B de 64 Kbps cada uno, más un canal D de 16 Kbps. En América del Norte y Japón, la interfaz PRI ofrece veintitrés canales B de 64 Kbps y un canal D de 64 Kbps. En la figura 3.4 se puede observar un diagrama esquemático de las opciones de acceso ISDN.



Canal	Capacidad	Se usa en gran media para
B	64 kbps	Datos conmutados por circuitos (HDLC; PPP)
D	16/64 kbps	Información de señalización (LAPSD)

VISIO

Figura 3.4 Opciones de acceso ISDN

3.2.2 Protocolo Telnet y programa Expect de LINUX [17 y 18]

Para realizar la configuración de los módems ISDN desde el *script*, se utilizó el programa Expect.
El programa Expect nace de la necesidad de automatizar las aplicaciones interactivas que requerían que el usuario ingresara información por el teclado. Principalmente Expect se mantiene escuchando a las instrucciones que salen en la pantalla, y si estos siguen un modelo establecido por el usuario, entonces Expect envía un mensaje u otra instrucción.

Para configurar el módem ISDN por la interfaz de la línea de instrucciones (CLI), se debía ingresar a éste por medio del protocolo Telnet. El protocolo Telnet (TELecomunication NETwork), es un protocolo de red que permite ingresar a una máquina o dispositivo desde otra máquina sólo en modo terminal o desde la pantalla de comandos.

De esta forma con el comando expect se logra ingresar y configura al módem ISDN mediante el protocolo Telnet.

3.2.3 Enrutadores con LINUX [13 y 14]

Para la conmutación del lado del servidor SICAT se utilizó la herramienta de LINUX llamada *route*, esta función permite configurar las rutas, es así como incorporar una nueva ruta estática en la máquina.
Recibe los siguientes parámetros:

/sbin/route add –-[net|host] [IP] netmask [gw [IP]] dev [interface]

Ejemplo para el caso del prototipo:
/sbin/route add–-net 10.150.1.0 netmask 255.255.255.0 gw 10.149.58.21

De esta forma se direccional, al puerto de enlace 10.149.58.21, todos los paquetes que estén dirigidos a la red 10.150.1.0

3.2.4 Protocolo RIP [21]

El protocolo que se utilizó para la configuración de los enrutadores del prototipo fue el protocolo RIPV2.

Este protocolo utiliza el algoritmo vector distancia para realizar el cálculo del camino más corto hacia la red de destino. La distancia o métrica, es el número de saltos de enrutadores que existe entre la red origen y la red destino y se calcula como la métrica indicada por el enrutador vecino más la métrica para alcanzar a ese vecino.

Las rutas, en este protocolo, tienen un tiempo de vida de 180 segundos, es decir, si no se recibe ninguna confirmación de los enrutadores vecinos que la ruta sigue activa, esta se borra de la tabla de rutas.

Además, la máxima cantidad de saltos que acepta RIP para una ruta son 15 saltos, si la ruta se excede de 15 saltos entonces se considera como infinita y es borrada de la tabla de rutas por lo que el destino es inalcanzable.

Existen dos tipos de mensajes entre enrutadores, los mensajes de petición y los de respuesta. Los de petición se dan, cuando algún enrutador se incorpora a una red y pide información reciente de los enrutadores vecinos.
Los enrutadores de respuesta, pueden ser de tres tipos, los mensajes ordinarios, los cuales se envían cada 30 seg indicando el estado tanto de la ruta como del enlace, los mensajes de respuesta a una petición en específico y los mensajes cuando cambia algún coste, en estos casos se envía toda la tabla de enrutamiento.

3.3 Descripción de los principales principios matemáticos relacionados con la solución del problema

3.3.1 Confiabilidad de un sistema [19 y 16]

La confiabilidad de un sistema indica la probabilidad de que el sistema funcione *sin* fallas, en un periodo de tiempo dado.

Para el cálculo de la confiabilidad de un sistema, primero se debe definir bajo qué sistema se realizará el cálculo. Los sistemas pueden ser series, paralelos, o series-paralelos.

Un sistema serie, se refiere a un sistema que contiene todos sus elementos interconectados, es decir, que cuando falla un componente del sistema, fallan todos los demás. En un sistema paralelo por el contrario, cuando falla un componente del sistema no afecta al resto del sistema.

Si se parte de la suposición de que la razón de falla es constante en el tiempo de vida útil de los componentes de un sistema y denotamos como la razón de falla a λ, entonces, la función de la distribución exponencial de los tiempos de falla es:

$$\boxed{f(t) = \lambda \cdot e^{-\lambda \cdot t}} \qquad \textbf{(1)}$$

O bien

$$\boxed{f(t) = 1 - e^{-\lambda \cdot t}} \qquad \textbf{(2)}$$

Entonces la probabilidad de falla del sistema paralelo, que se compone de dos subsistemas (1 y 2) es:

$$\boxed{f(t) = \left(1 - e^{-\lambda_1 \cdot t}\right) \cdot \left(1 - e^{-\lambda_2 \cdot t}\right)} \qquad \textbf{(3)}$$

Y dado que la confiabilidad es la probabilidad de que el sistema funcione *sin* fallas, se tiene que la confiabilidad del sistema Rk(t) es:

$$\boxed{Rk(t) = e^{-\lambda_1 * t} + e^{-\lambda_2 * t} - e^{-(\lambda_1 + \lambda_2) * t}} \qquad \textbf{(4)}$$

Y la razón de falla es:

$$\lambda = \frac{Tiempo_falla}{Tiempo_total} \qquad \textbf{(5)}$$

Capítulo 4: Procedimiento metodológico

4.1 Reconocimiento y definición del problema

Desde hace varios años el ICE ha presentado la problemática de las averías en la red de frontales, éstas pueden ser de tres tipos: de red, de puerto y de captura. Dada esta situación, el departamento de redes y sistemas planteó como solución la centralización de los frontales para evitar las averías de captura y de puerto, haciendo uso de los terminal servers (TS), sin embargo no se planteó ninguna solución para las averías de red.

La figura 4.1 presenta la cantidad de averías que ocurrieron desde febrero del 2007 hasta marzo del 2008. En esta gráfica se puede apreciar que la mayoría de las averías que ocurrieron son de captura y de puerto, las cuales se pretende reducir con la centralización de la red de frontales.

Una vez planeado el proyecto de la centralización, se vio la necesidad de atender con mayor urgencia las averías de red, ya que con la centralización de la red de frontales, las transacciones realizadas entre el SICAT y las centrales telefónicas serían únicamente a través de la red institucional, y dado el historial de la duración de las averías de red (de 10 minutos a 8 días) y la frecuencia en que ocurren, se detectó una gran necesidad de resolver casi en su totalidad las averías de red.

En la gráfica 4.2 se puede observar la duración de las averías ocurridas desde febrero del 2007 hasta marzo del 2008. En ella se puede apreciar que la mayoría de las averías de red tuvieron una duración menor a una hora, sin embargo gran parte de estas averías fueron mayores de 40 min. Otro fragmento de las averías ronda entre 1 hora y 3 horas. También cabe recalcar que ocurrieron, en una menor cantidad, mas no deja de ser relevante, averías mayores a un día.

La figura 4.3 se observa que la cantidad de averías de red que ocurren mensualmente en la red de frontales. Con un promedio de 85 averías de red por mes.

Finalmente en la figura 4.4 se puede observar la cantidad de averías que ocurrieron simultáneamente.

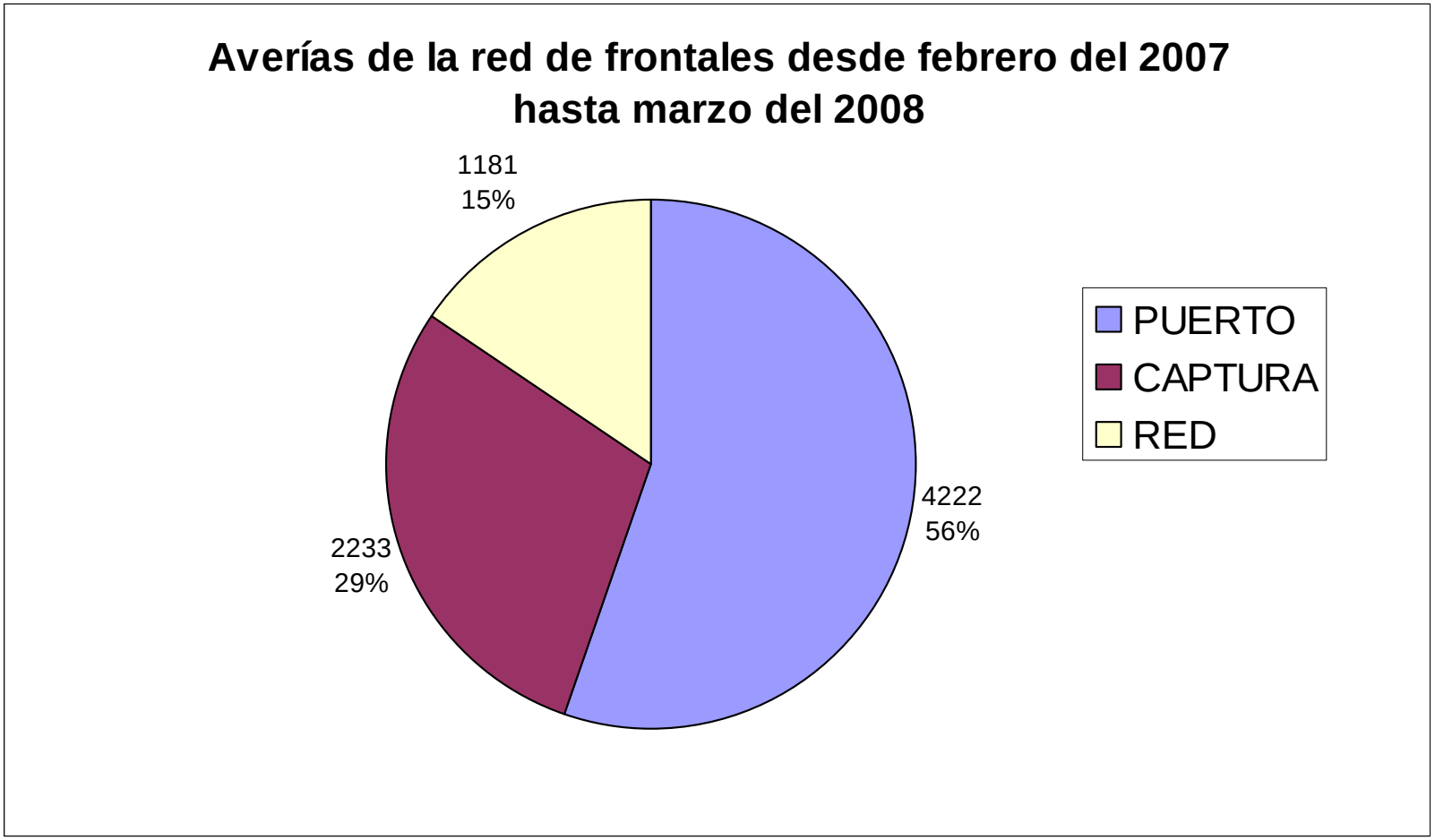


Figura 4.1 Averías ocurridas desde febrero del 2007 hasta marzo del 2008. Fuente del departamento de redes y sistemas.

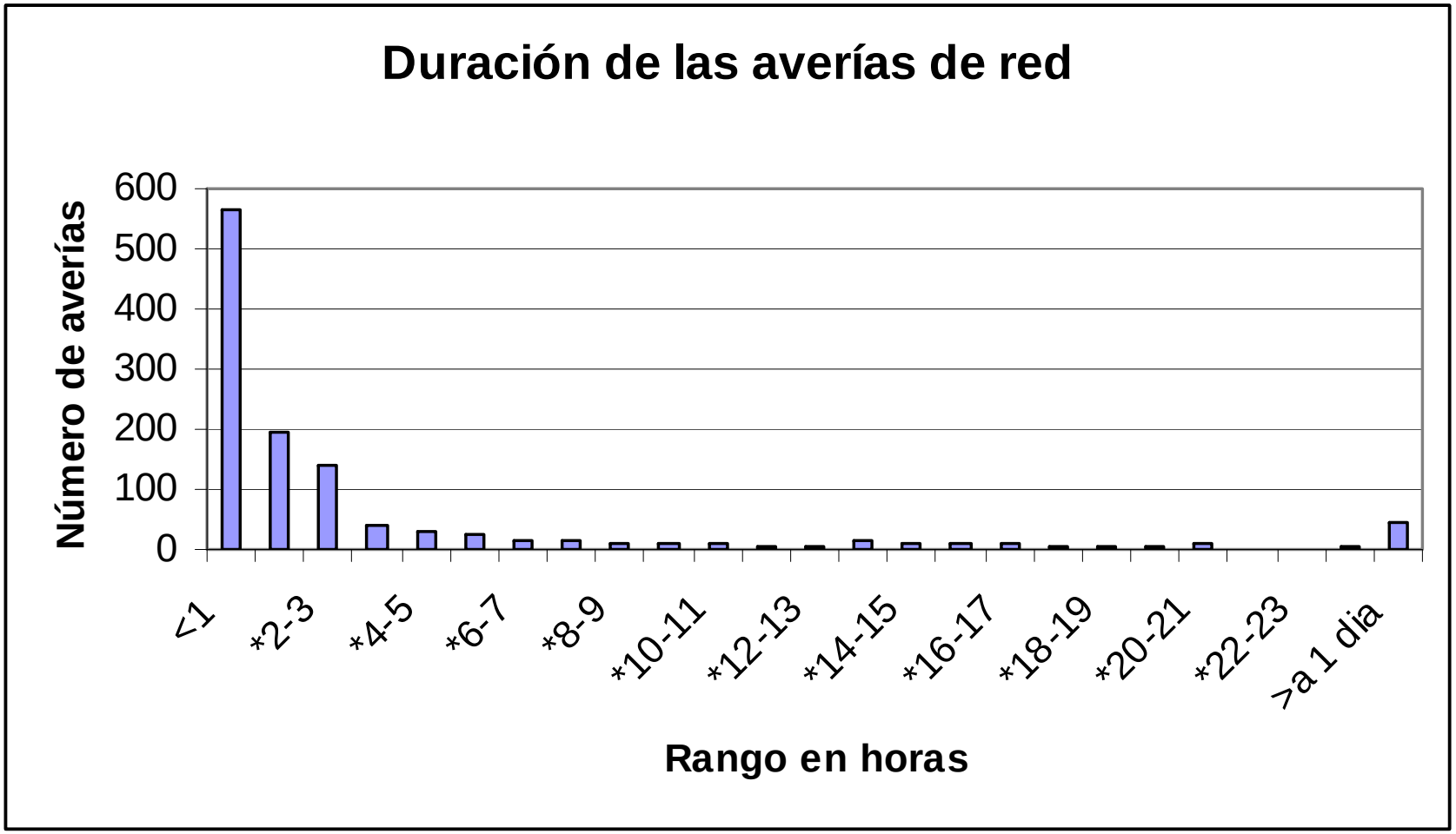


Figura 4.2 Duración de las averías de red ocurridas desde febrero del 2007 hasta marzo del 2008

Fuente del departamento de redes y sistemas

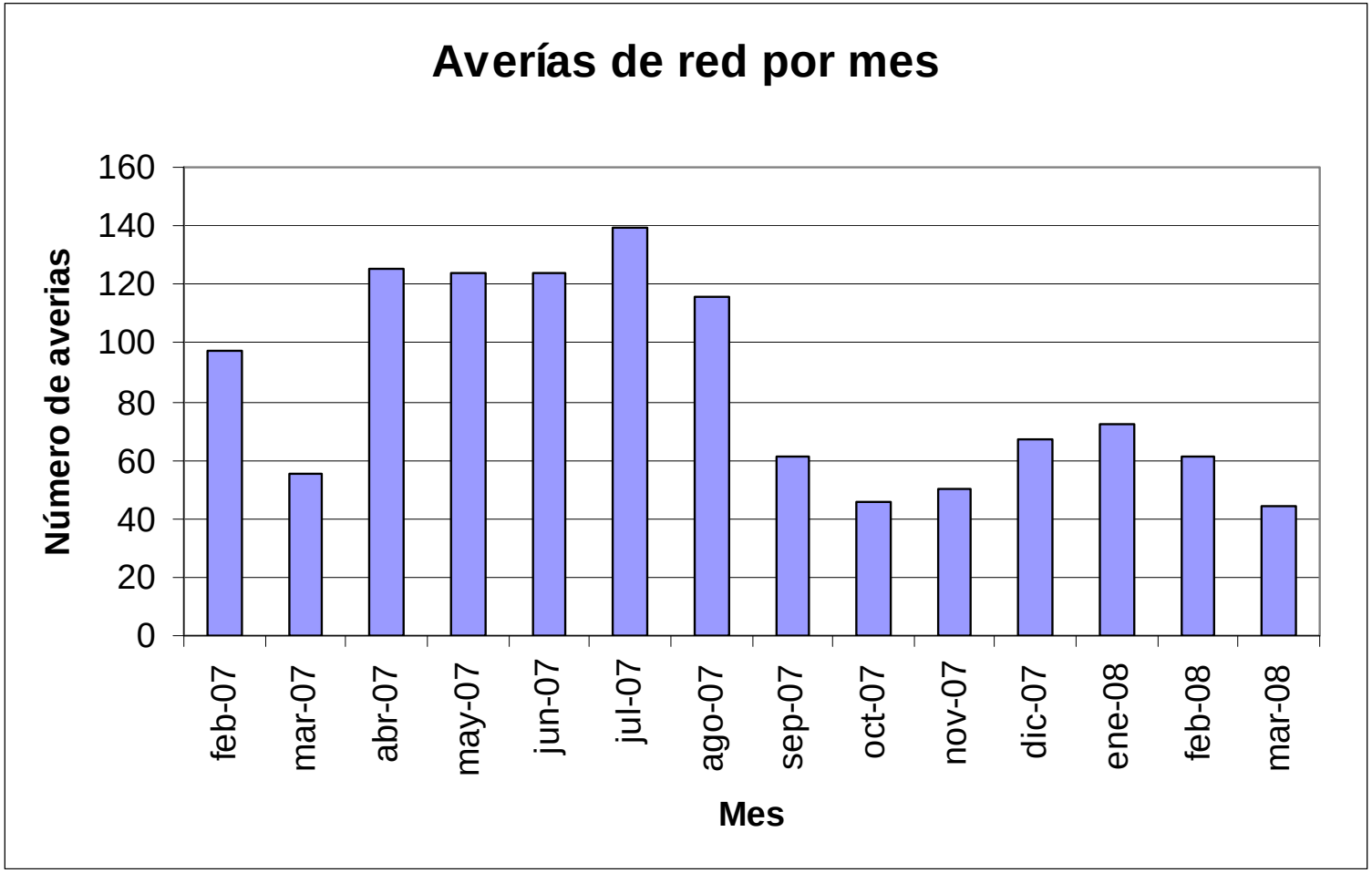


Figura 4.3 Cantidad de averías de red por mes

desde febrero del 2007 hasta marzo del 2008

Fuente del departamento de redes y sistemas

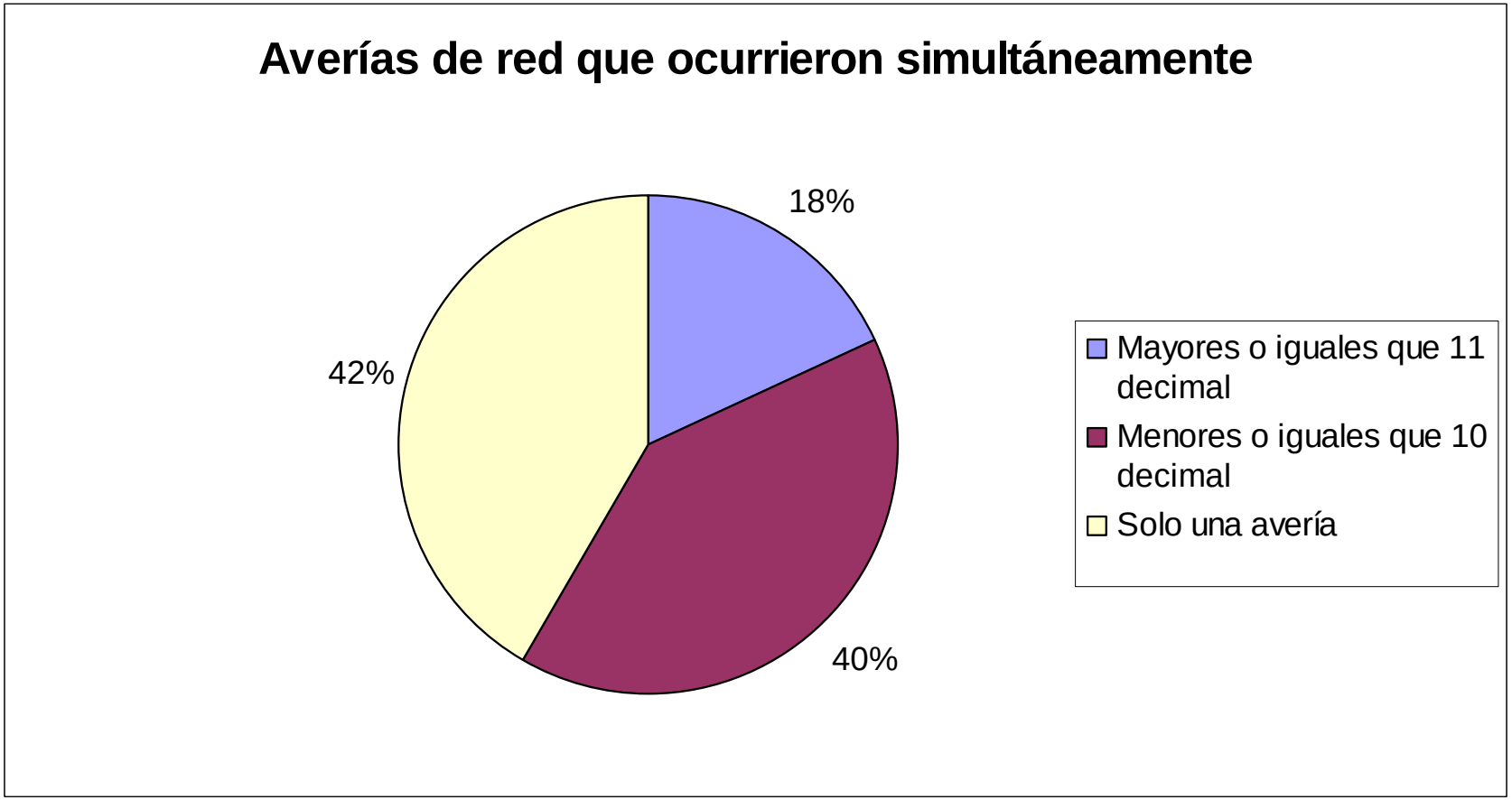


Figura 4.4 Cantidad de averías de red que ocurrieron simultáneamente desde febrero del 2007 hasta marzo del 2008

Fuente del departamento de redes y sistemas

4.2 Obtención y análisis de información

La información relevante al proyecto fue brindada por medio del Ing. Luis González Sandoval, quien empezó con el planteamiento de la centralización de la red de frontales y quién realizó la cotización de los TS desde hace dos años. Actualmente los TS ya se encuentran en el país, sin embargo el proyecto todavía no se ha puesto en marcha.

Después de varias reuniones con el Ing. Luis González, llegamos a un acuerdo en que la solución para casi la totalidad de las averías de red era desarrollar un sistema inteligente de enlaces redundantes hacia cada central telefónica del país.

El sistema a desarrollar debería tener un bajo costo dado a que la inversión inicial que se realizó con los TS fue elevada, por lo que era de preferencia que el sistema de enlaces redundantes fuera lo más económico posible y se ajustara a las necesidades de la empresa.

Con base a esta restricción económica se procedió a investigar cómo estaba implementado el sistema actual de la red de frontales y cuáles eran los recursos que el ICE contaba.

El proyecto se inicio realizando varias visitas a diferentes miembros de la institución para comprender el sistema de la red de frontales actual.

Inicialmente se realizaron entrevistas con los técnicos que estaban a cargo de las averías de la red de frontales, quienes conocen los aspectos técnicos del sistema y los problemas que implican estas averías, esto con el fin de conocer más afondo la problemática existente desde el punto de vista técnico además de conocer el funcionamiento del sistema actual.

Luego se realizaron entrevistas con los ingenieros que crearon las aplicaciones de los frontales para conocer su funcionalidad con las centrales telefónicas y el SICAT. También se realizaron otras reuniones con los ingenieros que trabajan con el sistema corporativo SICAT para entender su funcionamiento y la forma de comunicación con los frontales.

Finalmente se realizaron citas con varios ingenieros encargados de la estructura de la red institucional, para conocer la topología de la red institucional.

4.3 Evaluación de las alternativas y síntesis de una solución

Con base a la información obtenida se llegó a la conclusión de que se debía implementar un sistema de detección de averías de red que a su vez realizara una conmutación del lado de servidor SICAT (San Pedro) y del lado de la central telefónica (lugar remoto) y que la conmutación de ambos lados fuera sincronizada además de que fuera totalmente independiente de la red institucional.

Se plantearon varias soluciones y se realizaron análisis de costos, de diseño y simulaciones para estudiar la validez de cada propuesta. Además de la factibilidad de realizar cada solución en el tiempo establecido.

Finalmente la solución más factible fue la implementación de un sistema redundante mediante módems ISDN. Actualmente el ICE cuenta con varios de estos módems, un par para cada central telefónica, ya que éstos se habían utilizado mucho antes de que existiera la red de frontales, pero después de implementar la red de frontales se dejaron de utilizar.

Para la detección y el establecimiento de los enlaces por lo módems ISDN, se propuso realizar un *script* en Linux, que realiza dichas funciones. La finalidad

de este *script* es que sirva como un enrutador pero especializado para establecer la conexión entre los módems ISDN y la conmutación entre puertas de enlace requeridas. El *script* se propuso realizarlo en Linux con la idea inicial de instalarlo en la PC que servirá como frontal principal y este frontal tendrá un sistema operativo Linux al igual al de todos los frontales de la actualidad.

La conmutación del lado de las centrales telefónicas, se planteó realizarla por medio de los enrutadores Cisco encargados de brindar los servicios de red a cada región donde se encuentra cada central telefónica.

4.4 Implementación de la solución

La implementación del proyecto se llevó a cabo en cuatro etapas:
1) Programación del *script* en Linux para la detección de la avería y análisis de casos.
2) Conexión y configuración del los módems ISDN desde el *script*.
3) Programación de la conmutación del lado de la central telefónica por medio del *script*.
4) Configuración de los enrutadores Cisco para la realización de la conmutación del lado de las centrales telefónicas.

En la primera etapa, se realizó una investigación profunda sobre programación en Linux y se realizaron varios ejemplos para la familiarización con el lenguaje.
Luego se realizó un algoritmo que evaluara una serie de casos para la atención de las averías de red (programa principal).
Cabe mencionar que en esta primera etapa se realizó una modificación al programa. Inicialmente el *script* estaba diseñado para que cada módem ISDN de lado del servidor SiCAT pudiera llamar a una serie de módems específicos del lado de las centrales telefónicas. Por ejemplo, si hubiese tres módems para la atención de las averías cada uno de ellos tendría una lista de posibles módems remotos a los que podría llamar, así cada uno de los tres módem solo podría llamar a 22 módems diferentes de cada central telefónca para un total de 66 centrales telefónicas conectadas por módems ISDN.

Esta primera implementación se realizó de esta forma porque cada módem tanto el local, del lado del servidor SICAT, como el remoto debían tener configurados los números telefónicos del módem al que llama o del que recibe la llamada. Así, el módem remoto debía tener configurado el número telefónico del módem local y el módem local debía tener configurado el número del módem remoto, además de otras variables como la red en la que se encuentra cada uno, ya que en realidad los módems ISDN son tanto módems como enrutadores a la vez.

El problema surgió debido a que se pensaba que los módems solamente soportaban llamadas de un único número telefónico, de esta forma se podía configurar al módem local para que ejecutase llamadas a diferentes módems remotos mediante el *script*, pero no se podía cambiar la configuración de los módem remotos para que pudiesen recibir llamadas de otros módems y de ahí la idea de agrupar las llamadas de los módems locales a ciertos módems remotos.

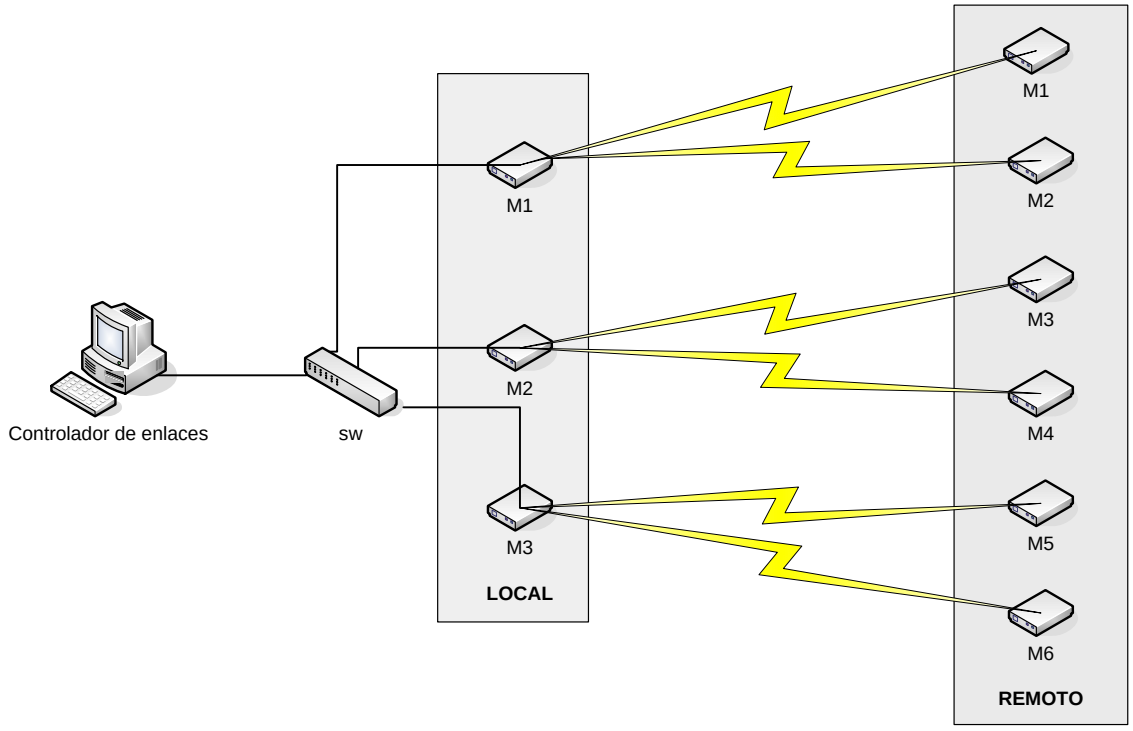
Evidentemente este sistema no era lo suficientemente eficiente, debido a que se podía dar el caso de que existiera una avería o varias en el grupo de un módem local que ya estaba siendo utilizado para atender otra avería dentro del mismo grupo, y aunque existieran módems libres para atender estas averías estas no podrían atenderse.

La figura 4.5 es un diagrama ilustrativo que refleja la idea de las conexiones entre módems inicialmente, en la que a cada módem se le asigna una cantidad de módems a los que puede llamar, para este caso dos módems remotos por cada módem local.

Se investigó más a fondo las características de los módems ISDN y se descubrió una forma para que el módem pudiera recibir llamadas telefónicas de más de un módem. Los módem ISDN marca DIVA LAN que se están utilizando pueden recibir llamadas de hasta 10 números telefónicos distintos.

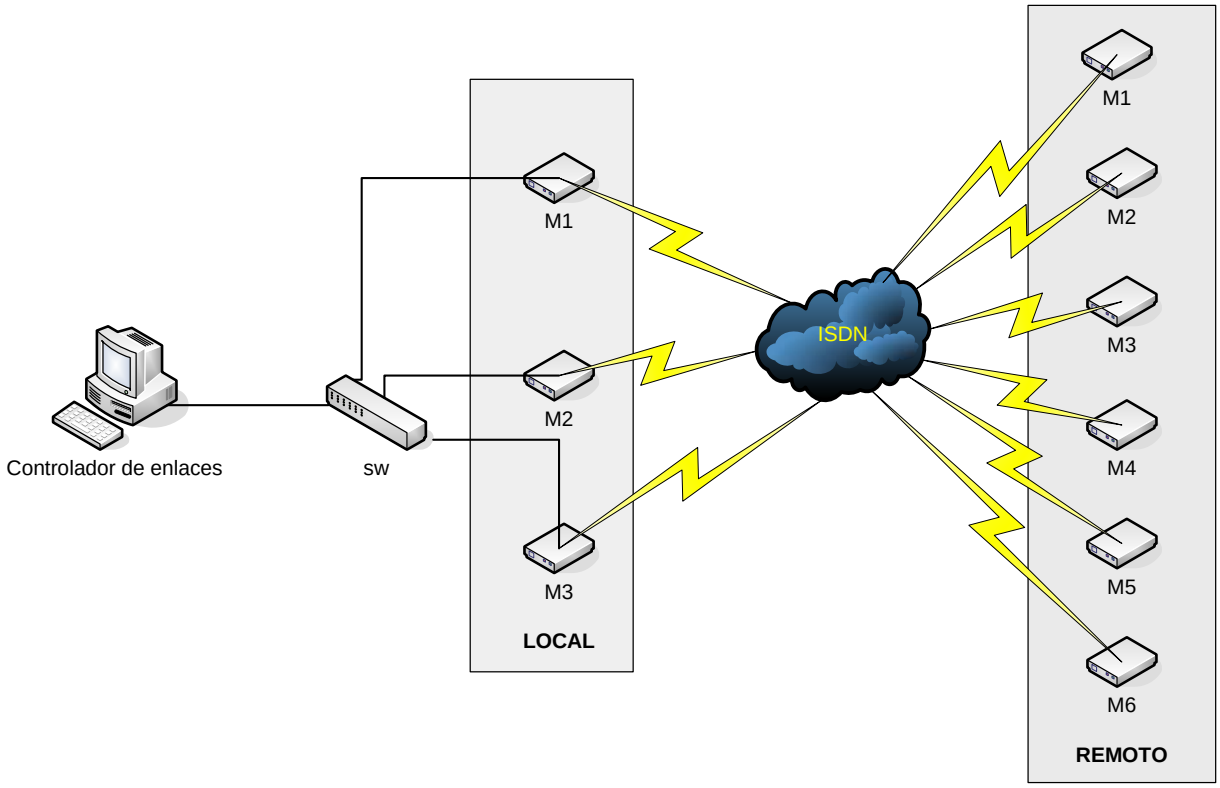
Por lo tanto, si se tienen 10 módems locales, entonces todos ellos van a poder llamar a cualquier módem remoto. Ver figura 4.2.

Entonces partiendo del punto de que el sistema contará con 10 módems locales para atender las averías, se realizaron los cambios necesarios al *srcirpt* inicial para que cualquier módem local pueda llamar a cualquier módem remoto.



VISIO

Figura 4.5 Ejemplo del sistema de conexión entre módems propuesto inicialmente



VISIO

Figura 4.6 Ejemplo del sistema de conexión entre módems propuesto finamente

Otra mejora que se realizó al *script* principal fue la forma en que se evaluaban las conexiones de red con cada central telefónica.
Inicialmente se enviaba una petición de eco ICMP (ping) a cada central telefónica secuencialmente, y se ejecutaban acciones de acuerdo al estado de la conexión de cada central telefónica. El inconveniente de realizar la evaluación de esta forma es que el tiempo de ejecución del *script* no sería el adecuado como para realizar una detección de la avería en menos de 5 minutos. Por recomendación del profesor asesor, se agregó una subrutina al programa que realiza todos los pings hacia 54 centrales telefónicas al mismo tiempo, es decir en paralelo, con esto se redujeron los tiempos en la detección de averías. Cabe recalcar que se realizará la evaluación a 54 centrales telefónicas conectadas por la red institucional, las restantes 13 centrales telefónicas se encuentran conectadas por módems ISDN DIVA LAN ya que se encuentran en lugares donde no llega el servicio de red del ICE.

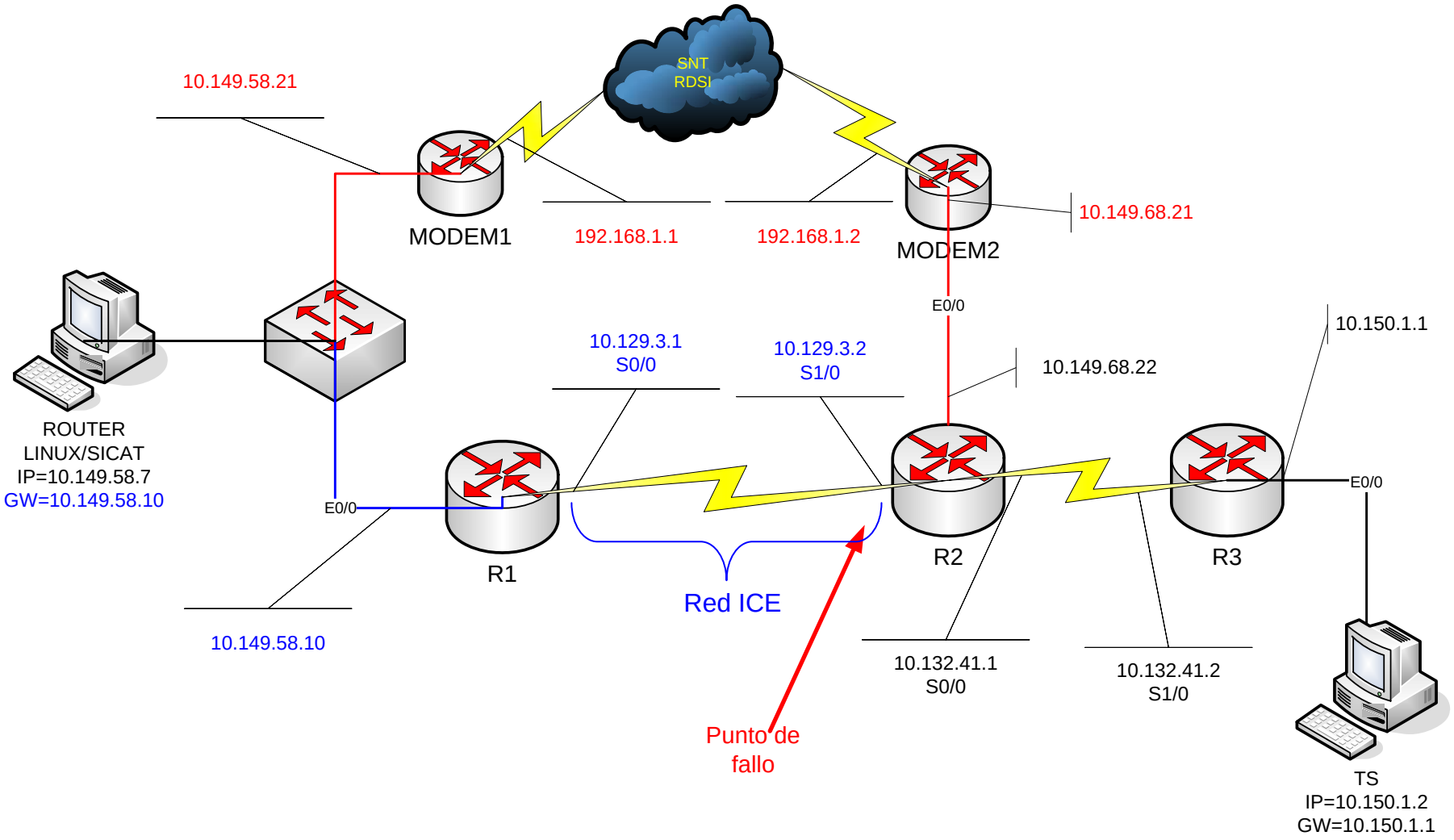
Para la ejecución de la segunda etapa se realizaron varias pruebas con los módems ISDN, primero se elaboró una configuración manual mediante instrucciones y luego se investigó la manera de poder realizar la configuración de los módems desde el *script*. Después de varias pruebas, la configuración desde el *script* fue exitosa.

En la tercera etapa se realizó una investigación en Internet para encontrar la forma adecuada para lograr que los paquetes procedentes del SICAT fueran enrutados a la puerta de enlace correspondiente al módem ISDN, esto se logró mediante la instrucción *route.*
Se verificó el correcto funcionamiento de la programación realizada para la conmutación mediante un programa llamado Ethereal, el cual es un programa que captura y analiza el tráfico de paquetes y se utiliza para el análisis de protocolos en redes de comunicaciones.

Finalmente la última etapa fue la implementación de la topología a montar para la puesta en marcha del prototipo. La topología montada se puede observar en

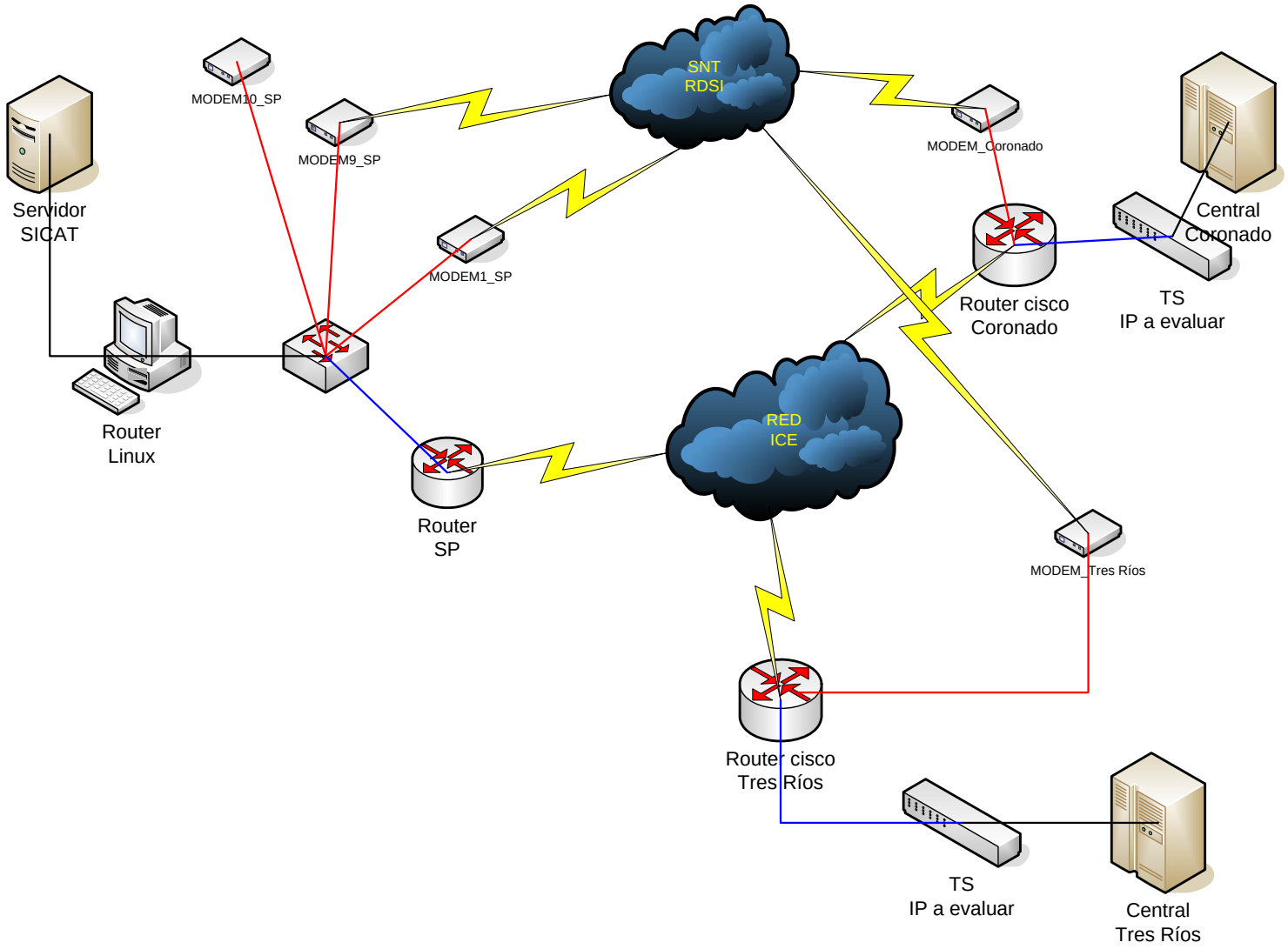
la figura 4.7 y a figura 4.8 muestra la topología del sistema redundante implementado.
Los componentes utilizados fueron: dos PC, un *switch*, dos módems ISDN DIVA LAN, tres enrutadores Cisco y dos líneas telefónicas ISDN.

Existe una PC con Linux la cual contendrá el *script* controlador de enlaces. El *script* determinará cuándo conectar los módems ISDN, realizará la configuración adecuada de los módems y realizará la conmutación de los paquetes que van dirigidos hacia la central telefónica que tuvo un fallo en la conexión de red. En el diagrama de la figura 4.7 se observa ambas rutas, la conexión por red institucional, que será la conexión por medio de los enrutadores y la conexión por las líneas ISDN delineada con color rojo.
La conexión entre el enrutador 1 (R1) y el enrutador 2 (R2), representa toda la red institucional.
Los enrutadores R2 y R3 en conjunto representan el enrutador Cisco de cada región donde se encuentra una central telefónica por el cual se obtiene la conexión de red. En este caso se utilizaron dos enrutadores ya que se requería un enrutador con dos tarjetas ethernet para la conmutación entre la conexión de red y la conexión por ISDN.
Actualmente todos los enrutadores Cisco de cada región cuentan con más de una tarjeta de red.
El *script* estará enviando un ping a la tarjeta de red del enrutador R2, que será el último punto de acceso de la conexión de red hacia el TS. Este es considerado el punto de fallo, si no se puede realizar un ping a esta tarjeta de red, entonces existe un problema en la red institucional y el *script* deberá configurar el módem local para que se establezca la conexión ISDN y luego realizar el enrutamiento de los paquetes dirigidos hacia esa central telefónica por el *gateway* del módem ISDN local (10.149.58.21).
Por otro lado, el enrutador R2 tendrá configurado por el protocolo RIP dos rutas para acceder a la misma red, donde se encuentra la PC Linux, con diferentes distancias administrativas, así, cuando se cae la conexión por la tarjeta que representa la conexión de la red del ICE (10.129.3.2), el enrutador automáticamente cambia la conexión del Terminal Server a la PC con Linux por la tarjeta de red conectada a los módems ISDN (10.149.68.22).



VISIO

Figura 4.7 Topología de prototipo



VISIO

Figura 4.8 Topología final propuesta, con enlaces redundantes

Capítulo 5: Descripción detallada de la solución (Explicación del diseño)

5.1 Análisis de soluciones y selección final

Antes de implementar la solución propuesta, se plantearon otras posibles soluciones y se analizó la factibilidad de cada una.

Para solucionar el problema existente, se debía atender básicamente dos puntos, el primero, cómo detectar una avería de red y establecer un nuevo enlace, y la segunda, una vez detectada la avería, cómo realizar el enrutamiento de los paquetes del lado de las centrales telefónicas.

Para atender el primer punto, se planteó la solución actual, realizar un *script* que se ejecutara cada cierto tiempo y que realizara la función de detectar una avería y establecer el enlace redundante correspondiente para atender la avería. A este *script* se le llamó controlador de tráfico, éste hace la función de un enrutador pero especializado, es decir, cambia la ruta del enlace entre el TS y el frontal principal, solo en caso de que la conectividad por la red institucional falle. La nueva ruta será establecida por el mismo programa al configurar y realizar la conexión entre los módems ISDN.

El sistema realiza las siguientes etapas:

1) Realiza un método para la comprobación de la conectividad de todas las centrales telefónicas con la red institucional.

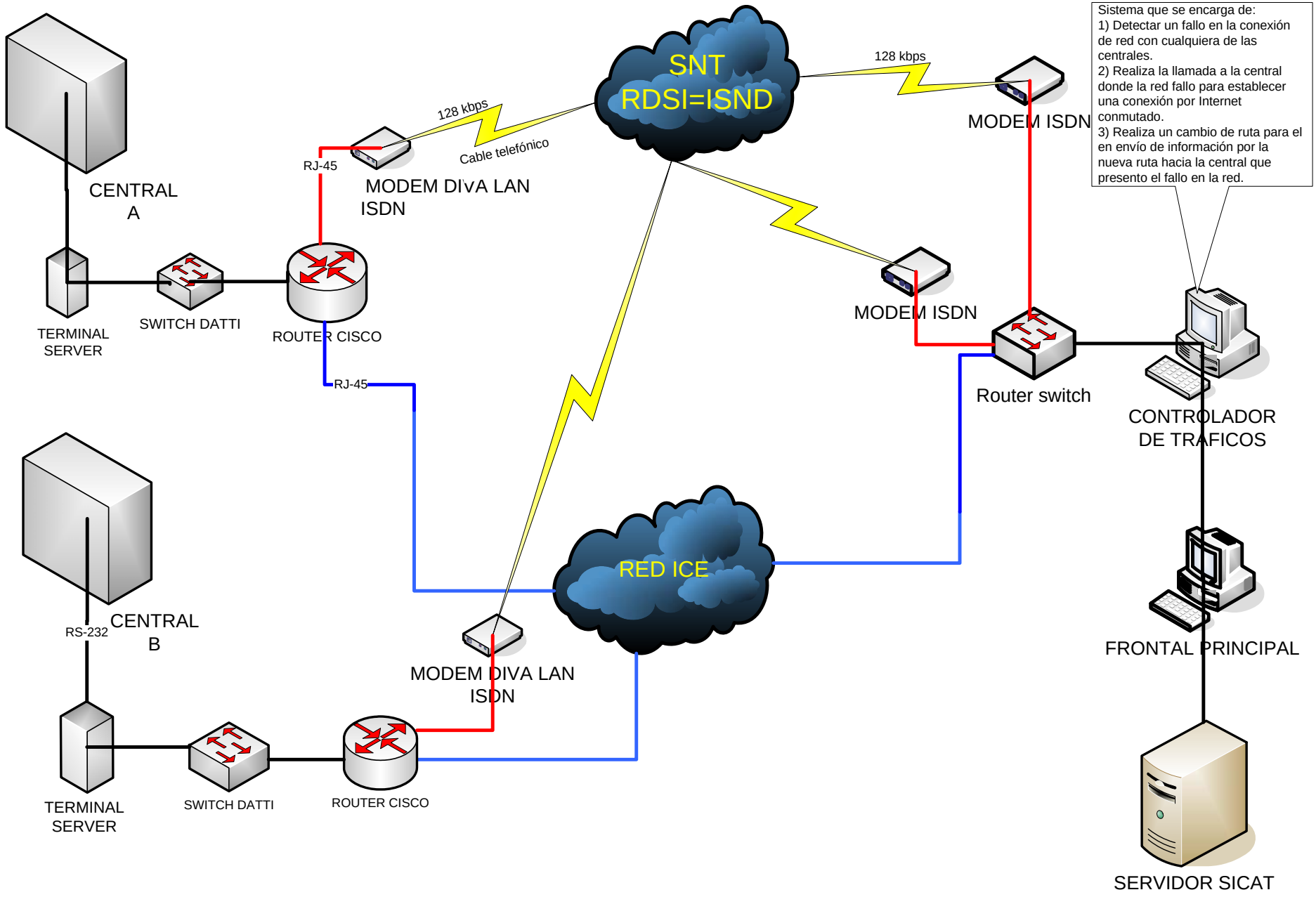
2) En el momento que detecta una falla en la conexión por la red del ICE en alguna central telefónica, realiza una llamada al número de teléfono del módem ISDN correspondiente a la central telefónica donde la red del ICE falló para así poder establecer un enlace temporal.

3) El método de revisión de la conexión siempre se está ejecutando. Cuando la conexión por la red del ICE se reestablece, el programa termina la conexión temporal y vuelve a enviar los paquetes por la antigua ruta.

La ventaja de la solución para el primer punto, es que es totalmente automatizada y de bajo costo ya que la empresa cuenta con los módems ISDN. En la figura 5.1 se puede observar la topología de la solución seleccionada.

La solución para el segundo punto, la conmutación entre enlaces del lado de la central telefónica, se decidió realizarla directamente desde los enrutadores destino, encargados de brindar el servicio de red a cada central telefónica, esto se logró definiendo distancias administrativas distintas para cada enlace.

Se estudió la posibilidad de que la conmutación la realizara los TS, para así evitar un punto de fallo, sin embargo, se descubrió que los TS no pueden hacer la conmutación como se requería.



VISIO

Figura 5.1 Topología para la solución seleccionada

5.2 Descripción de software

Descripción del programa para el controlador de enlaces.

La figura 5.5 muestra el diagrama de flujo general del programa que se realizó para el control del flujo de la información entre el SICAT y las centrales telefónicas, en caso de que una conexión de red falle. Este programa se compone de cinco métodos que son llamados por un programa principal.

El primer método, llamado *Paralelo.sh*, realiza un *ping* a todas las direcciones IP de los enrutadores que brindan la conexión de red a las regiones de cada central telefónica, desde una lista de diracciones IP que el método tendrá. Todos los *pings* se realizan en paralelo.

El segundo método, llamado *Conecta.sh*, realiza la función de configurar y conectar el módem que se encuentre libre en San Pedro (ubicación local) para ser conectado al módem ubicado en la central telefónica donde ocurrió el fallo de la red (ubicación remota).

El tercer método, llamado *Desconecta.sh*, se encarga de finalizar la conexión de los módems cuando la avería de red se restablece.

El cuarto método, llamado *Conmuta.sh*, realiza el cambio de *gateway* solo para los paquetes que van dirigidos hacia la central telefónica que presentó un fallo en la conexión por la red institucional.

Finalmente, el quinto método, llamado *ConmutaRestaura.sh*, realiza la restauración de la ruta anterior, es decir vuelve a enrutar los paquetes por la puerta de enlace predeterminada.

En la figura 5.5 se puede observar el diagrama del *script* principal y los métodos que llama y las variables que utiliza cada método.

Las variables utilizadas son las siguientes:

- **Usados.txt** : Archivo que guarda las direcciones IP de las regiones que están siendo conectadas por los módems ISDN.

Ej:
linux-ethereal:~ # cat Usados.txt
10.132.56.99 MODEM1
10.133.36.22 MODEM4

- **ModemsUsados.txt:** Archivo que guarda la lista de los módems ISDN que están siendo usados.

Ej:
linux-ethereal:~ # cat ModemsUsados.txt
MODEM1
MODEM4

- **ListaPendientes.txt:** Archivo que almacena las direcciones IP de las regiones que no pudieron ser atendidas porque todos los módems disponibles están siendo utilizados

- **ListaModems.txt:** Lista total de módems ISDN.

Ej:
linux-ethereal:~ # cat ListaModems.txt
MODEM1
MODEM2
MODEM3
MODEM4

- **Tabla_IPS_Y_Telefonos**: Archivo que contiene una tabla con las direcciones IP de cada región, el número telefónico del módem ISDN ubicado en esa región y la red en la que se encuentra ubicado el TS.

Ej:
linux-ethereal:~ # vi Tabla_IPS_Y_Telefonos.txt

REGION	IP_PuntoFallo	TEL_ISDN	RED
PingMalo	10.129.3.2	22344999	10.150.1.0
Alajuela	10.134.7.69	84439040	
Alto_Guadalupe	10.129.132.22	82455030	
Barrio_San_Jose	10.134.56.22	84333144	

- **IPdeModem.txt:** Archivo que guarda las direcciones IP de los módems a conectar, ubicados en San Pedro, esto para poder ingresar a ellos para configurarlos.

Ej:
linux-ethereal:~ # cat IPdeModem.txt
MODEM1 10.149.58.21

MODEM2 10.149.58.21
MODEM3 10.149.58.21
MODEM4 10.149.58.21

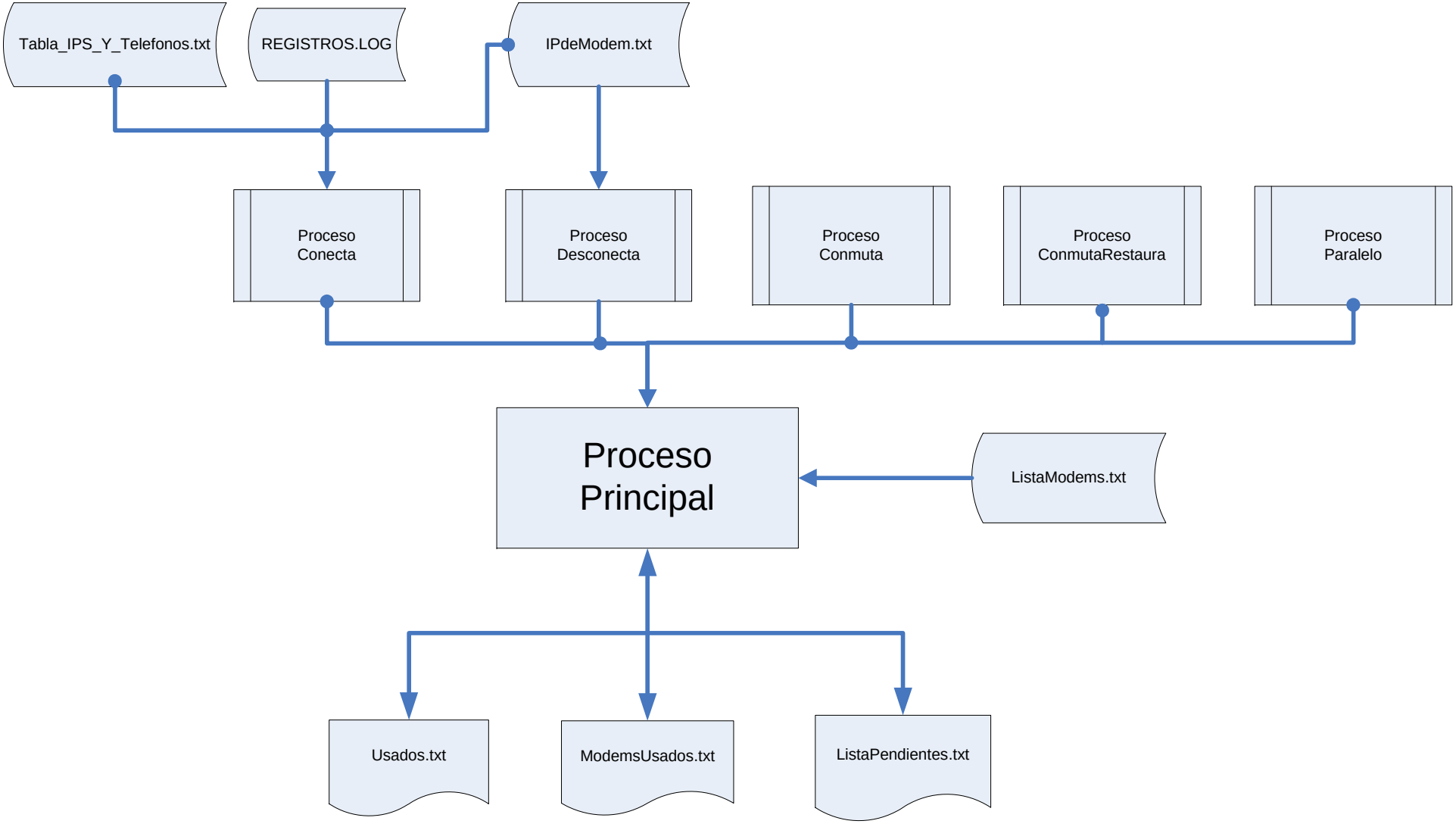
- **REGISTRO.log:** Archivo que guarda la historia de configuración y conexión de los módems ISDN.

Ej:

```
linux-ethereal:~ # cat REGISTRO.log
spawn telnet 10.149.58.21
Trying 10.149.58.21...
Connected to 10.149.58.21.
Escape character is '^]'.

DIVA LAN ISDN Modem version 1.3.2. Welcome!
Copyright (c) 1994-1999 Eicon Technology Corporation
Password:
Press F1 for Help, Ctrl-L to redraw the screen.

LOCAL> PROFILE   LOCAL
LOCAL> SET ISDN REMOTE 1 22344999
LOCAL> SET ISDN REMOTE 2 22344999
LOCAL> SET ISDN BACKUP 1 22344999
LOCAL> SET ISDN BACKUP 2 22344999
LOCAL> save
LOCAL> DELETE IP ROUTE 10.150.1.0
LOCAL> ADD IP ROUTE 10.150.1.0 24,1 192.168.1.2
LOCAL> save
LOCAL> dial
Checking initial state ...Ok
Checking ISDN ...Bringing up the line ...
Connecting with ISDN ...Connected
PPP negotiation ...Success
Authentication ...Success
IP address negotiation...Success
Pinging the remote...Pings received from the remote
This profile works properly.
```



VISIO

Figura 5.5 Diagrama de *script*

En la figura 5.6 se observa el diagrama de flujo del programa principal.

Inicialmente, el programa principal llama al método Paralelo, el cual realiza una interrogación a todas las centrales telefónicas, en paralelo o al mismo tiempo, y guarda el estado de la respuesta en un archivo el cual luego será evaluado por el programa principal para cada conexión con cada central telefónica. Si hubo un 100% de paquetes perdidos, se cataloga como conexión rota, si no se perdió el 100% de los paquetes se cataloga como conexión buena.

Con base a esta clasificación se realizan una serie de decisiones.

Si el estado de la conexión se considera buena, se pregunta si está en la lista de Usados.txt, donde se encuentran todas las direcciones IP de los enrutadores de cada región que están siendo conectados por módems ISDN.

Si se encuentra en la lista de Usados.txt, entonces se procede a desconectar el módem y a restablecer la ruta de los paquetes hacia esa central telefónica por el gateway por defecto.

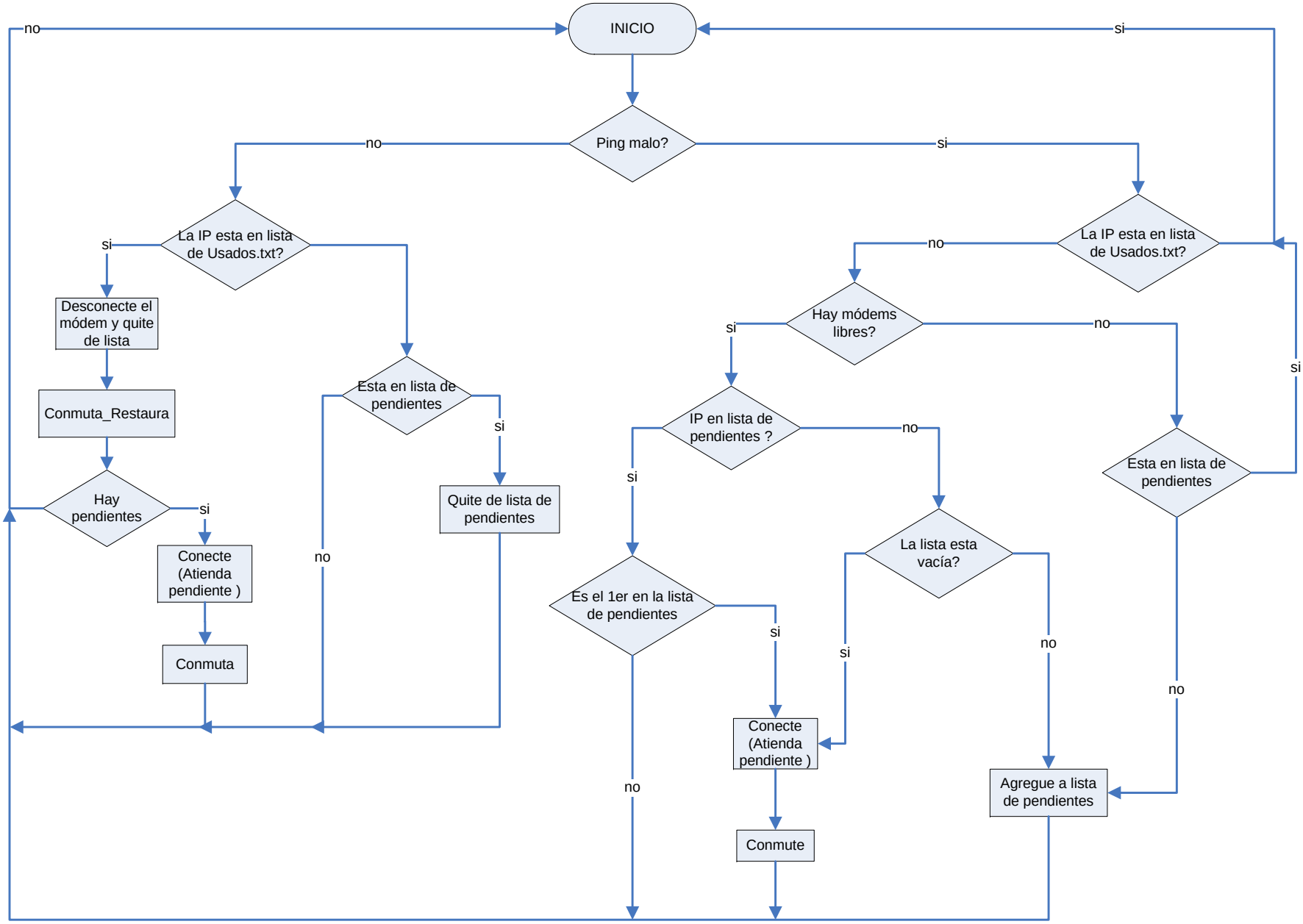
Luego, dado que se desocupó un módem, se pregunta si existe alguna central telefónica que tenga un fallo en la red y que se encuentre en la lista de pendientes, si es así, se utiliza el módem desocupado para conectarlo hacia la nueva central telefónica de la lista de pendientes. Si no vuelve a empezar el programa.

Si el estado de la conexión se considera malo, se vuelve a preguntar si está en la lista de Usados.txt, esto debido a que es posible que el programa detecte una conexión rota que ya fue atendida con anterioridad y continúa rota. Entonces, si se encuentra en la lista de Usados.txt y la conexión esta rota, entonces, vuelve a empezar el programa. Si no, se procede a preguntar si existen módems disponibles para atender el fallo de red. Si todos los módems están siendo ocupados, se guardará la dirección IP a atender en la lista de Pendientes.txt.

En caso de que exista un módem disponible, entonces se pregunta si la dirección IP esta en la lista de Pendientes.txt y de ser así, se pregunta si es el primero en la

lista, esto con la finalidad de establecer una prioridad en la lista de pendientes y atender a los que hayan entrado primero a la lista (FIFO).

Si la dirección IP no se encuentra en la lista de Pendientes.txt, entonces se pregunta si la lista de Pendientes.txt está vacía, de ser así, se procede a establecer la conexión por módems, éste sería el único caso en que se atienda la dirección IP de una avería sin que se encuentre en la lista de Pendientes.txt.



VISIO

Figura 5.6 Diagrama de flujo del *script* principal

Capítulo 6: Análisis de Resultados

6.1 Resultados

Una vez montada la topología del prototipo se procedió a medir los tiempos de respuesta del sistema.

Para determinar cuánto tiempo tardaría el *script* en ejecutar las tareas de identificación del estado de la conexión de red, conexión, desconexión y enrutamiento se incluyó dentro del *script* la instrucción *date* para obtener el tiempo de inicio y fin de cada tarea del programa. Esta instrucción indica la hora en los puntos del *script* donde uno lo coloque.

En las siguientes tablas se muestran los tiempos obtenidos para los procesos de conexión y conmutación, desconexión y conmutación y para el caso en que todos los módems están ocupados y se deba agregar la dirección IP del la red con avería en la lista de Pendientes.txt.

Estas mediciones posteriormente son utilizadas para calcular cada cuánto tiempo se debe de ejecutar el *script* así como para realizar el cálculo de la confiabilidad del sistema.

Tabla 6.1 Tiempos de ejecución del *script* para la medición de la duración en conectar los módems y realizar el enrutamiento (conmutación) de los paquetes a la nueva ruta.

#Medición	T de ejecución del *script*		Duración	T de ejecución de Paralelo.sh		Duración	Duración Conecta/Conmuta
	Ti	Tf		Ti	Tf		
1	8:52:38	8:53:13	0:00:35	8:52:38	8:52:49	0:00:11	0:00:24
2	9:22:36	9:23:11	0:00:35	9:22:36	9:22:47	0:00:11	0:00:24
3	9:50:15	9:50:50	0:00:35	9:50:15	9:50:26	0:00:11	0:00:24
4	10:13:55	10:14:30	0:00:35	10:13:55	10:14:06	0:00:11	0:00:24

Tabla 6.2 Tiempos de ejecución del *script* para la medición de la duración en desconectar los módems y realizar el enrutamiento (conmutación) de los paquetes a la ruta por defecto.

#Medición	T de ejecución del *script*		Duración	T de ejecución de Paralelo.sh		Duración	Duración Desconecta/Conmuta
	Ti	Tf		Ti	Tf		
1	9:17:08	9:17:20	0:00:12	9:17:08	9:17:19	0:00:11	0:00:01
2	9:36:15	9:36:27	0:00:12	9:36:15	9:36:26	0:00:11	0:00:01
3	10:36:45	10:36:57	0:00:12	10:36:45	10:36:56	0:00:11	0:00:01
4	11:12:09	11:12:21	0:00:12	11:12:09	11:12:20	0:00:11	0:00:01

Tabla 6.3 Tiempos de ejecución del *script* para la medición de la duración en agregar una dirección IP en la lista de Pendientes.txt.

#Medición	T de ejecución del *script*		Duración	T de ejecución de Paralelo.sh		Duración	Duración Agrega a Pendientes.txt
	Ti	Tf		Ti	Tf		
1	8:46:12	8:46:24	0:00:12	8:46:12	8:46:23	0:00:11	0:00:01
2	9:27:49	9:28:01	0:00:12	9:27:49	9:28:00	0:00:11	0:00:01
3	1:22:27	1:22:39	0:00:12	1:22:27	1:22:38	0:00:11	0:00:01
4	1:36:46	1:36:58	0:00:12	1:36:46	1:36:57	0:00:11	0:00:01

6.2 Cálculo del tiempo de ejecución del *script*

La estructura del programa principal es la siguiente:

1) Carga todos los subprogramas en memoria.
2) Ejecuta el subprograma Paralelo.sh.
3) Crea una archivo llamado log2.txt que contiene el resultado de la ejecución del *script* Paralelo.sh (Resultado de los *pings*)
4) Inicia programa para la evaluación de cada conexión de red.

Como se mencionó con anterioridad, se utilizó la instrucción *date* para la medición de la duración del el *script* en realizar: una conexión completa., una desconexión completa y el tiempo que dura en realizar todos los *pings* hacia todas las centrales telefónicas (Proceso Paralelo.sh).

De esta forma se colocó el comando date al inicio y fin de todo el *script* para ver la durabilidad del *script* completo y también se colocó al inicio y final de la ejecución del *script* Paralelo.sh, para poder conocer el tiempo de ejecución de todos los pings en paralelo.

En la figura 6.1 se presenta una imagen del resultado de la ejecución del *script* cuando se desconectó el enlace entre los enrutadores R1 y R2, que es una representación de un fallo en la conexión por red institucional.
En esta imagen se puede observar con un enmarcado rojo el tiempo de inicio y de fin del *script* en total y con enmarcado amarillo el tiempo de inicio y de fin del método Paralelo.sh, el cual se encarga de enviar una interrogación a todas las 54 centrales telefónicas al mismo tiempo.

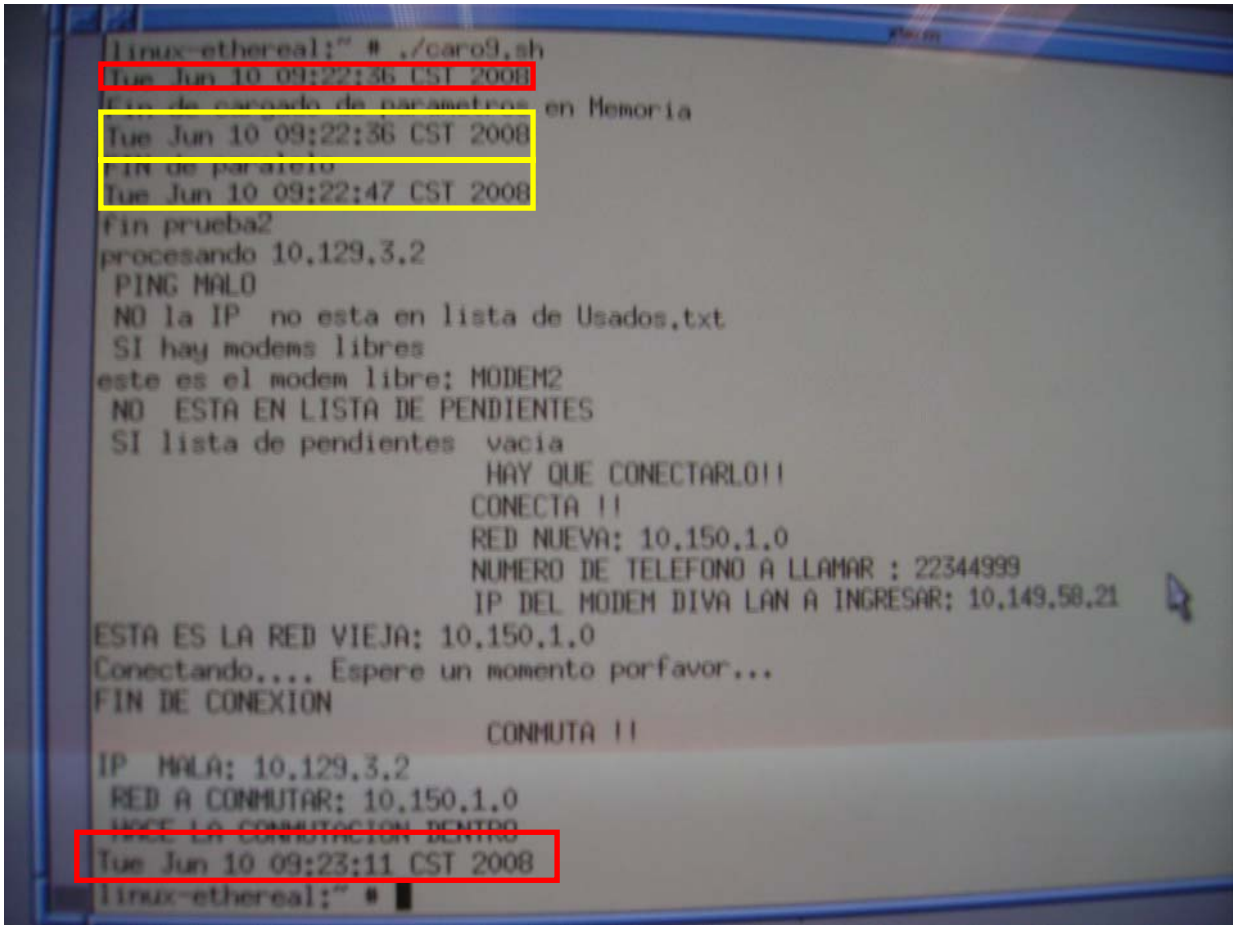


Figura 6.1 Imagen de los resultados del *script* después de realizar la conexión de los módems y el enrutamiento de los paquetes.

En la figura 6.2 se muestran los módems ISDN conectados por el *script* automáticamente.

Figura 6.2 Módems ISDN conectados

Las mediciones indicaron los siguientes tiempos:
Tiempo en ejecutar el *script* Paralelo.sh : 11 seg.
Tiempo en ejecutar en ejecutar una conexión completa: 25 seg.
Tiempo en ejecutar una desconexión completa: 1 seg.
Tiempo en ejecutar cualquier otra función: 1 seg. (Tomando como base el tiempo en agregar una dirección IP en la lista de Pendientes.txt)

Con base a estos tiempo se realzó el cálculo para saber cuanto tiempo se tardaría en evaluar las 54 centrales telefónicas para el peor de los casos.

El peor de los casos es, que de las 54 centrales telefónicas a evaluar, se tenga que realizar el máximo de conexiones posibles (10 conexiones), se tengan que realizar 10 desconexiones y realizar otras funciones.
Así, el *script* inicialmente tardará siempre 11 segundos realizando los *pings* hacia las centrales telefónicas, 240 segundos que resulta de la multiplicación de las 10 averías por 24 seg y 44 segundos ya sea de desconexiones u otras funciones.

Esto en total sería: 11 seg + (10 * 24 seg) + 44 seg = 295 seg = 4 min 55 seg
Por este motivo el *script* se ejecuta cada 5 minutos.

6.2 Cálculo de la confiabilidad del sistema

Realizando el cálculo de la confiabilidad para un sistema paralelo en el que el sistema de comunicación por la red del ICE es el sistema 1 y el sistema de comunicación por los módems ISDN el sistema 2.
Entonces de acuerdo a la ecuación (4) la confiabilidad para un sistema paralelo es:

$$\boxed{f(t) = e^{-\lambda_1 * t} + e^{-\lambda 2 * t} - e^{-(\lambda_1 + \lambda_2) * t}}$$

El tiempo promedio de la averías de red para el sistema 1 son 4 horas con 10 minutos, es decir 4.18 h y el tiempo promedio de falla para el sistema 2 son 5 minutos o bien 0.083 h.

Así la razón de falla para cada sistema es:

$$\lambda_1 = \frac{4.18}{9984} = 0.418 \times 10^{-3}$$

$$\lambda_2 = \frac{0.083}{9984} = 8.35 \times 10^{-6}$$

Por lo tanto, la confiabilidad del sistema en un tiempo igual al que se tomaron las muestras de averías (9987 horas) es:

$$f(9984) = e^{-0.418E-3*9984} + e^{-8.35E-6*9984} - e^{-(0.418E-3+8.35E-3)*9984}$$

$$f(9984) = 92{,}12\%$$

Mientras que la confiabilidad sin el sistema de respaldo es:

$$f(9984) = e^{-0.418E-3*9984}$$

$$f(9984) = 1{,}53\%$$

6.2 Análisis

Como se ha mencionado con anterioridad, el sistema está diseñado para atender 10 averías de red simultáneamente, esto debido a una limitación del los módems ISDN que se usarán, ya que estos soportan recibir llamadas hasta de 10 números telefónicos distintos.

Si bien la atención de máximo 10 averías simultáneamente es una limitación del sistema, esta cantidad de conexiones se ajusta satisfactoriamente al total de averías que han ocurrido al mismo tiempo en el sistema actual de la red de frontales.

En la gráfica de la figura 4.1 presentada en el capítulo 4 en el tema 4.1 se puede observar que el 40% de las averías que ocurrieron conjuntamente son menores o iguales que 10 y 42% ocurren solas, es decir, el sistema puede atender hasta el 82% de los casos que ocurren en las averías de red. Cabe mencionar que en el periodo en que se tomaron las mediciones de las averías de red hubieron varios días en que ocurrió un problema con la red institucional y fallaron por pequeños periodos todas las conexiones de red hacia las centrales telefónicas del país, esto es un caso aislado que muy rara vez ocurre, sin embargo se está tomando en cuenta en el análisis.

El proyecto definió como meta reducir casi en su totalidad las averías de red y se propuso lograr solventar por lo menos el 80% de las averías de red. Por lo tanto, si este sistema hubiera sido implementado hace un año se hubiera podido solucionar el 82% de las averías de red, con un tiempo máximo de conexión de 5 minutos, con lo cual se hubiera alcanzado la meta.

Ahora bien, como se mencionó anteriormente, el año pasado hubo un problema que generó la desconexión de la red hacia todos los frontales de manera intermitentemente por varios días, lo cual es algo muy poco probable que vuelva a suceder y por lo que la cifra de las averías simultáneas mayores de 10

aumentó, si se parte que este hecho no volverá a suceder, entonces el porcentaje de las averías simultáneas menores de 10 aumentaría y con esto el porcentaje de atención de averías en menos de 5min también aumentaría.

Para comprobar el cumplimiento del objetivo general, se realizó el cálculo de la confiabilidad del sistema redundante o paralelo, dando como resultado una confiabilidad de 92,12%, con este porcentaje se cumple satisfactoriamente el objetivo general, el cual tiene como indicador garantizar el envío y recepción de paquetes en un 90%.

Es importante mencionar que no se va a presentar problemas en la pérdida de información de las transacciones realizadas entre el SICAT y las centrales telefónicas, a pesar de que pueda existir un máximo de 5 minutos en que la avería no es atendida. Esto debido a la aplicación del sistema corporativo SICAT y al protocolo de comunicación utilizado. Cuando se envía alguna transacción desde el SICAT a una central telefónica y no llega respuesta de la central telefónica confirmando que la transferencia fue exitosa ya sea para este caso por un problema en la red; entonces, después de varios intentos, la aplicación del SICAT le indica al usuario, quien gestiona la transacción, que ocurrió un error en el envío del paquete y que se debe realizar la transacción más adelante. Esta es la forma en que trabaja el protocolo TCP/IP el cual se utiliza para la comunicación entre el SICAT y la central telefónica. En este sentido, puede ser que los datos se pierdan temporalmente pero el sistema SICAT lo detecta y vuelve a realizar las transacciones.

Dados los tiempos de ejecución del *script* para la detección de la avería de red, la conexión y desconexión de los módems ISDN, se realizó el cálculo de la duración del *script* para la evolución de 54 conexiones de red en el peor de los caso. Son 54 conexiones ya que de las 67 centrales telefónicas 54 se encuentran conectadas por la red institucional.

El *script* duraría en ejecutarse 4 minutos con 55 segundos para el peor de los casos, es decir, el caso en que al evaluar las 54 conexiones se presenten 10

simultáneamente con un fallo en la conexión de red. Uno de los objetivos específicos del proyecto era la detección de una avería de red en un tiempo máximo de 5 minutos. Dados los tiempos del *script* se puede comprobar que se logró cumplir este objetivo.

Otro de los objetivos específicos era lograr que el sistema realizara la conexión del enlace redundante en menos de 30 segundos.
La tabla 6.1 muestra los tiempos de inicio y fin de ejecución del *script* para el caso en que se detecte una avería de red y se deba establecer una conexión por medio de los módems ISDN.
En esta tabla se puede observar el tiempo de inicio y fin del *script* total, evaluando únicamente la dirección IP donde se detecta la avería de red. El *script* ejecutó primero el método llamado Paralelo.sh, la duración de este método para las cuatro mediciones realizadas fue de 11 seg. Con el tiempo total de ejecución del *script* (35 seg) y el tiempo en que tardó en ejecutarse el método Paralelo.sh se obtuvo el tiempo en que el *script* tarda en establecer la conexión de los módems ISDN y el enrutamiento de los paquetes hacia el módem ISDN actual que se conectó. La duración en configurar y realizar la conexión de los módems ISDN junto con el enrutamiento de los paquetes fue 24 segundos para todas las mediciones realizadas con lo cual se demuestra que el objetivo se cumplió satisfactoriamente.

El último objetivo es garantizar en un 99.5% la conmutación entre enlaces del lado de la central telefónica. Como se explicó con anterioridad, la conmutación del lado de la central telefónica se realiza desde el último enrutador encargado de brindar el servicio de red a las centrales telefónicas. A este enrutador se le conecta en una tarjeta de red, el módem ISDN y en otra la PC, para el caso del prototipo, en la realidad sería el TS.

En el diagrama del prototipo ilustrado en la figura 4.1.3, el enrutador mencionado es representado por el enrutador R2 y R3, se utilizaron dos

enrutadores ya que no se contaba con un enrutador que tuviera dos tarjetas de red, pero en la red actual estos enrutadores si cuentan con más de una tarjeta de red.

A todos los enrutadores (R1, R2, R3) se les configuró el protocolo RIP y se configuró en el enrutador R2, como una ruta estática de red (flotante), la red donde se encuentra el módem ISDN (10.149.68.21). Se debió configurar este segmento de red como una ruta estática debido a que en ella está conectado el módem ISDN, si no se define como una ruta estática el protocolo RIP no aprende esta ruta, por esta razón hay que definirla. Luego se definieron métricas o distancias administrativas, tanto a la red donde se encuentra el Módem ISDN (10.149.68.21), con métrica de 10, como a la red conectada al enrutador R1 (10.129.3.1) con métrica de 5. Al segmento de red de la 10.149.68.21 se le definió una distancia administrativa mayor que la de la red 10.129.3.2 para que se ejecutara la conmutación en caso de que falle la conexión por los enrutadores.

De esta forma la conmutación del lado de la central telefónica es realizada por el enrutador y en todas las mediciones que se realizaron, las cuales fueron más que las presentadas en los resultados experimentales, no se presentó ningún problema en la conmutación o enrutamiento realizado por el enrutador, es decir se realizaron el 100% de los enrutamientos.

Capítulo 7: Conclusiones y recomendaciones

7.1 Conclusiones

- El sistema redundante aumentó la confiabilidad del sistema actual en un 90,59%.

- El sistema logró tener un tiempo de respuesta ante cualquier fallo de red de 5 min.

- Se logró que el sistema atienda hasta 10 averías de red simultáneamente, lo cual cubre alrededor del 82% de los casos.

- Se logró establecer una conexión redundante en menos de 30 segundos.

- Se logró obtener una conmutación segura y estable tanto del lado del lado del servidor SICAT como del lado de las centrales telefónicas.

7.2 Recomendaciones:

- Para reducir la cantidad de puertos Ethernet utilizados en el router destino, se puede colocar un *switch* en un puerto Ethernet y conectar al *switch* el módem ISDN y el TS.

- Para aumentar la confiabilidad del sistema, enviar un mensaje al frontal principal cuando se presenta algún error o problema al realizar la conexión entre módems ISDN.

- Para reducir el tiempo de ejecución del *script*, recibir del SICAT una lista de las averías de red que detecte y que esta lista se actualice con cada fallo nuevo para así evitar enviar un *ping* a todas las redes de las centrales telefónicas y atender solo las regiones que están siendo utilizadas por el SICAT.

- Para reducir puntos de fallo en el sistema total, se puede incorporar dentro del servidor SICAT el frontal principal y el *script* controlador de enlaces.

Bibliografía

1. Configurar su módem y puerto serie [en línea] Wikilearning 2008 [citado 10 Marzo 2008]. Disponible en: http://www.wikilearning.com/tutorial/linux_pppconfigurar_su_modem_y_puerto_serie/20532-9

2. Configuración de una conexión PPP con un módem RTB bajo Unix - Permisos de archivos serie [en línea] Wikilearning 2008 [citado 10 Marzo 2008]. Disponible en: http://www.wikilearning.com/articulo/configuracion_de_una_conexion_ppp_con_un_modem_rtb_bajo_unix-permisos_de_archivos/7092-4

3. Ajustando el crontab [en línea] Aguayoki 2008 [citado 12 Mayo 2008]. Disponible en: <http://www.aguayoki.cl/blog/2005/06/18/ajustando-el-crontab/

4. Balanceo de Carga (1 LAN x WAN) [en línea] PreguntasLinux.Org 2008 [citado 12 Mayo 2008]. Disponible en:http://preguntaslinux.org/howto-balanceo-de-carga-lan-wan-t-129.html

5. Configuración de un gateway en Linux mediante IP Masquerading [en línea] El rincón del programador 2008 [citado 10 Marzo 2008]. Disponible en: http://www.elrincondelprogramador.com/default.asp?pag=articulos/leer.asp&id=40#ap3

6. Configuration Examples and TechNotes [en línea] Cisco 2008 [citado 10 Marzo 2008]. Disponible en: http://www.cisco.com/en/US/tech/tk801/tk379/tech_configuration_examples_list.html

7. Bridging Across ISDN [en línea] Cisco 2008 [citado 10 Marzo 2008]. Disponible en: http://www.cisco.com/en/US/tech/tk801/tk379/technologies_configurationexample09186a008009433e.shtml

8. Comparación entre IGRP y RIP [en línea] Aprende redes 2008 [citado 10 Marzo 2008]. Disponible en: http://www.aprenderedes.com/?p=83

9. Configuración básica de red 3 (Rutas dinámicas, RIP) [en línea] Diario de un aprendiz 2008 [citado 10 Marzo 2008]. Disponible en: http://vnanock.wordpress.com/2007/05/14/configuracion-basica-de-red3rutas-dinamicasrip/

10. Manual rapido de configuracion de un enrutador [en línea] Dpto. Ingeniería de Sistemas TelemáticosE.T.S.I. Telecomunicación – U.P.M. 2005 [citado 22 Abril 2008]. Disponible en: http://asignaturas.diatel.upm.es/rrss1/documentacion_archivos/LABORATORIO%20ACTUAL/manual_rapido_cisco.pdf

11. About the Cisco IOS Software Documentation [en línea] Cisco 2008 [citado 10 Marzo 2008]. Disponible en: http://www.cisco.com/en/US/docs/ios/12_0/np1/configuration/guide/1cabout.html

12. Comandos de RIP [en línea] [citado 10 Mayo 2008]. Disponible en: http://www.gratisweb.com/gulle79/network/ios/rip-commands.htm#def-metric

13. Configuracion de RIP [en línea] Aprende redes 2008 [citado 10 Mayo 2008]. Disponible en: http://www.aprenderedes.com/?p=77

14. Enrutamiento basico en Linux [en línea] [citado 7 Mayo 2008]. Disponible en: http://daniellerch.com/sources/doc/enrutamiento_basico_linux.html#La_herramienta_route

15. Manual como configurar Routers [en línea] Monografías.com 2008 [citado 7 Mayo 2008]. Disponible en: http://www.monografias.com/trabajos42/configurar-routers/configurar-routers.shtml

16. Confiabilidad de sistemas eléctricos [en línea] [citado 13 Junio 2008]. Disponible en: http://www.procobre.org/archivos/peru/confiabilidad_sistemas_electricos.pdf

17. Conectar a través de ssh sin password con expect eléctricos [en línea] LinuTeca 2008 [citado 13 Junio 2008]. Disponible en: http://linuteca.com/conectar-a-traves-de-ssh-sin-password-con-expect/

18. Telnet [en línea] Wikipedia 2008 [citado 13 Junio 2008]. Disponible en: http://es.wikipedia.org/wiki/Telnet

19. Richard A. Jonson. *Probabilidad y Estadística para ingenieros de Millar y Freíd.* 5ta ed (pp 549).México. Prentice-Hall Hispanoamericana S.A, 1997.

20. Módulo 4: ISDN y DDR [en línea] Blog de Serapa 2008 [citado 19 Junio 2008]. Disponible en:http://serapa.blogspot.com/2008/01/semestre-4-ccna-mdulo-3_29.html

21. RIP (Protocolo) [en línea] Wikipedia 2008 [citado 19 Junio 2008]. Disponible en: http://es.wikipedia.org/wiki/RIP_(protocolo)

Apéndices

A.1 Glosario, abreviaturas y simbología

Frontal: Computadora cliente en un sistema de comunicación tipo servidor – cliente.

Red: Existe una red, cuando dos o más dispositivos se encuentran conectados entre sí.

Red IP del ICE: Red de dispositivos del ICE que utilizan el protocolo de comunicación TCP/IP.

Intranet: Es una red privada.

Cliente: Es quien realiza una petición de algún servicio.

Servidor: Es un recurso de cómputo dedicado a atender las peticiones de los clientes.

Servidor SICAT: Sistema de Categorización Automática.

RDSI: Red Digital de Servicios Integrados, red establecida por conexiones de líneas telefónicas RDSI.

Paquete: Contiene la información a transmitir así como las características de ésta, por ejemplo, dirección origen, dirección destino, tamaño de la información, chequeo de errores, temporización y características propias del protocolo de comunicación.

Enlace redundante: Enlace de respaldo que entra a funcionar cuando el enlace principal falla, generando más de una posible ruta para cada paquete.

Ruta: Camino por donde se envía un paquete.

Sistema corporativo: Sistema para la gestión de diversos servicios.

SNT: Acrónimo de Sistema de Telefonía Nacional.

Ping: Es una orden utilizada para verificar el acceso a direcciones IP, este envía un paquete ICMP de petición de eco y espera la respuesta desde la dirección a donde envió el paquete

HDLC: Control de enlace de datos de alto nivel.

PPP: (Point to Point Protocol - Protocolo Punto a Punto). Protocolo de nivel de enlace de datos para hacer conexión entre dos puntos (dos computadoras o nodos).

Trama: es un bloque de datos de longitud fija o variable, que ha sido codificado por un protocolo de comunicaciones en la capa de enlace de datos, para la transmisión digital sobre un enlace nodo-a-nodo.

LAPD: El LAPD es un protocolo de capa de enlace de datos basado en el HDLC, utilizado en el canal D de la red RDSI.

Cron: En Linux cron es un planificador de tareas que se utiliza para ejecutar procesos, definiendo una frecuencia de ejecución (cada minuto, día, semana, día de la semana o mes).

Full duplex: Se refiere a la transmisión de datos en dos direcciones simultáneamente

A.2 Información sobre la empresa/institución

Nombre: Instituto Costarricense de Electricidad (ICE).

Zona: San José, San Pedro.

Actividad Principal: Brindar servicios de energía y telecomunicaciones a todo el país

Información del encargado en la empresa:

Nombre: Ing. Javier Alan.

Puesto que ocupa: Jefe de la plataforma de Servicios

Departamento: Departamento de Redes y Sistemas.

Teléfono: 206-1513

Email: jalan@ice.co.cr

Información del asesor en la empresa:

Nombre: Ing. Javier Alan

Puesto que ocupa: Jefe de la plataforma de Servicios

Departamento: Departamento de Redes y Sistemas.

Teléfono: 206-1513

Email: jalan@ice.co.cr

Anexos

Manual de usuario del módem ISDN marca DIVA LAN

Chapter Four

The Web-based Configuration Interface

The DIVA LAN ISDN Modem uses a single ISDN link to provide communications services for all your connected devices. It manages incoming and outgoing data calls from your computers, as well as incoming and outgoing analog calls from connected telephones and/or fax machines.

To accomplish all this, the DIVA LAN ISDN Modem implements a number of important ISDN features that enable complex communications requirements to be supported on a single link. When you define your setup with the Internet wizard, a number of parameters are set to default values that give good results for most cases. However, due to the number of options that are available, the Internet wizard cannot fine tune all settings for your particular installation. For optimal performance, or to define a custom setup, you must manually adjust the configuration of the DIVA LAN ISDN Modem.

The web-based configuration interface provides you with an easy way to manage the configuration of the DIVA LAN ISDN Modem, and perform other tasks like viewing status and statistics on your connections, and updating your system firmware.

This chapter explains how to access the web-based configuration interface, and gives step-by-step instructions for some common tasks.

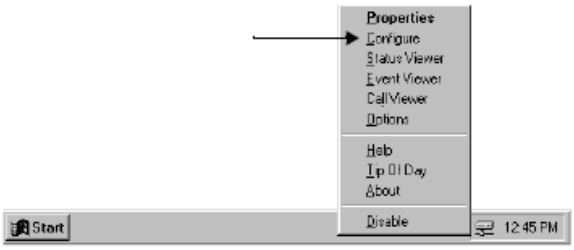
Starting the web-based configuration interface

The web-based interface enables you to manage the configuration and operation of the DIVA LAN ISDN Modem. It also lets you view status information and perform maintenance tasks like updating the firmware.

Note *Only one user can access the web-based configuration interface at a time.*

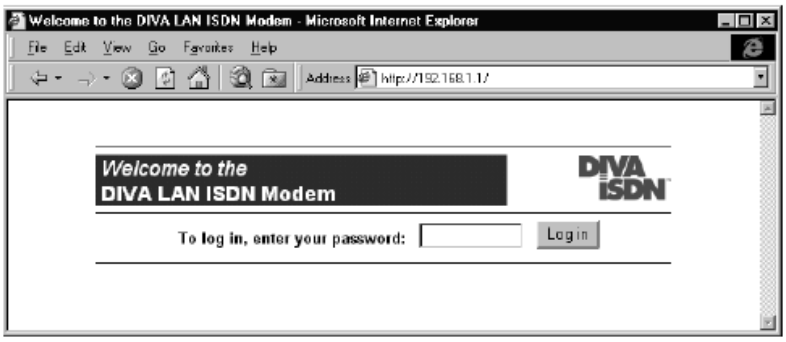
To start the web-based configuration interface

1. *If you installed the Modem Monitor software*
   - Right-click the DIVA LAN ISDN Modem icon in your system tray, and click Configure on the menu. Your default web browser will start.



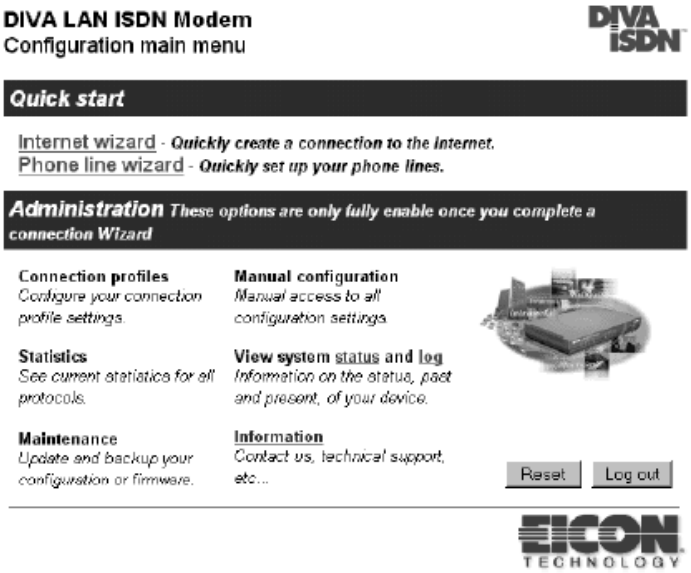
If you did not install the Modem Monitor software
   - Start your web browser software, specify the URL "diva.lanmodem" or the default IP address of the DIVA LAN ISDN Modem (192.168.1.1), and press Enter. (If you changed the address or name of the DIVA LAN ISDN Modem, enter the new name or address instead.)

2. Your web browser will load the Log In page.



3. Enter the *system password*, if required, and click Log In.
4. The first time you log in, you must choose the country or region you are located in and click OK. If your region does not appear in the list, choose International (the last entry in the list).

5. The DIVA LAN ISDN Modem displays the Main configuration menu.



Note *The first time you access the web-based configuration interface, most of the options in the Administration section are not available. They are only activated once you have defined your configuration settings using the Internet wizard.*

Saving configuration settings

Most pages in the configuration interface have a Save button. When you click this button, your changes are sent to the DIVA LAN ISDN Modem. However, for the changes to take effect, you must reset the DIVA LAN ISDN Modem. Do this by clicking the Reset button on the Manual Configuration menu.

Getting help

Context-sensitive help is available for each parameter. Simply click the parameter name to display its description.

On some pages, you can get general information about the page by clicking the question mark that appears on the title bar.

General settings and connection profiles

Before you begin customizing your configuration, you should familiarize yourself with how the DIVA LAN ISDN Modem organizes its configuration settings.

Configuration settings are split into two groups: general settings and connection profile settings.

General settings

General settings apply to the DIVA LAN ISDN Modem as a whole, and cover global settings like system time, password, ISDN phone numbers, phones lines, etc.

Connection profile settings

A connection profile is a group of configuration settings that define the characteristics of an incoming or outgoing connection. Each profile has a number of settings that you can customize.

Connection profile types

The DIVA LAN ISDN Modem supports two profiles: ISP and Corporate. Both can be active at the same time, allowing you to handle different types of connections.

ISP profile

This profile is created by the Internet wizard. It defines the settings for a connection to the Internet. You can use the Manual Configuration option to customize the settings of this profile.

Corporate profile

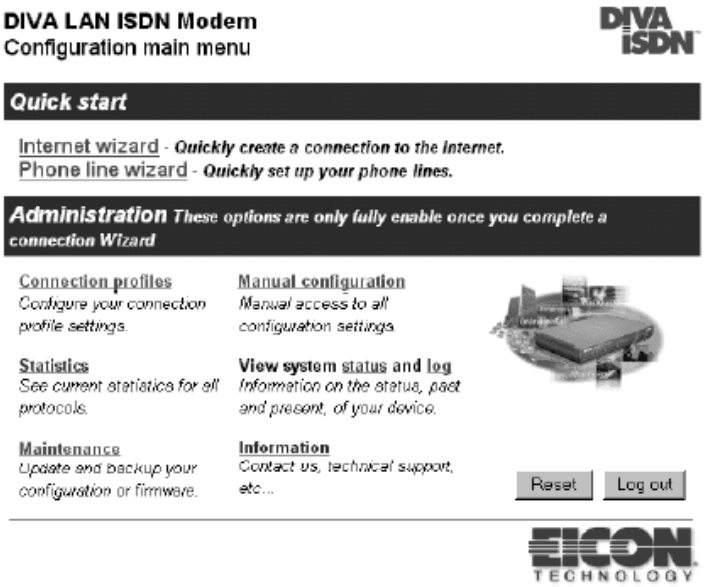
This profile is provided so you can define the settings for a connection to a remote corporate network. See Chapter Eight for more information.

Editing the ISP profile

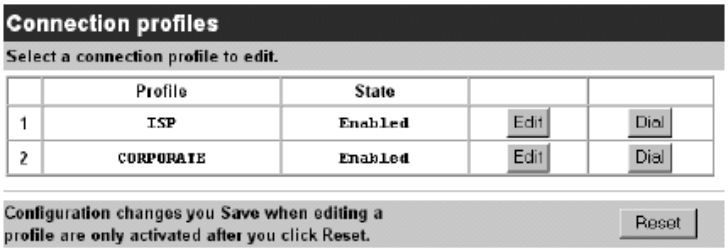
After you have defined your connections with the Internet wizard, it may be necessary to fine tune certain parameters manually. To do this, you need to edit the ISP profile settings. Although it is possible to change the names of this profile, it is not recommended.

To edit the ISP profile

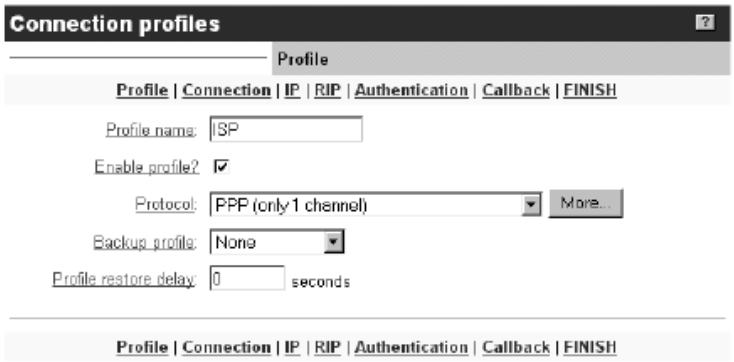
1. Start the web-based configuration interface and log in. The DIVA LAN ISDN Modem displays the Main configuration menu.



2. Click *Connection profiles*. The DIVA LAN ISDN Modem displays the Connection Profiles list page.



3. Click *Edit* for the ISP profile. The DIVA LAN ISDN Modem displays the Profile page.



4. Use the menu bar to navigate between the six configuration pages: Profile, Connection, IP, RIP, Authentication, and Callback. For a description of each parameter, just click the parameter name. The DIVA LAN ISDN Modem will display a help window.
5. When you are done with your settings, click *Finish*, then click *Save*.
6. To activate the settings you must reset the DIVA LAN ISDN Modem. Click the *Reset* button on the Connection Profiles list page.

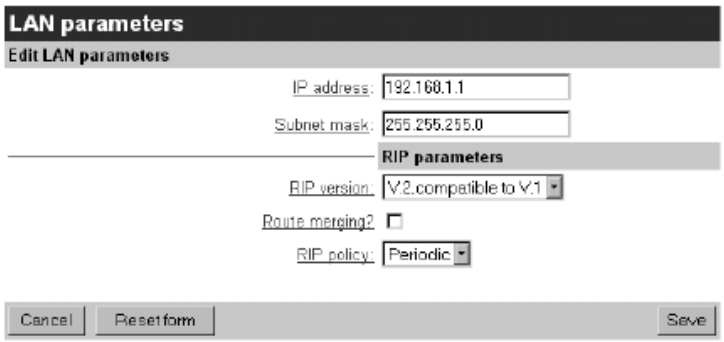
Editing LAN settings

The LAN parameters page defines the settings for the LAN created by the Ethernet hub built into the DIVA LAN ISDN Modem. You need to modify these settings if:

- you need to assign a specific (static) IP address to it. This is usually the case when installing on an existing LAN. See page 104 for more information.
- you want to alter the routing information protocol (RIP) settings the DIVA LAN ISDN Modem uses on the LAN. For more information see "The Routing Information Protocol (RIP)" on page 117.

To edit the LAN profile

1. On the Manual Configuration menu, click *LAN*. The DIVA LAN ISDN Modem displays the LAN Parameters page.



2. Make your configuration changes. For a description of each parameter, just click the parameter name. The DIVA LAN ISDN Modem will display a help window.
3. Click *Save*.
4. Click *Reset*.

System status

Indicates the status of each of your ISDN channels (via front panel lights).

The status of each porfile is also shown. It can be one of the following:

- *Connected:* The profile is in use for a data connection.
- *Ready:* The profile is ready to make a connection.
- *Pause before dialing:* Profile is about to dial out.
- *Failed:* The profile was disabled automatically because:
  - The profile failed to connect and exceeded the retry limit. See "Connection retries" on page 103.
  - The profile exceeded the defined call thresholds. See "Data call thresholds" on page 52
- *Disabled:* The profile was disabled manually.

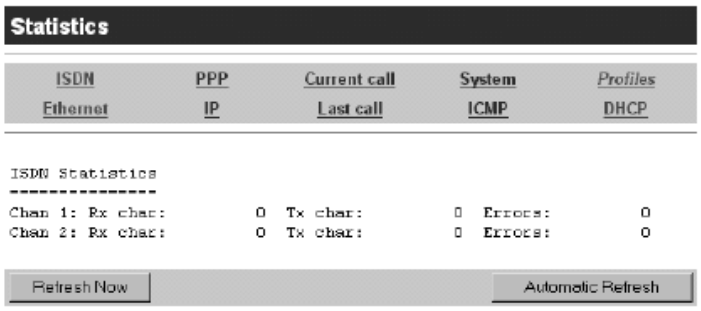
Front panel display

Shows the status of the front panel LEDs. See "DIVA LAN ISDN Modem indicator lights" on page 147 for more information.

Obtaining statistics

The DIVA LAN ISDN Modem records a view variety of statistics, which you can use for information and troubleshooting purposes.

Click Statistics on the Main configuration menu, then choose the type of statistics you want to view from the menu bar. For example, the following screen shows ISDN statistics.



Click the *Automatic Refresh* button to have the page updated every 4 seconds. Otherwise, click the *Refresh Now* button to update the statistics when you require them.

Chapter Six

Security

Connecting your computers to the internet or a remote corporate LAN creates a wide range of benefits, but also exposes your computers to certain risks. To safeguard your data and systems, the DIVA LAN ISDN Modem provides a comprehensive range of security features. This chapter explains how to use and configure each feature for optimal protection of your systems.

Security features

This table lists all security features offered by the DIVA LAN ISDN Modem, and their default settings.

Feature	Default	Description
System password	None	Restricts access to the DIVA LAN ISDN Modem configuration interfaces.
Automatic log out	Active	Automatically terminates idle configuration sessions.
Network address translation (NAT)	Active	NAT hides the addresses of the computers on the internal Ethernet LAN from the external network.
Remote management	Disabled	Permits remote systems to log on to the DIVA LAN ISDN Modem configuration interfaces (Web or CLI).
Incoming data calls	Disabled	Permits the DIVA LAN ISDN Modem to answer incoming data calls.
Call screening	Disabled	Allows you to accept incoming data calls from specific phone numbers only.
Call authentication	Always authenticate	Lets you validate incoming data calls, or respond to authentication requests when making outgoing data calls.
Callback	Disabled	Forces the remote site to call back to establish the connection.
Manual dialing	Disabled	Enables you to manually control when the ISDN link is established.
Custom security using IP filters	None	Enables you to filter specific IP datagrams for security reasons.

The following table lists the security features that can be applied to restrict access to the DIVA LAN ISDN Modem configuration interfaces.

Source system	Connected via	Security features that apply
Remote computer	ISDN	• System password • Automatic log out • Remote Management • Answer incoming data calls • Call screening • Call authentication • Custom security using IP filters
Local computer	Ethernet	• System password • Automatic log out • Custom security using IP filter
Local computer	Serial	• System password
Telephone	Phone port	• (Only available when the ISDN is not connected.)

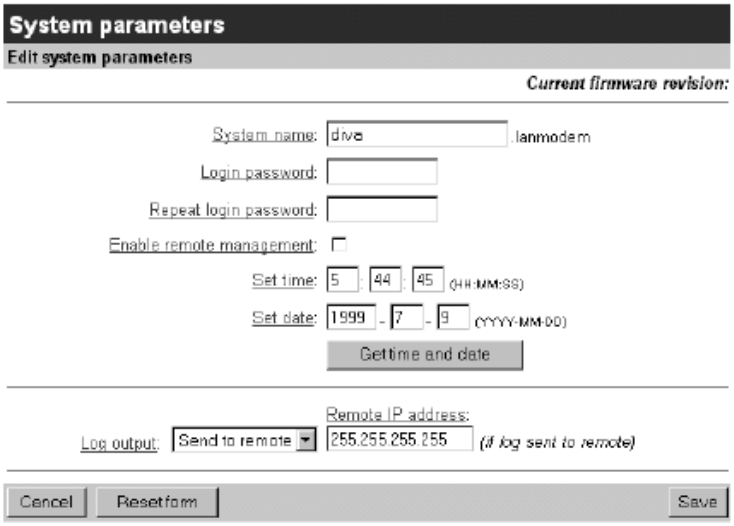
System password

The DIVA LAN ISDN Modem provides a system password that restricts access to the Web-based configuration interface and the CLI. This ensures that configuration changes can only be made by authorized personnel.

By default, no password is defined.

To set the system password

1. On the Manual Configuration menu, click *System*.
2. Enter the system password in the *Login Password* and *Repeat Login Password* fields.



3. Click *Save*.
4. Click *Reset*.

To erase the system password

It can happen that you might forget your system password. The only way to erase the system password is to reset the DIVA LAN ISDN Modem to its factory defaults. This also returns all configuration settings to their default values. See "Resetting the DIVA LAN ISDN Modem" on page 150 for instructions.

Automatic log out

The DIVA LAN ISDN Modem applies an automatic time out to configuration sessions. When a configuration session is idle for more than the time out value, the DIVA LAN ISDN Modem automatically logs the user out. This reduces the risk of unauthorized persons taking advantage of a logged-in computer that has been left unattended. Time outs are not configurable and are set as follows:

- If you are using the web interface, the time out is 30 minutes.
- If you are using Telnet, the time out is 5 minutes.
- If you are using a direct serial connection, there is no time out.

Note *Changes that have not been saved are lost when the configuration session is terminated.*

Incoming data calls

By default, the DIVA LAN ISDN Modem refuses all incoming ISDN data calls. This effectively shuts the door on unauthorized systems dialing-in. (Voice calls are not blocked by this setting.)

When support for incoming data calls is activated and an incoming call is received, the DIVA LAN ISDN Modem compares the user name and password supplied by the remote site against the remote user name and remote password configured for the ISP profile, then the CORPORATE profile. If a match is found, the call is accepted. Otherwise, the call is rejected. Therefore, to accept incoming data calls you must define call authentication settings for the appropriate profile (as explained in the steps below).

Note *Since the DIVA LAN ISDN Modem checks the ISP profile first, if both profiles have the same remote user name, the incoming call will always connect with the ISP profile.*

Incoming data calls can only be received if there is an available B-channel. To keep a free channel, you must use PPP (or V.120) for your existing connection. If you are using MLPPP, you will only be able to receive incoming voice calls if no data call is active. See "Choose a connection protocol" on page 19 for more information.

Note *When you enable callback support (page 76) using the web configuration interface, the DIVA LAN ISDN Modem automatically enables support for incoming data calls.*

Incoming calls and IP addressing

For an incoming call to successfully connect, you must define a proper IP addressing scheme for the profile that will handle the connection. This means setting the following three parameters: *IP address*, *Subnet mask*, and *Remote IP address*.

Generally, when you configure the DIVA LAN ISDN Modem to connect to the Internet, you set the *IP address* parameter to 0.0.0.0, which means that the address will be dynamically assigned by the ISP when the profile connects. When you receive an incoming call however, it may be the responsibility of the DIVA LAN ISDN Modem to assign an IP address to the caller. In this case, the static address you set for *Remote IP address* would be adopted by the caller.

The following diagram illustrates the effects of potential addressing schemes. (The subnet mask is omitted from this discussion, but should be set to match the IP address. See"About IP addresses" on page 111 for more information on masks.)

	DIVA LAN ISDN Modem		Remote Computer
1	IP address: *static* Remote IP address: *static*	*Assigned to* →	IP address: dynamic Remote IP address: dynamic
2	IP address: *static* Remote IP address: dynamic	*No assignments*	IP address: *static* Remote IP address: dynamic
3	IP address: *static* Remote IP address: *static*	← *Addresses must match* →	IP address: *static* Remote IP address: *static*
4	IP address: dynamic Remote IP address: dynamic	← *Assigned to*	IP address: *static* Remote IP address: *static*
5	IP address: *static* Remote IP address: dynamic	*Fails*	IP address: dynamic Remote IP address: dynamic
6	IP address: dynamic Remote IP address: dynamic	*Fails*	IP address: static Remote IP address: dynamic
7	IP address: dynamic Remote IP address: dynamic	*Fails*	IP address: dynamic Remote IP address: dynamic

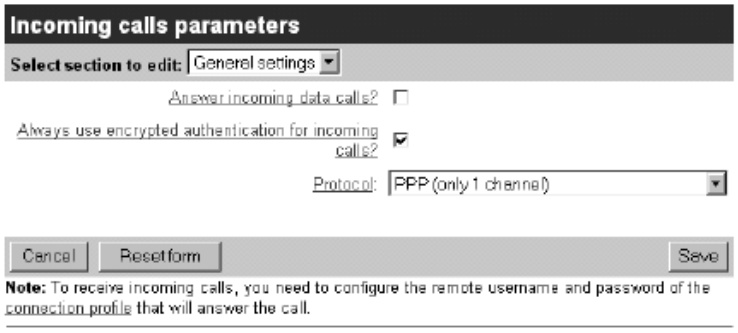
Notes on the diagram

1. The DIVA LAN ISDN Modem provides an IP address to the remote computer.
2. Both the DIVA LAN ISDN Modem and the remote computer have their own fixed IP addresses so no assignments are made.
3. Both the DIVA LAN ISDN Modem and the remote computer have their own fixed IP addresses AND have specified remote addresses. This means they will only be able to connect if the remote addresses match the IP addresses of the other device.
4. The remote computer provides an IP address to the DIVA LAN ISDN Modem.
5. The remote computer has no IP address and the DIVA LAN ISDN Modem is not configured to supply one.
6. The DIVA LAN ISDN Modem has no IP address and the remote computer is not configured to supply one.
7. Neither device has an IP address and neither is configured to supply one.

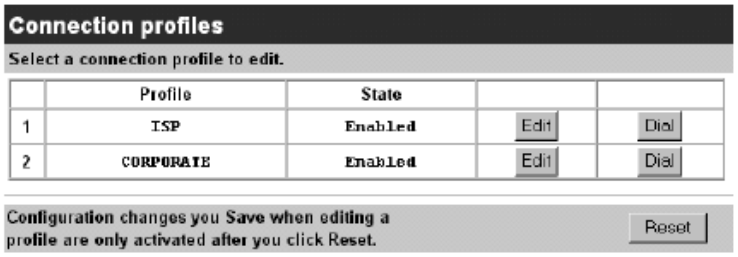
To enable support for incoming data calls

To turn on and configure support for incoming calls, do the following:

1. On the Manual Configuration menu, click *Incoming data calls*. This displays the Incoming calls parameters page.



2. Enable *Answer incoming data calls*.
3. Specify the type of password the DIVA LAN ISDN Modem expects the remote to send: encrypted or any (unchecked). If the supplied password is not in the proper format the call is rejected.
4. Choose the type of connection protocol to use for the call. The setting you make here takes precedence over the setting for the profile that will answer the call.
5. Click *connection profile* in the Note at the bottom of the page. The DIVA LAN ISDN Modem displays the Connection profiles list page.



6. Click *Edit* for the profile that will answer the call.
7. Click *Authentication*.
8. Define the *Remote username* and *Remote password* the DIVA LAN ISDN Modem expects the remote to send. See "Call authentication" on page 74 for more information.
9. Click *IP*.
10. Set *IP address*, *Subnet mask*, and *Remote IP address* as required.

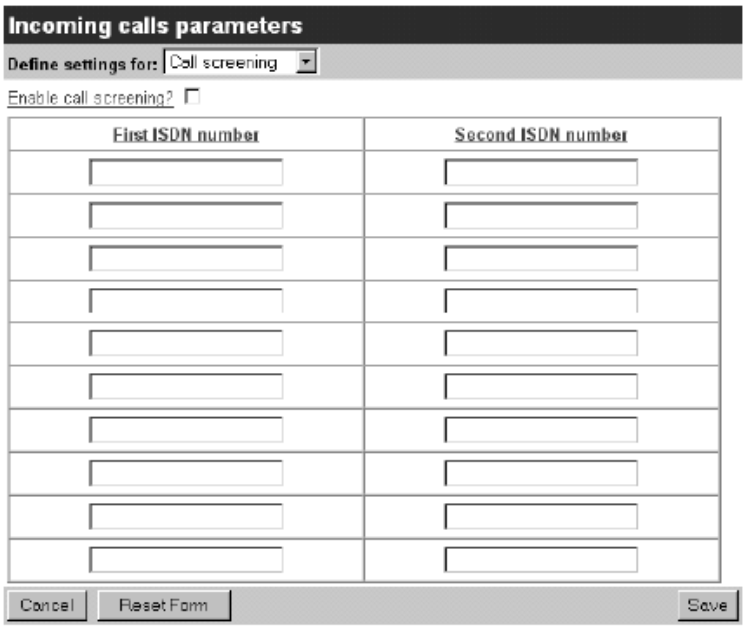
11. Click *Finish*.
12. Click *Save*.
13. Click *Reset*.

Call screening

Call screening enables you to accept or reject incoming data calls based on their phone number. This is an effective way to limit dial-in access to the DIVA LAN ISDN Modem to a small group of remote sites.

To set up call screening

1. On the Manual Configuration menu, click *Incoming data calls*.
2. In the *Define settings for* box choose *Call screening*. You will see the following page.



3. Check the *Enable call screening* box.
4. Enter the phone numbers of the remote sites you want to receive calls from. Enter the same phone number under *First ISDN number* and *Second ISDN number*.
5. Click *Save*.
6. Click *Reset*.

Call authentication

Call authentication enables ISDN devices, like the DIVA LAN ISDN Modem, to validate the identity of the device at the other end of the line. Authentication works through the exchange of usernames and passwords. It can be one-way (either the caller gets validated or the callee gets validated) or two-way (both sides validate each other).

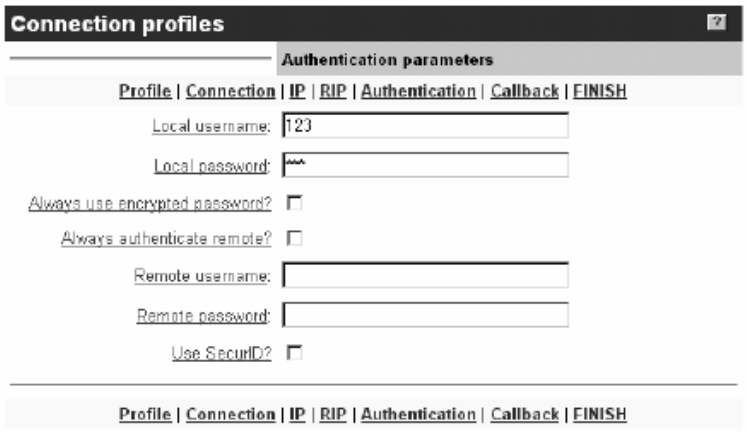
Generally, authentication is one-way, with the caller getting validated. For example:

- When the DIVA LAN ISDN Modem calls an ISP or a corporate network, it will be authenticated (i.e., it must supply a username and password to log on).
- When a remote computer calls the DIVA LAN ISDN Modem, it will be authenticated (i.e., it must supply a username and password for the call to be accepted).

To successfully use call authentication it is important that both devices are configured to support the same authentication options.

To set up call authentication

1. On the Configuration main menu, click *Connection Profiles*.
2. Click *Edit* for the profile you want to configure.
3. Click *Authentication* on the menu bar. You will see the following page:



4. Specify the *Local username* and *Local password* this profile will send to the remote site during the authentication process. For example, the ISP profile uses these values to log on to your ISP account.

   Note *Local username and Local password are case-sensitive.*

5. Specify the type of password the DIVA LAN ISDN Modem will send to the remote: encrypted or any (unchecked). If the remote is not using the same type of encryption, the call will be rejected.

   Note *This setting applies to outgoing calls only.*

6. Enable *Always authenticate the remote* if you want the DIVA LAN ISDN Modem to ask the remote to identify itself with a username and password. The DIVA LAN ISDN Modem will compare the values the remote sends against the settings you make for *Remote username* and *Remote password*. Remote username and Remote password are case-sensitive.

   Note *This setting applies to outgoing calls only. The DIVA LAN ISDN Modem always authenticates the remote when receiving an incoming call.*

7. Click *Finish*.
8. Click *Save*.
9. Click *Reset*.