# ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

## Facultad de Ingeniería en Electricidad y Computación

"Simulador de Protocolos de Comunicaciones"

## TESIS DE GRADO

Previo a la obtención del Título de:

## INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentada por:

Manuel Freire Medina
Roberto Muñoz Jaramillo
Johnny Rivero Guevara

GUAYAQUIL – ECUADOR
Año: 2009

# A G R A D E C I M I E N T O

A todas las personas que de una u otra manera colaboraron en la realización de este trabajo y específicamente a la gran ayuda de mi Director el Ing. José Escalante.

# DEDICATORIA

A DIOS

A NUESTROS PADRES

Y A TODA NUESTRA

FAMILIA

# TRIBUNAL DE GRADUACIÓN

Msc. Jorge Aragundi
SUB-DECANO
PRESIDENTE

Ing. José Escalante
DIRECTOR DE TÓPICO

Ing. Ivonne Martin
VOCAL

Dr. Boris Ramos
VOCAL

# DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL).

**Roberto Muñoz Jaramillo** **Johnny Rivero Guevara**

**Manuel Freire Medina**

# RESUMEN

En el capítulo 1 se dará a conocer los modelos de arquitectura de comunicaciones como el OSI y el TCP/IP, sus similitudes y diferencias, también los tipos de redes digitales y analógicas, así también podremos diferenciar redes que usan conmutación por circuitos con redes que usan conmutación por paquetes, y por último conoceremos las diferentes interfaces que existen tanto para redes LAN como WAN.

En el capítulo 2 analizaremos a profundidad la estructura de los protocolos de comunicaciones que se usan en la actualidad como el MAC, IP para redes LAN; y HDLC, Frame Relay y ATM para redes WAN. Se revisará las diferencias y ventajas que brindan los protocolos de capa 2 como Frame Relay y ATM para transporte de datos multimedia.

En el capítulo 3 se tratarán con las diferentes tipos de herramientas que existen para analizar y monitorear las redes, así como analizadores y/o simuladores, se revisará software que sirve para analizar el tráfico en las redes así como también hardware que sirve para analizar y simular redes con diferentes protocolos a nivel LAN y WAN.

En el capítulo 4 se realizarán las pruebas de monitoreo de redes con protocolos a nivel LAN y WAN. El objetivo de este capitulo es tener como

referencia una herramienta de análisis y simulación de redes y tener modelos de practicas para poder simular redes bajo protocolo IP, HDLC, Frame Relay y ATM.

En el capítulo 5 se realizarán los costos de la implementación de un laboratorio.

Finalmente se dan a conocer las conclusiones y recomendaciones.

# INDICE GENERAL

**Pág.**

# INDICE DE FIGURAS

# INDICE DE TABLAS

# INTRODUCCIÓN

Para compartir datos por la red es necesaria una comunicación previa, y esta comunicación se rige a través de ciertos protocolos que, bajo su cumplimiento, permiten la comunicación. Esta premisa originó la idea del proyecto "Simulación de protocolos de Comunicaciones” que con equipos de simulación permite analizar, entender como un paquete o trama viaja a través de una red para proveer servicios de datos usando un equipo analizador de protocolos Radcom RC-100WL. Se tratarán con las diferentes tipos de herramientas que existen para analizar y monitorear las redes, así como analizadores y/o simuladores, se revisará un software que sirve para analizar y simular redes con diferentes protocolos a nivel LAN y WAN. Se realizará un análisis de la estructura de las tramas o paquetes de los protocolos que se usan en la actualidad como MAC, IP para redes LAN y HDLC, Frame Relay y ATM para redes WAN.

# CAPÍTULO 1

## 1. Aspectos Básicos de Redes

### 1.1.- Modelo OSI

El Modelo de Referencia de Interconexión de Sistemas Abiertos, fue creado por la Organización Internacional de Normalización (ISO), debido a que a principios de la década del ochenta, se produjo un gran crecimiento de las redes de datos; esto implicó que los equipos de distintos fabricantes no puedan intercambiar información dado a que utilizaban diferentes especificaciones.

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI) lanzado en 1984, fue el modelo de red descriptivo creado por la ISO; esto es; un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones[1].

---

[1] Tomado de http://es.wikipedia.org/wiki/Modelo_OSI

### 1.1.1 Ventajas del Modelo OSI

El modelo OSI se utiliza por las siguientes razones:

- Al dividir la comunicación de red permite un menor tiempo en el diagnóstico de fallas de las redes
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Previene que los cambios que se producen en un área afecten a las demás, para que cada área pueda evolucionar más rápidamente.
- Permite que los diseñadores de red elijan los dispositivos y las funciones de red adecuadas para esa capa.

### 1.1.2 Capas del modelo OSI

El modelo OSI se puede comprender como viaja la información a través de una red, en este, hay siete capas enumeradas (ver figura 1.1), cada una de las cuales tiene una función específica.

**Aplicación (Capa 7)** – Se encarga de suministrar servicios de red a las aplicaciones del usuario final. Estos servicios de red incluyen acceso a archivos, aplicaciones, etc.

| |
|---|
| 7 Aplicación |
| 6 Presentación |
| 5 Sesión |
| 4 Transporte |
| 3 Red |
| 2 Enlace de datos |
| 1 Física |

**Figura 1.1** Capas del modelo OSI

**Presentación (Capa 6)** – Se encarga de la representación de los datos transmitidos, es decir cada ordenador puede tener su propia forma de representación interna de los datos, por lo que es necesario tener acuerdos y convenciones para poder asegurar el entendimiento entre diferentes ordenadores.

**Sesión (Capa 5)** – Esta capa de sesión establece, mantiene y administra conversaciones, denominadas sesiones, entre dos o más aplicaciones de distintas computadoras. La capa de sesión se encarga de mantener las líneas abiertas durante la sesión y de desconectarlas cuando concluyen.

**Transporte (Capa 4**) – Esta capa toma el archivo de datos y lo divide en segmentos para facilitar la transmisión. Su principal objetivo es garantizar una comunicación fiable y eficiente entre dos computadoras, con independencia de los medios empleados para su interconexión. Para conseguir este objetivo se emplea protocolos de transporte.

**Red (Capa 3)** – La capa de red agrega direcciones lógicas o de red, como las direcciones de Protocolo de Internet (IP), a la información que pasa por ella. Con la adición de esta información de direccionamiento, los segmentos en esta etapa se denominan paquetes. Esta capa determina la mejor ruta para transferir los datos de una red a otra.

**Enlace de datos (Capa 2)** – La capa de enlace de datos administra la notificación de errores, la topología y el control de flujo. Reconoce identificadores especiales que son únicos para cada host, tales como las direcciones de control de acceso a medios (MAC). Los paquetes de la Capa 3 se colocan en tramas que contienen estas direcciones físicas (MAC) de cada host origen y de destino.

**Física (Capa 1)** – Esta capa incluye los medios, como cable de par trenzado, cable coaxial y cable de fibra óptica para transmitir las tramas de datos. Además se define los medios eléctricos y mecánicos; el procedimiento y las funciones para activar, mantener y desactivar el enlace físico entre sistemas finales.

### 1.1.3 Proceso detallado de encapsulamiento

En todas las comunicaciones de una red parten de un origen y se envían a un destino. La comunicación es iniciada por la capa de aplicación desde un host origen hasta un host destino. En cuanto los datos se transfieren entre las capas del modelo OSI, estos van agregando información como encabezados y otros tipos de datos que es interpretada solo en la misma capa, la figura 1.2 detalla el envío de un correo electrónico.

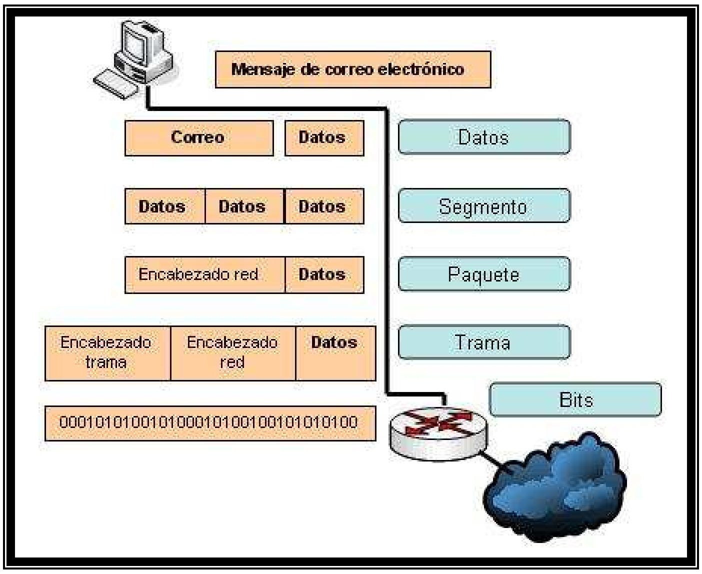



**Figura 1.2** Proceso detallado de encapsulamiento[2]

---

[2] Figura tomada de http://es.wikipedia.org/wiki/Modelo_OSI

Las redes deben realizar los siguientes cinco pasos de conversión a fin de encapsular los datos:

- Crear los datos.
- Empaquetar los datos para ser transportados de extremo a extremo.
- Agregar la dirección de red IP al encabezado.
- Agregar el encabezado y la información final de la capa de enlace de datos.
- Realizar la conversión a bits para su transmisión.

## 1.2 Comunicaciones de par a par

En el modelo OSI cuando existe una comunicación entre dos host los protocolos de cada capa en un mismo nivel intercambian información, esto se denomina comunicación par a par. Esta información que es intercambiada se denomina PDU, con lo cual cada capa del modelo OSI tiene un PDU específico como se detalla en la siguiente figura 1.3.

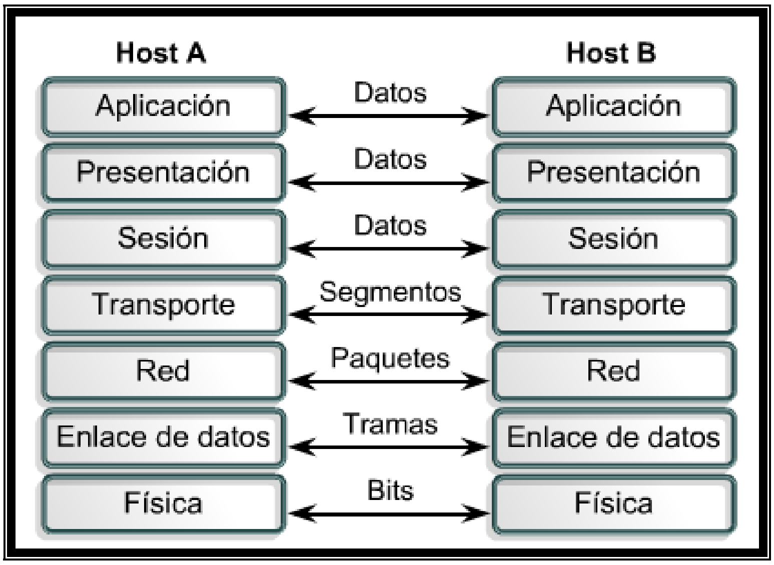



**Figura 1.3** Comunicación Par a Par[3]

## 1.3 Arquitectura de Comunicación

Es un conjunto de módulos que se comunican entre sí para la transferencia de datos, ejemplo TCP/IP.

### 1.3.1 Arquitectura TCP/IP

El Departamento de Defensa de EE.UU. (DoD) desarrolló el modelo de referencia TCP/IP que es un conjunto de reglas para que equipos compartan información en una red en cualquier tipo de medio.

---

[3] Figura tomada del curriculum CCNA 1

TCP/IP se creo como un estándar abierto que permitió un desarrollo acelerado del mismo.

### 1.3.2 Capas de la Arquitectura TCP/IP

El modelo TCP/IP tiene las siguientes cuatro capas:

- Capa de aplicación.
- Capa de transporte.
- Capa de Internet.
- Capa de acceso a la red.

**Aplicación (Capa 4)** – Esta capa se encarga de manejar aspectos de representación, codificación y control de diálogo.

**Transporte (Capa 3)** – Esta capa se encarga de aspectos como control de flujo, calidad del servicio, corrección de errores, segmentación y reensamble de datos en la comunicación. El protocolo principal de esta capa es el de control de transmisión (TCP), definido en la RFC-793; es un protocolo orientado a conexión, es decir mantiene una conexión lógica entre sus extremos. Además está el protocolo de datagrama de usuario (UDP) definido en la RFC-768; que es un protocolo no orientado a conexión y se lo utiliza cuando la aplicación necesita un tiempo de respuesta menor dado a que su cabecera es muy simplificada por lo cual no consume muchos recursos en su transmisión.

**Internet (Capa 2)** – El propósito de la capa Internet es utilizar los datos de las capas superiores, es decir; los segmentos TCP o UDP empaquetarlos y enviarlos en la red. En este caso el protocolo Internet (IP) definido en la RFC-791 el que permite que los paquetes lleguen a su destino independientemente de la ruta que utilizaron para llegar allí.

**Acceso a la red (Capa 1)** – En esta capa se refiere a cualquier tecnología utilizada en una red. Esto incluye a todas las tecnologías de la capa física y enlace de datos del modelo OSI.

### 1.4 Diferencia y similitudes entre el Modelo OSI y TCP/IP

Entre el modelo OSI con los modelos TCP/IP, surgen algunas similitudes y diferencias.

Las similitudes incluyen:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.

- Ambos suponen que se conmutan paquetes, esto significa que para llegar a un destino común varios paquetes pueden utilizar distintas rutas en la red.

Las diferencias incluyen:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en la capa de acceso de red.
- TCP/IP parece ser más simple porque tiene menos capas.

### 1.5.- Redes conmutadas

Cuando los datos son enviados de un nodo origen a un destino, generalmente deben pasar por varios nodos intermedios. Estos nodos son los encargados de dirigir los datos para que lleguen a su destino. Hay nodos sólo conectados a otros nodos y su única misión es conmutar los datos internamente a la red. También hay nodos conectados a host y a otros nodos, por lo que deben de añadir a su función como nodo, la aceptación y emisión de datos de los host que se conectan.

Generalmente hay más de un camino entre dos host, para así poder desviar los datos por el camino menos congestionado. Para redes WAN, generalmente se utilizan otras técnicas de conmutación: conmutación de circuitos y conmutación de paquetes.

### 1.5.1.- Conmutación por circuitos

Para cada conexión entre dos host, los nodos intermedios dedican un canal lógico a dicha conexión. Para establecer el contacto y el paso de la información de host a host a través de los nodos intermedios, se requieren estos pasos:

- Establecimiento del circuito
- Transferencia de datos
- Desconexión del circuito

Para tráfico de datos, la conmutación de circuitos suele ser bastante ineficiente ya que los canales están reservados aunque no circulen datos a través de ellos.

Para tráfico de voz, en que suelen circular datos (voz) continuamente, puede ser un método bastante eficaz ya que el único retardo es el establecimiento de la conexión, dado a que el canal ya está establecido.

### 1.5.2.- Conmutación por paquetes

En conmutación de paquetes, los datos se transmiten en paquetes cortos. Para transmitir grupos de datos grandes, el emisor divide estos grupos en paquetes pequeños y les adiciona una serie de bits de control. En cada nodo, el paquete se recibe, se almacena durante un cierto tiempo y se transmite hacia el emisor o hacia un nodo intermedio.

Las ventajas de la conmutación de paquetes frente a la de circuitos son:

- La eficiencia de la línea es mayor, cada enlace se comparte entre varios paquetes que estarán en cola para ser enviados en cuanto sea posible. En conmutación de circuitos, la línea se utiliza exclusivamente para una conexión, aunque no haya datos a enviar.

- Se permiten conexiones entre host de velocidades diferentes, esto es posible porque los paquetes se irán guardando en cada nodo conforme lleguen (en una cola) y se irán enviando a su destino; en cada nodo se crean criterios de prioridad.

Cuando un emisor necesita enviar un grupo de datos mayor que el tamaño fijado para un paquete, este los fragmenta en paquetes y los envía uno a uno al receptor.

Hay dos técnicas básicas para el envío de estos paquetes:

**Técnica de datagramas**: cada paquete se trata de forma independiente, es decir, el emisor enumera cada paquete, le añade información de control (por ejemplo número de paquete, nombre, dirección de destino, etc.) y lo envía hacia su destino. Puede ocurrir que por haber tomado caminos diferentes y lleguen a su destino en diferente orden, por lo que tiene que ser el receptor el encargado de ordenar los paquetes y saber los que se han perdido (para su posible reclamación al emisor), y para esto los protocolos de capa superior son los encargados.

**Técnica de circuitos virtuales**: antes de enviar los paquetes de datos , el emisor envía un paquete de control que es de Petición de Llamada , este paquete se encarga de establecer un camino lógico de nodo en nodo por donde irán uno a uno todos los paquetes de datos. De esta forma se establece un camino virtual para todo el grupo de paquetes. Este camino virtual será enumerado o nombrado inicialmente en el emisor y será el paquete inicial de petición de llamada el encargado de ir informando a cada uno de los nodos por los que pase de que más adelante irán llegando los paquetes de datos con ese nombre o número. De esta forma, el encaminamiento sólo se hace una vez (para la petición de llamada). El sistema es similar a la conmutación de circuitos, pero se permite a cada nodo mantener multitud de circuitos virtuales a la vez.

Las ventajas de los circuitos virtuales frente a los datagramas son:

- Las rutas en cada nodo sólo se hace una vez para todo el grupo de paquetes. Por lo que los paquetes llegan antes a su destino.
- Todos los paquetes llegan en el mismo orden del de partida ya que siguen el mismo camino.
- En cada nodo se realiza detección de errores, por lo que si un paquete llega erróneo a un nodo, este lo solicita otra vez al nodo anterior antes de seguir transmitiendo los siguientes.

Desventajas de los circuitos virtuales frente a los datagramas:

- En datagramas no hay que establecer llamada (para pocos paquetes, es más rápida la técnica de datagramas).
- Los datagramas son más flexibles, es decir que si hay congestión en la red una vez que ya ha partido algún paquete, los siguientes pueden tomar caminos diferentes (en circuitos virtuales, esto no es posible).
- El envío mediante datagramas es más seguro ya que si un nodo falla, sólo un paquetes se perderá (en circuitos virtuales se perderán todos).

### 1.6.- Interfaces de comunicaciones

En la realización de nuestro proyecto tenemos la necesidad de conectar equipos de comunicaciones, dicha necesidad nos llevó a crear un marco donde debemos conocer las recomendaciones o reglas de la transmisión de la señal a través de un enlace de comunicaciones; es en la interfaz donde se define un conjunto de cables y un tipo de enlace.

#### 1.6.1.- Características de la interfaz

Para que un par de equipos conectados de distintos fabricantes intercambien datos es necesario definir sus características y el estándar a utilizar. Las interfaces están incluidas en el nivel físico del modelo OSI, debido a que proporciona especificaciones eléctricas, mecánicas y de procedimiento para el medio de transmisión.

##### 1.6.1.1.- Mecánicas, eléctricas, funcionales y de procedimientos

La especificación o característica mecánica se define el tipo de cable a utilizar, longitud de los cables.

La especificación eléctrica se refiere a tipos de señales, niveles de voltajes, impedancias, frecuencias y codificaciones utilizadas.

La especificación funcional y de procedimiento define las asignaciones de cada señal del conector utilizado, además su modo de transmisión y los procedimientos para establecer una comunicación.

#### 1.6.1.2.- Transmisión de datos digitales seriales

En un sistema digital, las unidades básicas uno y cero pueden agruparse de n bits para ser transportadas, en la transmisión serial o en serie; estos bits son transportados por un mismo canal uno a uno entre dos dispositivos. Con cada pulso de reloj sólo se transmite un bit, esta puede ser de dos maneras sincrónica y asincrónica, en los equipos actuales debido a la necesidad de altas tasas de transmisiones de datos se utiliza la transmisión sincrónica y es en la que se hará referencia en esta parte del capítulo.

##### 1.6.1.2.1.- Transmisión serie sincrónica

En la transmisión sincrónica los datos fluyen continuamente por el mismo canal bits tras bits formando bytes y estos a su vez trama, lo que implica que el receptor tiene la tarea de separar cada en byte para reconstruir los datos.

Podemos observar en la **figura 1.4** como fluyen los bits en una transmisión sincrónica, en donde se vuelve importante la temporización.

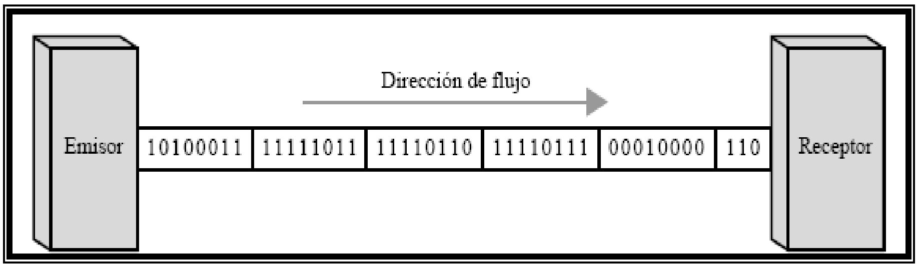



**Figura 1.4** Transmisión serie sincrónica[4]

#### 1.6.1.3.- Interfaz DTE-DCE

En un enlace de comunicaciones existen cuatro unidades básicas como lo muestra la **figura 1.5**: un DTE y un DCE de un extremo y un DCE y un DTE del otro extremo.

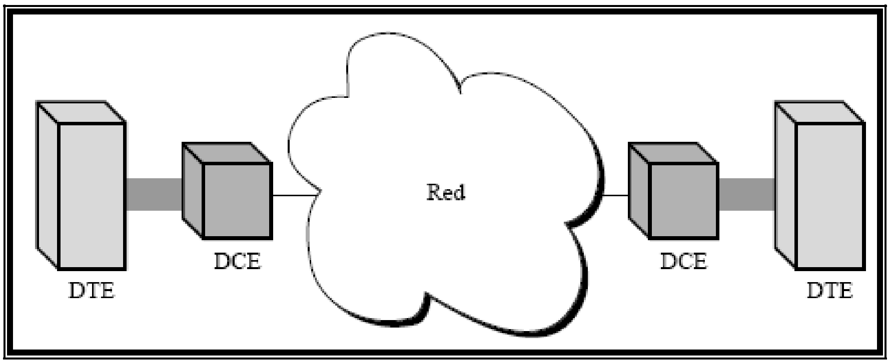



**Figura 1.5** DTE y DCE[5]

**DTE:** Un equipo DTE (Data Terminal Equipment) o ETD (Equipo Terminal de datos) es cualquier equipo informático, sea receptor o emisor final de datos.

---

[4] Figura tomada del Libro Transmisión de datos, Autor Forouzan, Edit McGrawHill

[5] Figura tomada del Libro Transmisión de datos, Autor Forouzan, Edit McGrawHill

El DTE es aquel componente del circuito de datos que hace de fuente o destino de la información. Puedes ser un computador como también un ruteador.

**DCE:** Un DCE (Data Circuit-Terminating Equipment) o ETCD (equipo terminal del circuito de datos) es todo dispositivo que participa en la comunicación entre dos dispositivos pero que no es receptor final ni emisor original de los datos que forman parte de esa comunicación. Un equipo DCE puede ser un MODEM ó un ruteador y un equipo DTE generalmente es un computador.

### 1.6.2.- Interfaz EIA-232

En telecomunicaciones la interfaz EIA-232 es un estándar de la Electronic Industries Alliance (EIA) para señales seriales de datos binarios que se utilizan en la conexión entre un DTE y un DCE, esta tiene su estándar similar en la Unión Internacional de Telecomunicaciones (ITU) la V.24.

Además al no definir codificación de caracteres (ASCII, EBCD), bits de inicio y de parada, velocidad, etc. Estas pueden ser configuradas antes de iniciar la transmisión, por lo que son muy utilizadas en configuración de equipos por terminal, pero muy poca utilizada para transmisión de datos.

Este estándar define las siguientes características:

Especificación mecánica: Se define como un cable de 25 hilos con un conector DB-25 macho y hembra respectivamente en los extremos con una longitud máxima de 15 metros. También existe otra implementación que utiliza un cable de 9 hilos con un conector DB-9.

Especificación eléctrica: La especificación eléctrica del estándar define los niveles de voltaje y el tipo de señal a transmitir en cualquier dirección entre el DTE y el DCE.

De los 25 hilos utilizados, no todos están implementados, cuatro son utilizados para funciones de datos y el resto están reservados para funciones de control, temporización y tierra.

La especificación eléctrica del EIA-232 define que las señales de datos deben enviarse usando uno negativo (-15 a -3 voltios) y otro positivo (+3 a +15 voltios). Además define que las señales distintas a las de datos deben enviarse usando OFF (menor que –3 voltios) y ON (mayor que +3 voltios).

Especificación funcional: Implementación DB-25. El EIA-232 define las funciones asignadas a cada uno de las 25 patillas del conector DB-25. La

Figura 1.6 muestra la orden y la funcionalidad de cada patilla de un conector macho.

Implementación DB-9. Muchas de las patillas de la implementación del DB-25 no son necesarias en una conexión asíncrona sencilla, este conector está mostrado en la **figura 1.6**. Por ello, se ha desarrollado una versión más sencilla del EIA-232 que solo usa 9 patillas, conocida como DB-9 y mostrada en la **Figura 1.7**. Observe que no hay una relación patilla a patilla entre ambas implementaciones.

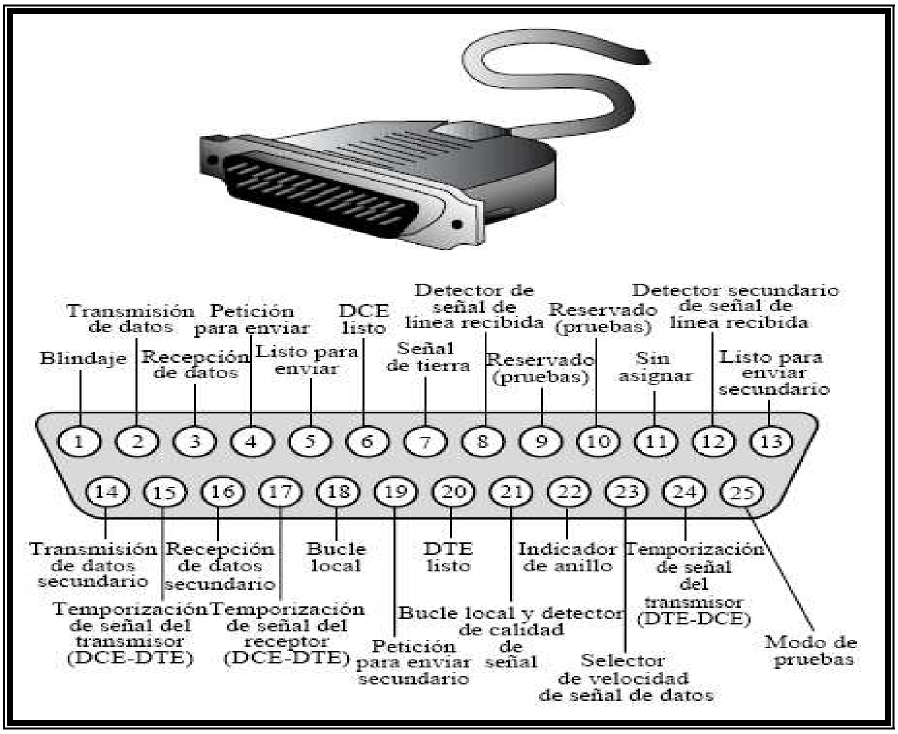



**Figura 1.6** Funciones de los pines en la versión DB-25[6]

[6] Figura tomada del Libro Transmisión de datos, Autor Forouzan, edit McGrawHill

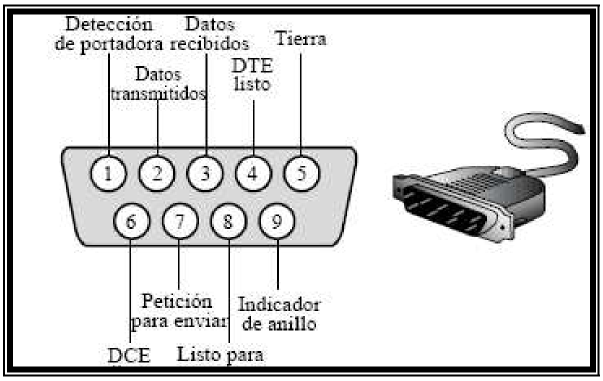



**Figura 1.7** Funciones de los pines en la versión DB-9[7]

A continuación se ajunta la **tabla 1.1** con la disposición de pines.

**Tabla 1.1** Disposición de pines EIA-232.

| Pin DB-25 | Pin DB- | Función |
|---|---|---|
| 1 | | Blindaje |
| 2 | 2 | Transmisión de datos |
| 3 | 3 | Recepción de datos |
| 4 | 7 | Petición para enviar |
| 5 | 8 | Listo para enviar |
| 6 | 6 | DCE listo |
| 7 | 5 | Señal tierra |
| 8 | 1 | Detector de señal de línea recibida |
| 9 | | Reservado |
| 10 | | Reservado |
| 11 | | Sin asignar |
| 12 | | Detector secundario de señal de línea recibida |
| 13 | | Listo para enviar secundario |
| 14 | | Transmisión de datos secundario |
| 15 | | Temporización de señal del transmisor(DCE-DTE) |
| 16 | | Recepción de datos secundario |
| 17 | | Temporización de señal del receptor(DCE-DTE) |
| 18 | | Bucle local |
| 19 | | Petición para enviar secundario |
| 20 | 4 | DTE listo |
| 21 | | Bucle local y detección de calidad de señal |
| 22 | 9 | Indicador de anillo |
| 23 | | Selector de velocidad de señal de datos |
| 24 | | Temporización de señal del transmisor(DTE-DCE) |
| 25 | | Modo de prueba |

[7] Figura tomada del Libro Transmisión de datos, Autor Forouzan, edit McGrawHill

### 1.6.3.- Interfaz V.35

V.35 es una norma originalmente desarrollada por el CCITT (ahora ITU) llamado “Transmisión de datos a 48 Kbit/s por medio de circuitos en grupo primario de 60 a 108 KHz.”

En 1989 ITU recomienda reemplazar la interfase por el estándar V.10/V.11, sin embargo ha sido usado por muchos años para velocidades desde 20 Kbps hasta más de 2 Mbps. A pesar de esto la interfaz V.35 sigue siendo muy popular en la interconexión de router y equipos que trabajan con estándares PRI/BRI y es completamente interoperable con la interfaz V.35/V.11.

V.35 es una norma de transmisión sincrónica de datos que especifica: tipo de conector, disposición de pines, niveles de tensión y de corriente.

Las señales usadas en V35 son una combinación de las especificaciones V.11 para temporizadores y data y V.28 para señales de control. Utiliza señales balanceadas, niveles de tensión diferencial; para transportar datos y temporizadores a alta velocidad.

Utiliza señales desbalanceadas, niveles de tensión referidos a masa; para la señalización, control y propósito general como RTS, CTS, DSR, DTR, estas señales tienen el mismo propósito que en EIA-232.

La velocidad varía entre 56 Kbps hasta 2 Mbps, dependiendo el equipamiento y los cables utilizados. Los valores típicos son 64 Kbps, 128 Kbps, 256 Kbps, generalmente en pasos de 64Kbps debido a la utilización de canales de E1. Típicamente se utiliza para transportar protocolos de nivel 2 como HDLC, Frame Relay, PPP, etc.

En la figura 1.8 se puede apreciar el conector que utiliza Winchester, también conocido como MRAC-34, pudiéndose también utilizar conector DB-15.

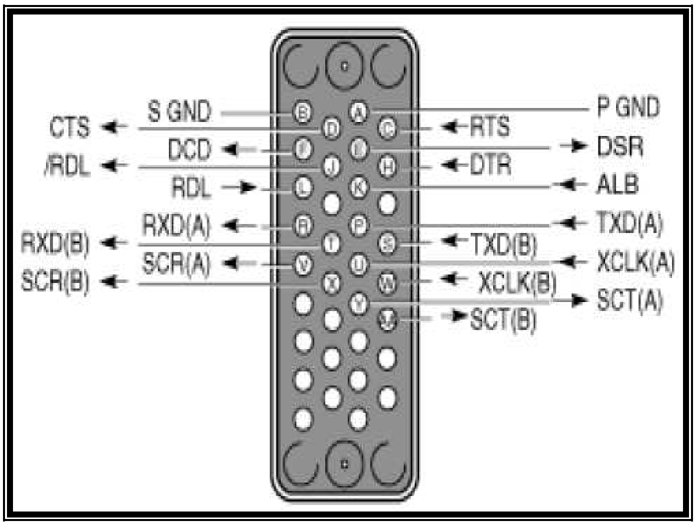



**Figura 1.8** Conector Winchester.

A continuación se adjunta la **tabla 1.2** con los pines en MRAC-34.

**Tabla 1.2** Disposición de pines V.35.

| Pin | Nombre | Descripción | Tipo |
|---|---|---|---|
| A | FG | Frame/Chassis Ground | - |
| B | SG | Signal Ground | - |
| P | SDA | Send Data A | Differential |
| S | SDB | Send Data B | Differential |
| R | RDA | Receive Data A | Differential |
| T | RDB | Receive Data B | Differential |
| C | RTS | Request To Send | Unbalanced |
| D | CTS | Clear To Send | Unbalanced |
| E | DSR | Data Set Ready | Unbalanced |
| H | DTR | Data Terminal Ready | Unbalanced |
| F | RLSD | Received Line Signal Detect | Unbalanced |
| U | TCEA | Transmit Clock Ext A | Differential |
| W | TCEB | Transmit Clock Ext B | Differential |
| Y | TCA | Transmit Clock A | Differential |
| AA | TCB | Transmit Clock B | Differential |
| V | RCA | Receive Clock A | Differential |
| X | RCB | Receive Clock B | Differential |
| J | LL | Local Loopback | Unbalanced |
| BB | RLB | Remote Loopback | Unbalanced |
| K | TM | Test Mode | Unbalanced |
| L | - | Test Pattern | Unbalanced |

El diseño de los cables depende de como se están conectando las interfaces envueltas. Usualmente, pero no siempre, la interfaz “facing away” desde la red es DCE y la interfaz "facing toward" hacia la red es DTE. El DCE normalmente da la señal de reloj. En la **figura 1.9** se muestra las distintas conexiones entre un DTE-DCE y un DTE-DTE.

| DTE - DCE | | | DTE - DTE | | |
|---|---|---|---|---|---|
| **DTE** | | **DCE** | **DTE** | | **DTE** |
| P | ------------------- | P | P | ------------------- | R |
| S | ------------------- | S | S | ------------------- | T |
| R | ------------------- | R | R | ------------------- | P |
| T | ------------------- | T | T | ------------------- | S |
| C | ------------------- | C | C | ------------------- | D |
| D | ------------------- | D | D | ------------------- | C |
| E | ------------------- | E | E | ------------------- | H |
| H | ------------------- | H | H | ------------------- | E |
| Y | ------------------- | Y | Y & U | ------------------- | V |
| AA | ------------------- | AA | W & AA | ------------------- | X |
| V | ------------------- | Y | V | ------------------- | Y & U |
| X | ------------------- | X | X | ------------------- | W & AA |

**Figura 1.9** Configuraciones DTE-DCE y DTE-DTE.

# CAPÍTULO 2

## 2. Protocolos de Comunicación

### 2.1.- Protocolos de capa 2

En este subcapítulo, cuatro diferentes protocolos serán revisados: MAC, HDLC, Frame Relay y ATM. Una definición de la función de la capa de enlace de datos (capa 2) es obtener servicio de la capa física (capa 1) para la transmisión de datos y maneja la notificación de error, la topología de la red, y el control de flujo.

#### 2.1.1.- MAC

El protocolo MAC (Control de acceso al medio), Pertenece al estándar Ethernet, es parte de la capa 2, este permite direccionamiento y mecanismos de control al canal de acceso que hace posible que varias host se puedan comunicar dentro de una red; típicamente una LAN (Área de red local) o MAN (Área de red metropolitana).

Ethernet es un método de acceso al medio que permite a todos los host de una red compartir el mismo medio. Ethernet es popular pues es muy escalable, por esto es fácil de integrar a nuevas tecnologías como Fast Ethernet dentro de la misma infraestructura.

#### 2.1.1.1.- Ethernet y el modelo OSI

El protocolo MAC pertenece al estándar Ethernet; Ethernet ocupa la capa física y la mitad inferior de la capa de enlace como muestra en la **figura 2.1**. La capa de enlace está dividida en dos subcapas: la capa MAC y la subcapa LLC, también llamado cliente MAC.

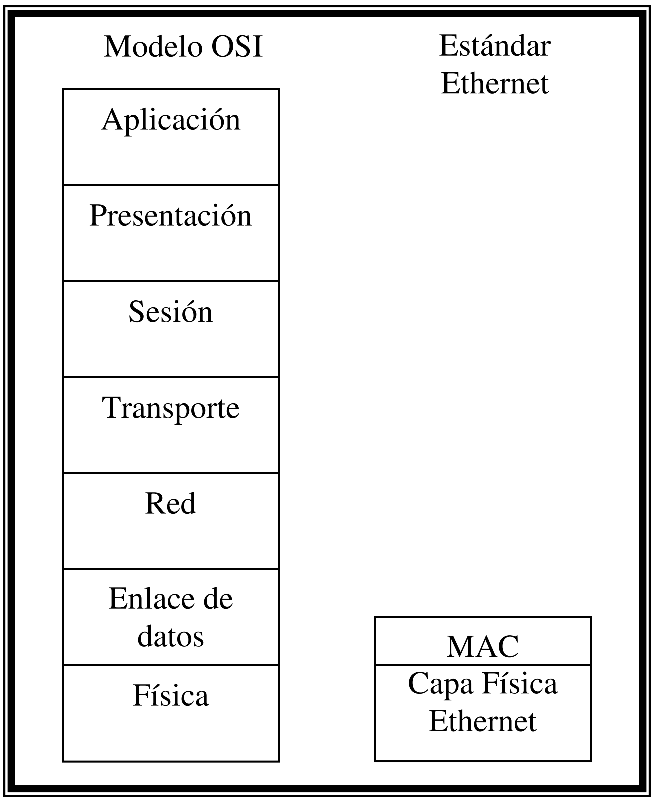



**Figura 2.1** Modelo OSI y Ethernet

Las funciones principales de la subcapa MAC es: encapsulación de los datos, incluyendo ensamblar la trama antes de la transmisión y detección de error durante y después de la recepción. Acceso de control al medio, incluyendo iniciación de la transmisión de la trama y recuperación de una transmisión no exitosa.

Se relaciona una gran variedad de tecnologías Ethernet físicas con la subcapa MAC, la cual es la misma para todas sin variantes como Fast Ethernet, Gigabit Ethernet, etc; por esto se dice que Ethernet es muy escalable.

#### 2.1.1.2.- Denominación

Para el direccionamiento en Ethernet se utiliza la dirección MAC o física del host; es decir cada host en la red tiene un identificador de 48 bits (6 bytes) escrito en formato hexadecimal como se muestra en la **figura 2.2**. Esta dirección es también llamada dirección unicast porque identifica a una NIC (Network Interface Card).

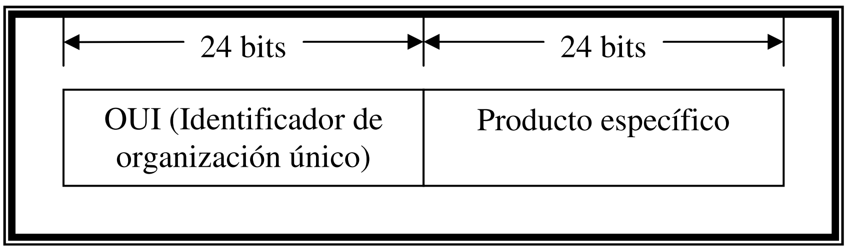



**Figura 2.2** Dirección MAC

El campo OUI (Identificador de organización único) es asignado por la IEEE a las empresas que manufacturan Ethernet NIC, este está compuesto por 3 bytes o 24 bits.

Los 24 bits menos significativos son asignados por la empresa a sus productos, estas son únicas por NIC.

El bit más significativo indica si la dirección es individual (0) o de grupo (1). Entonces para transmisiones broadcast la dirección es FF.FF.FF.FF.FF.FF, o simplemente todo 1.

### 2.1.1.3.- Estructura y campos de la trama Ethernet

La función de Ethernet es transmitir tramas entre host usando un formato MAC Data Frame, como muestra en la **figura 2.3**; este provee detección de error pero no corrección.

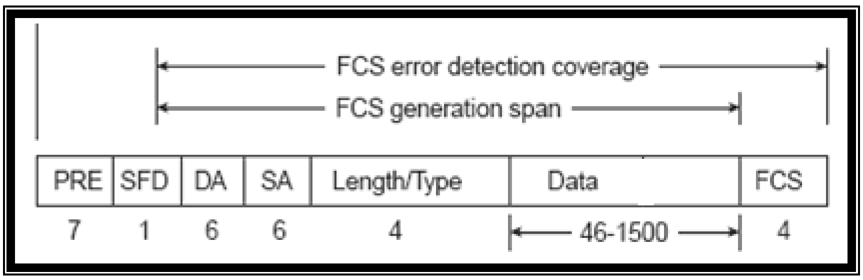



**Figura 2.3** Formato MAC data frame

**Preámbulo (P):** Consiste de 8 bytes, con bits alternados de 1 y 0 para sincronización.

**Delimitador de inicio de trama (SFD):** Es el último byte del campo Preámbulo y termina con dos 1 consecutivos, indicando que inicia el campo de dirección destino.

**Dirección destino (DA):** Consiste de 6 bytes y este campo se refiere a la dirección MAC del host destino.

**Dirección fuente (SA):** Consiste de 6 bytes y este campo se refiere a la dirección MAC del host fuente. Esta dirección siempre es una dirección unicast.

**Tipo/Longitud (T):** Consiste de 2 bytes, este campo se refiere al tipo de protocolo utilizado en la capa de red. Si el valor es menor a 0x600 este indica la longitud y el protocolo de capa de red utilizado se encuentra en el campo de datos de la subcapa LLC.

**Datos (D):** Consiste de n bytes, donde n es menor o igual a 1500 bytes. SI la longitud del campo es menor a 46 bytes, este debe ser rellenado con bytes hasta completar 46 bytes.

**Chequeo de secuencia de la trama (FCS):** Consiste de 4 bytes. Este contiene un valor CRC, que fue creado cuando se envió la trama y es chequeada cuando se recibió la trama. El FCS solo asegura que la trama está dañada pero no permite recuperación.

#### 2.1.1.4.- Reglas de MAC y detección de la colisión/postergación de la retransmisión

El protocolo CSMA/CD fue originalmente desarrollado para que 2 o más host compartieran el mismo medio. Cada host determina por sí mismo cuando está permitido enviar una trama.

Las reglas de acceso CSMA/CD están divididas por cada protocolo:

**Detección de portadora (CS):** Cada host escucha el tráfico en el medio para determinar cuando puede transmitir.

**Acceso múltiple (MA):** Host empiezan a transmitir cuando detectan que nadie está transmitiendo.

**Detección de colisión (CD):** Si varias host empiezan la transmisión al mismo tiempo, las tramas desde los host colisionarán el uno con el otro volviendo la trama irrecuperable. Si esto ocurre cada host debería detectar la colisión antes de que finalice la trama. Además cada host debería dejar de transmitir y esperar un periodo de tiempo para volver a intentarlo.

Recordar que en Ethernet Half-duplex comparte el mismo dominio colisión y provee una baja eficiencia que Ethernet full-duplex, el cual típicamente tiene dominio de colisión privados y alta eficiencia.

### 2.1.2.- HDLC

#### 2.1.2.1.- Introducción

HDLC (High-Level Data Link Control) es un protocolo de comunicaciones de datos punto a punto entre dos elementos basado en el ISO 3309. Proporciona recuperación de errores en caso de pérdida de paquetes de datos, fallos de secuencia y otros.

Este es un protocolo de propósito general, que opera a nivel de enlace de datos y ofrece una comunicación confiable entre el trasmisor y el receptor.
Es el protocolo más importante para el enlace de datos (IS0 3309, IS0 4335).

No solo porque es el más utilizado, sino porque además es la base para otros protocolos importantes de esta capa, en los que se usan formatos similares e iguales procedimientos a los que se usan en HDLC. Actualmente en los equipos Cisco se utiliza una versión simplificada de HDLC, llamada cHDLC en referencia a Cisco. En esta la parte de control no es utilizada.

### 2.1.2.2.- Cisco HDLC

Las tramas cisco HDLC se usan de una estructura alternativa del estándar ISO HDLC. Una de las principales razones de la creación de cHDLC es que el campo de dirección pueda soportar varios protocolos. Las tramas cHDLC es una trama HDLC con un código de tipo Ethernet que identifica que protocolo de red que está siendo encapsulado.

La estructura de la trama se muestra en la **figura 2.4.**

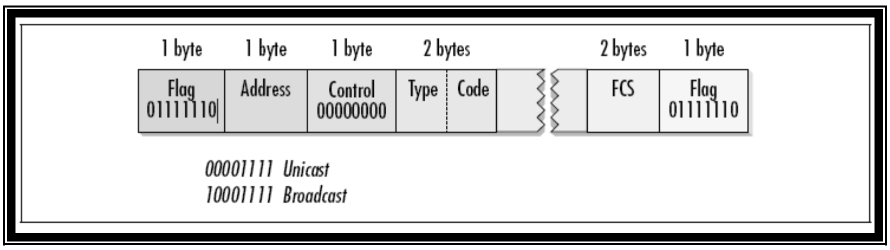



**Figura 2.4** Trama cHDLC[8]

[8] Figura tomada del Libro T1 A Survivor Guide, Autor Matthew Gast, Edit. O'reilly P.71

El direccionamiento en cHDLC es simple, puede ser una trama de broadcast (0x8F) o una trama unicast (0x0F); una trama broadcast es un reflejo de los protocolos de capas superiores designando una trama como broadcast.

El campo de control siempre está en cero, posteriormente tenemos los campos de tipo y código que es usualmente un tipo de código de protocolos de niveles superiores como se muestra en la **tabla 2.1**.

**Tabla 2.1** Código de protocolos cHDLC.

| **Protocolo** | **Código protocolos cHDLC(hexadecimal)** |
|---|---|
| IP 0x0800 | 0x0800 |
| Cisco SLARP (not RARP!) | 0x8035 |
| cisco Discovery | 0x2000 |

**2.1.2.3.- CiscoSLARP**

Las extensiones de cHDLC incluyen la definición de la línea serial del protocolo ARP (SLARP). Slarp es usado para proporcionar la asignación de dirección dinámica  entre dos puntos finales a través de una línea serial, utiliza un mecanismo Keep alive para garantizar la disponibilidad de un determinado enlace.

Los mecanismo Keep Alive trabajan en modo de request/responde entre dos puntos finales del enlace serial. Los números de secuencia transportada dentro de las tramas SLARP son incrementados por cada keep-alive enviado y los puntos finales son los encargados de determinar las pérdidas de tramas.

### 2.1.2.4.- Estructura de la Trama SLARP (Request/Response)

Una trama SLARP es designado por un valor específico en el campo de código de protocolos (0x8035) en una trama cHDLC. La estructura de la trama SLARP se encuentra detallada en la **tabla 2.2**.

Hay 3 tipos de tramas SLARP en el campo Op-code que son definidos:

- Address requests (0x00)
- Address replies (0x01)
- Tramas keep-alive (0x02)

**Tabla 2.2** Estructura de trama cHDLC SLARP.

| Address | Control | Protocol Code | SLARP Op-Code | Address | Mask | Reserved | FCS | Flag |
|---|---|---|---|---|---|---|---|---|
| 8 bits | 8 bits | 16 bits (0x8035) | 32 bits | 32 bits | 32 bits | 8 bits | 16 bits | 8 bits |

En el campo de Dirección y máscara contienen la dirección ip.

El campo reservado no es usado y siempre está seteado en 0xFF.

### 2.1.2.5.- Estructura de la trama Slarp Keep-alive

La mayoría de los protocolos de la capa de enlace de datos tiene un sistema de keep-alive, dado a que es muy eficiente y consume pocos recursos. A continuación en la tabla 2.3 se detalla la trama de cHDLC slarp keep-alive.

**Tabla 2.3** Estructura de trama cHDLC SLARP keep-alive.

| Address | Control | Protocol Code | SLARP Op-Code | Sequence Number (Sender) | Sequence Number (Last Received) | Reserved | FCS | Flag |
|---|---|---|---|---|---|---|---|---|
| 8 bits | 8 bits | 16 bits (0x8035) | 32 bits | 32 bits | 32 bits | 8 bits | 16 bits | 8 bits |

### 2.1.3.- FRAME RELAY

#### 2.1.3.1.- Introducción

Frame Relay es una tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y/o como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones, mediante la integración de tráfico de voz y datos.

Frame Relay fue desarrollada para hacer un mejor uso de la característica del ancho de banda compartido del modo trama, e incluso ahorrarse la desventaja de los largos retrasos en la red.

Frame Relay es una técnica orientada a la conexión, lo que significa que un circuito virtual debe estar configurado para que exista la comunicación. Frame Relay multiplexa estadísticamente paquetes o tramas hacia destinos diferentes con una sola interfaz.

### 2.1.3.2.- Diferencias entre Frame Relay y X.25

Frame Relay funciona de la misma manera que X.25 muchos usuarios comparten los recursos de red, y los datos se dividen en paquetes pequeños.

En la tabla 2.4 se proporciona una lista de las funciones suministradas por cada uno de los niveles OSI para X.25 y Frame Relay. Gran parte de las funciones de X.25 se eliminan en Frame Relay. La función de direccionamiento se desplaza desde la capa 3 en X .25 a la capa 2 en Frame Relay. Todas las demás funciones del nivel 3 de X.25 no están incorporadas en el protocolo de Frame Relay.

**Tabla 2.4** Diferencias entre FR y X.25

| X.25 | | Frame Relay |
|---|---|---|
| Establecimiento de circuito<br>Control de circuito<br>Control de flujo de circuito<br>Direccionamiento | Red | |
| Control de enlace<br>Creación de tramas<br>Control de errores | Enlace | Direccionamiento<br>Creación de tramas<br>Control de errores |

| | | |
|---|---|---|
| Control de flujo de enlaces<br><br>Fiabilidad | | Gestión de interfaces |
| Conexión Física | Físico | Conexión Física |

Así por lo tanto con X.25, utiliza la detección de errores y corrección de errores, en cada uno de los nodos a lo largo de la ruta, lo que provoca que la velocidad de transmisión se vea severamente limitada, mientras que en Frame relay se utiliza detección de errores y si este es detectado se descarta la trama y los protocolos de capa superior son los encargados de solicitar una retransmisión.

2.1.3.3.- **Topologías de conexión**

Las dos características más destacadas entre los usuarios de frame relay son:

- Ellos tienen una red que interconecta LANs usando routers para circuitos alquilados o de ancho de banda controlado y están buscando reducción de costos o el crecimiento de la red.
- Las redes están basadas en topología de estrella.

### 2.1.3.4.- Características técnicas

Es un servicio WAN de conmutación de paquetes, orientado a conexión.
Opera en la capa de enlace de datos del modelo de referencia OSI.
Usa un subconjunto de HDLC, el LAPF.
Las tramas transportan datos entre los dispositivos de usuarios DTE y el equipo de comunicaciones de datos DCE en la frontera de la WAN.
F.R especifica como opera el circuito local, pero no especifica de qué manera la trama atraviesa la nube WAN.

Se suele usar FR. para interconectar LANs, un ruteador en cada LAN será el DTE. Una conexión serial como una línea arrendada E1 conecta el router al switch FR. del proveedor en su punto de referencia más cercano al ruteador.
Las tramas se crean y se entregan desde un DTE a otro DTE, atravesando la red de FR creada por los DCE o switches del proveedor.

El FRAD o ruteador conectado a la red Frame Relay puede disponer de múltiples circuitos virtuales que lo conectan a diversos destinos. Esto hace que Frame Relay sea una alternativa muy económica a las de líneas de acceso dedicadas. Con esta configuración, todos los destinos comparten una sola línea de acceso y una sola interfaz. Se generan ahorros adicionales ya que la capacidad de la línea de acceso se establece según las necesidades de ancho de banda promedio de los circuitos virtuales, y no según las necesidades máximas de ancho de banda.

Los diversos circuitos virtuales en la línea de acceso única se diferencian mediante un identificador de canal de enlace de datos (DLCI) para cada circuito. El DLCI se almacena en el campo de dirección de cada trama transmitida. El DLCI en general tiene sólo importancia local y puede ser diferente en cada extremo de un circuito virtual (VC).

**Estructura y transmisión de tramas**

La red Frame Relay obtiene datos de los usuarios en las tramas recibidas, comprueba que sean válidas, y las enruta hacia el destino, indicado en el DLCI del campo "dirección". Si la red detecta errores en las tramas entrantes, o si el DLCI no es válido, la trama se descarta; ver figura 2.5.

| FLAG | DIRECION | INFORMACIÓN | FCS | FLAG |
|---|---|---|---|---|
| 1 byte | 2 byte | n byte | 2 byte | 1 byte |

**Figura 2.5** Estructura de la trama

El "flag" es la secuencia de comienzo y fin de trama. El campo de "dirección" contiene el DLCI y otros bits de congestión. Los datos de los usuarios se ingresan en el campo "Información", de longitud variable que permite transmitir un paquete entero de protocolos LAN. En este campo es donde están los datos del nivel superior, es decir, esta información se ingresa en la trama y; en recepción, se pasa directamente al nivel superior. Su longitud máxima no está normalizada, normalmente los operadores de redes FR la sitúan alrededor de 1500 bytes.

**FLAG**

Cada trama FR empieza y finaliza con un delimitador de carácter 7Eh. Esta secuencia de bit permite al receptor sincronizar la secuencia de inicio y fin de trama.

**Campo de Dirección**

Se llama campo de dirección a los bytes que siguen al Flag y que están por delante de los Datos de usuario. Puede tener varios formatos, pero normalmente suele tener 16 bits de longitud (2 octetos), como se muestra en la figura 2.6.

- **DLCI: (**Data Link Connection Identifier). Estos diez bits son el identificador de conexión de enlace de datos. Permite definir hasta 1024 circuitos virtuales, los DLCIs disponibles van desde el 16 al 1007 y con el DLCI se identifica al canal lógico al que pertenece cada trama, en general tiene solo importancia local y puede ser diferente en cada extremo de un camino virtual.

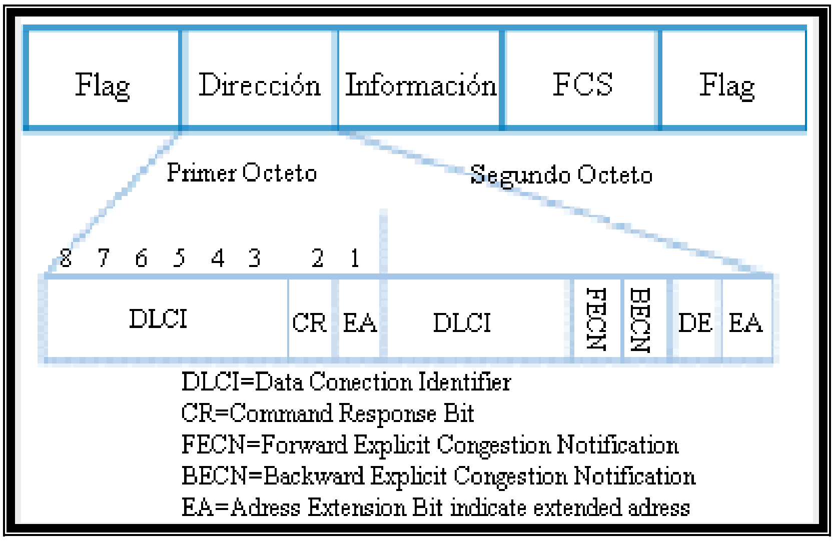



**Figura 2.6** Campo de Dirección[9]

- **E A:** (Extended Address). Campo de extensión de dirección. Puesto que se permiten más de dos octetos en el campo de control, este primer bit de cada octeto indica (cuando está marcado con un '0') si detrás siguen más octetos o bien (cuando está marcado con un '1') si se trata del último del campo de control.
- **C R:** Bit de Comando / Respuesta. No es un bit utilizado por la red. Se introduce por compatibilidad con protocolos anteriores, como los del tipo HDLC. Cuando el protocolo de enlace es fiable, utilizan este bit.
- **FECN** (Forward Explicit Congestion Notification), 1 bit de notificación de congestión de tráfico hacia el destino.

[9] Tomado de http://www.angelfire.com/sc/itiuax/formatos.html

- **BECN** (Backward Explicit Congestion Notification), 1 bit notificación de congestión en el retorno.
- **DE** (Discard Elegibility), bit que indica que la trama tiene baja prioridad y que es candidata de ser descartada.

**Campo de Información**

La figura 2.7 muestra el campo de información que puede contener datos de usuario o el mensaje de señalización, definido por el estándar Frame Relay.

La información de niveles superiores en el campo de usuario puede ser cualquier protocolo de alto nivel por ejemplo IP.

Todos los protocolos encapsularán sus paquetes dentro de una trama, adicionalmente las tramas contendrán información necesaria para identificar el protocolo transportado dentro de la unidad de datos del protocolo FR, para que permita al receptor procesar de forma apropiada el paquete entrante.

El primer octeto del campo de información de usuario de FR es el campo de control Q.922, para la transferencia de información sin confirmación, se usa el valor UI (0x03).

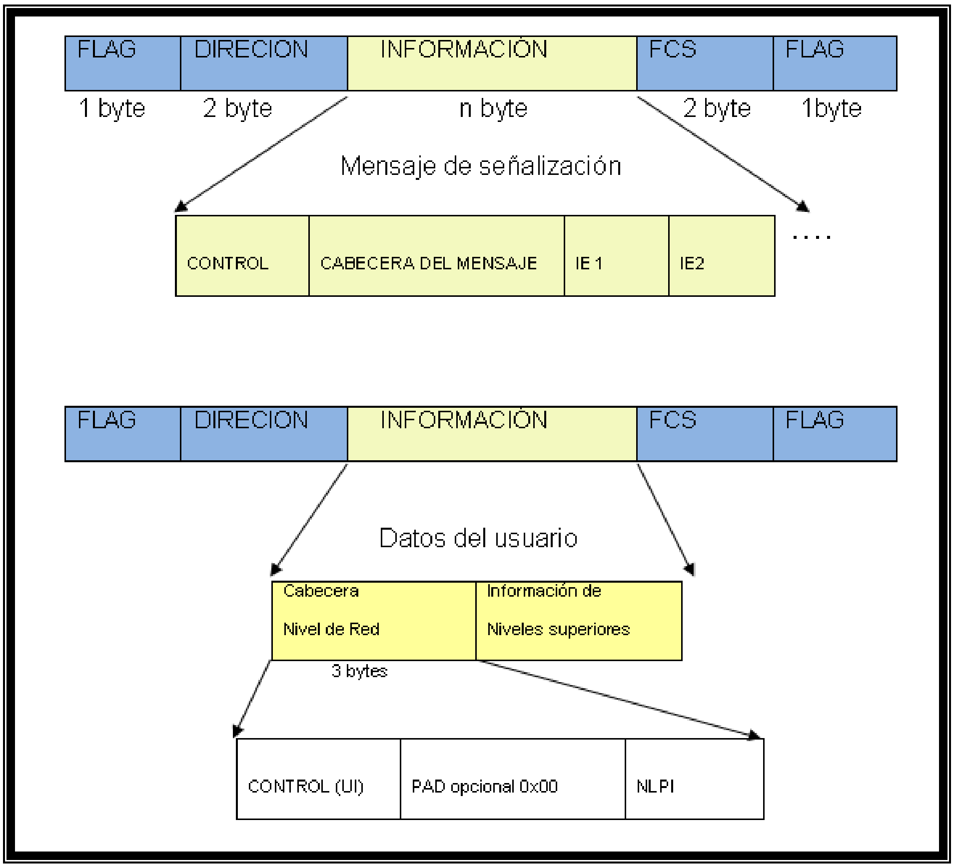



**Figura 2.7** Campo de información

El campo de relleno PAD se usa para alinear el resto de tramas hasta el límite de dos octetos. Pueden haber cero o un octeto de relleno dentro del campo de relleno y si existe el octeto de relleno debe de estar todo a ceros 0x00.

El campo de identificador de protocolo de nivel de red (NLPID) está administrado por la ISO y el UIT. Contiene valores para muchos protocolos diferentes. Este campo indica al receptor que encapsulación o cual es el protocolo que sigue a continuación, como se detalla en la siguiente tabla 2.5.

**Tabla 2.5** IP sobre frame relay

| 8 7 6 5 4 3 2 1 | Octeto |
|---|---|
| Dirección | 1 |
| (2 octetos) | 2 |
| Control 0x03 | 3 |
| NLPID 0xCC | 4 |
| Datagrama IP | 5 |
| ------ | |
| FCS | n-1 |
| | N |

El NLPID del protocolo de Internet (IP) está definido como 0xCC. Los datagramas IP enviados sobre la red FR seguirán a la encapsulación multiprotocolo. El campo NLPID indicará IP y el datagrama IP irá a continuación.

El campo FCS permite realizar comprobación de errores en la cabecera y los detecta pero no corregirlos.

**Parámetros de dimensionamiento (CIR, Bc, Be)**

**CIR:** (Committed Information Rate, o tasa de información comprometida). Tasa a la cual la red se compromete, en condiciones normales de operación, a aceptar datos desde el usuario y transmitirlos hasta el destino. Puede ser distinto en cada sentido. Son las tramas 1 y 2 de la figura 2.8.

Las CIR individuales son por lo general menores a la velocidad del puerto. Sin embargo, la suma de las CIR, en general, será mayor que la velocidad del puerto. Algunas veces, este factor es de 2 o 3. La multiplexión estadística aprovecha el hecho de que las comunicaciones en computación son usualmente por ráfagas, lo que hace improbable que los diversos canales estén a su máxima velocidad de transmisión de datos al mismo tiempo.

**Bc:** (Committed Burst Size o ráfaga comprometida). Es la cantidad de bits transmitidos en el periodo T a la tasa CIR (CIR=Bc/T). En las redes Frame Relay se permite al usuario enviar picos de tráfico a la red por encima de CIR, durante intervalos de tiempo muy pequeño, incluido en el periodo T.

**Be:** (Excess Burst Size, o ráfaga en exceso): es la cantidad de bits transmitidos en el periodo T por encima de la tasa CIR. Si la red tiene capacidad libre suficiente admitirá la entrada de este tipo de tráfico en exceso (trama 3 de la figura 2.8), marcándolo con DE activo.

El tráfico entrante en la red, por encima de Bc + Be, es el descartado directamente en el nodo de entrada, (trama 4).

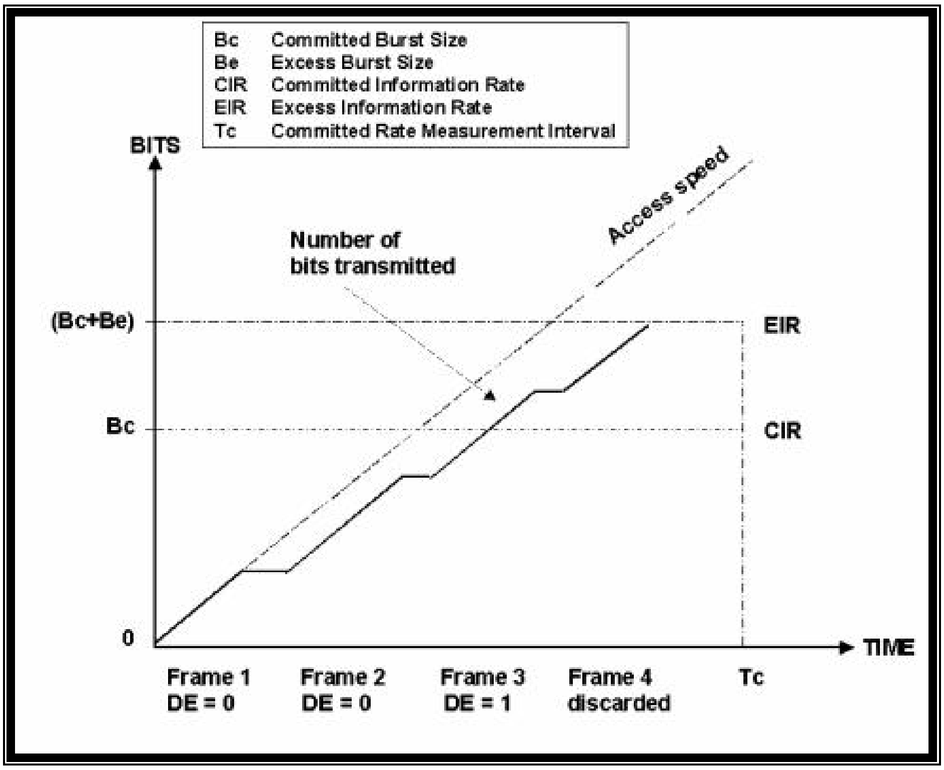



**Figura 2.8** Parámetros de frame relay[10]

**Interfaz de Gestión Local (LMI)**

Cuando un ruteador que está conectado a una red Frame Relay inicia, envía un mensaje de consulta de estado LMI a la red. La red contesta con un mensaje de estado LMI que contiene detalles de cada PVC configurado en el enlace de acceso.

Periódicamente el ruteador repite la consulta de estado, pero las respuestas siguientes sólo incluyen los cambios en el estado. Después de un

[10] Tomado de http://es.wikipedia.org/wiki/Frame_Relay

determinado número de respuestas abreviadas, la red enviará un mensaje de estado completo.

Esta interfaz notifica al dispositivo final información sobre el estado de los DLCIs de la red. Indica al usuario si un DLCI está activo, presente, ausente o si falla.

El protocolo LMI activa un proceso de chequeo periódico cada 10 segundos, en el cual el dispositivo de acceso Frame Relay (FRAD) de forma periódica realiza una actualización de estado hacia la nube Frame Relay, usando los mensajes "status enquiry".

Los mensajes LMI se intercambian entre los DTE y los DCE utilizando los DLCI reservados.

Hay tres tipos de LMI que se detallan en la siguiente tabla 2.6.

**Tabla 2.6** Tipos de LMI

| **Tipo LMI** | **Documento** | **Parámetros Cisco IOS Lmi-Type** | **Rango DLCI permitidos** | **DLCI LMI** |
|---|---|---|---|---|
| Cisco | Propietario | Cisco | 16-1007(992) | 1023 |
| ANSI | T1.617 Annex D | Ansi | 16-991(976) | 0 |
| ITU | Q.933 Annex A | Q933a | 16-991(976) | 0 |

Los mensajes LMI se envían a través de una variante de las tramas LAPF.

El protocolo LMI activa un proceso de chequeo periódico como en la figura 2.9, en el cual el FRAD de forma periódica realiza un polling hacia la red usando los mensajes Status enquiry. El mensaje contiene dos elementos de información: tipo de informe y la secuencia Keep alive

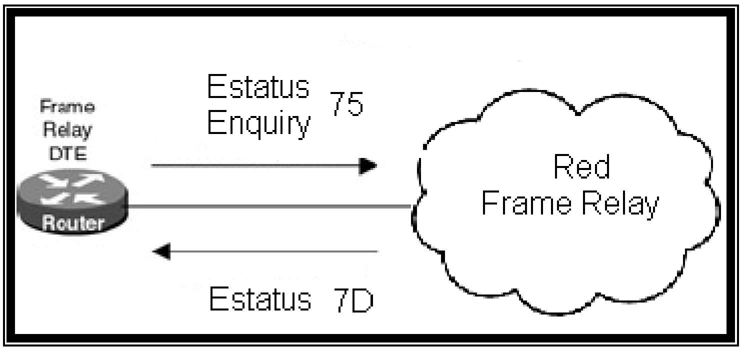



**Figura 2.9** Intercambio de mensajes del estado del enlace.

La red contesta al FRAD con un mensaje de estado. El mensaje de estado contiene elementos de información sobre el estado de los PVC´s. Cuando se pide un mensaje de estado completo habrá un elemento de información en la trama por cada PVC configurado en la red.

**Etapas del ARP inverso y operación de los LMI**

Los mensajes de estado LMI combinados con los mensajes del ARP inverso permiten que un ruteador vincule direcciones de capa de red con direcciones de la capa de enlace de datos.

Si el ruteador necesita asignar los VC a direcciones de capa de red, enviará un mensaje ARP inverso desde cada VC. El mensaje ARP inverso incluye la dirección de capa de red del ruteador, de modo que el DTE o el ruteador remoto, pueda realizar la vinculación. La respuesta ARP inversa permite que el router haga los registros necesarios en su tabla de asignaciones de direcciones a DLCIs. Si el enlace soporta varios protocolos de capa de red, se enviarán mensajes ARP inversos para cada uno de ellos

**2.1.3.5.- Ventajas**

Alta velocidad y bajo retardo.

Soporte eficiente para tráficos a ráfagas.

Flexibilidad.

Eficiencia.

Buena relación coste-prestaciones.

Transporte integrado de distintos protocolos de voz y datos.

Conectividad "todos con todos".

Simplicidad en la gestión.

Interfaces estándares.

### 2.1.3.6.- Aplicaciones

Intercambio de información en tiempo real, dentro del ámbito empresarial.

Correo electrónico.

Transferencia de ficheros e imágenes.

Impresión remota.

Aplicaciones host-Terminal.

Aplicaciones cliente-servidor.

Acceso remoto a bases de datos.

Construcción de bases de datos distribuidas.

### 2.1.4.- Protocolo ATM

#### 2.1.4.1 Introducción

Asynchronous Transfer Mode (ATM) es una tecnología de conmutación basada en unidades de datos de un tamaño fijo de 53 bytes llamadas celdas. ATM opera en modo orientado a la conexión, esto significa que cuando dos nodos desean transferir deben primero establecer un canal o conexión por medio de un protocolo de llamado o señalización. Una vez establecida la conexión, las celdas de ATM incluyen información que permite identificar la conexión a la cual pertenecen.

En una red ATM las comunicaciones se establecen a través de un conjunto de dispositivos intermedios llamados switches.

Transmisiones de diferentes tipos, incluyendo video, voz y datos pueden ser mezcladas en una transmisión ATM que puede tener rangos de 155 Mbps a 2.5Gbps. Esta velocidad puede ser dirigida a un usuario, grupo de trabajo o una red entera, porque ATM no reserva posiciones específicas en una celda para tipos específicos de información. Su ancho de banda puede ser optimizado identificando el ancho de banda bajo demanda. Conmutar las celdas de tamaño fijo significa incorporar algoritmos en chips eliminando retrasos causados por software. Una ventaja de ATM es que es escalable. Varios switches pueden ser conectados en cascada para formar redes más grandes.

#### 2.1.4.1.1.- Modelo de referencia ATM

ATM lleva a cabo la transferencia de datos en paquetes segmentados discretos, permitiendo la multiplexación de varias conexiones lógicas sobre una única interfaz física.

Estas unidades discretas que componen una interfaz lógica son paquetes de tamaño fijo, denominadas celdas.

Dos de los factores que hacen de ATM una tecnología de alta velocidad son:

- ATM es un protocolo con mínima capacidad de control de errores y de flujo, lo que reduce el tamaño y el coste de procesamiento de las celdas.
- El empleo de celdas de tamaño fijo simplifica el procesamiento necesario en cada nodo.

La **figura 2.10** muestra el modelo de referencia del protocolo ATM:

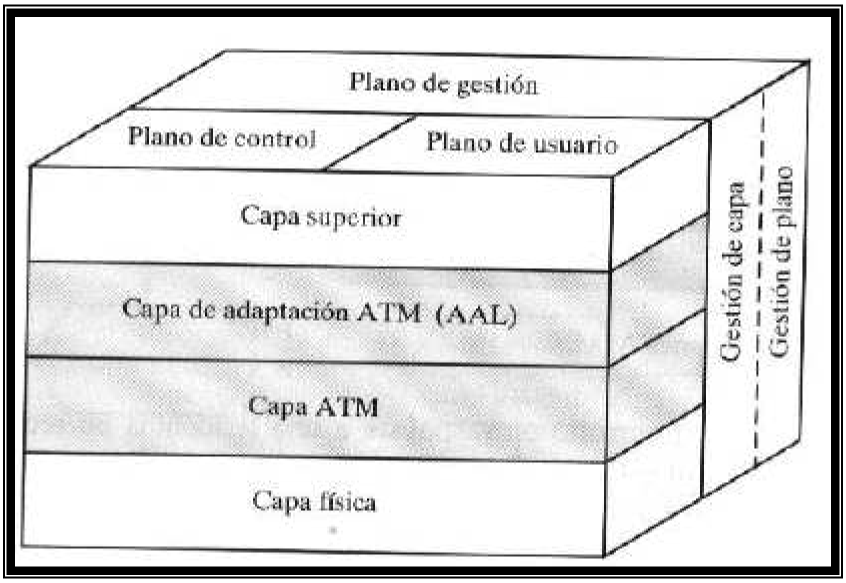



**Figura 2.10** Modelo de referencia del Protocolo ATM[11]

*La capa física:*

La primera capa llamada capa física (Physical Layer), define las interfaces físicas con los medios de transmisión y el protocolo de trama para la red ATM es responsable de la correcta transmisión y recepción de los bits en el medio físico apropiado. Es independiente de los medios físicos.

Tiene dos subcapas

- TC (Transmission Convergence Sublayer)
- PM (Physical Medium Sublayer)

[11] Tomado de libro: Tecnologías y redes de transmisión de datos Autor: Enrique Herrera

*La capa ATM:*

Provee un solo mecanismo de transporte para múltiples opciones de servicio. Es independiente del tipo de información que es transmitida (datos, voz, video) con excepción del tipo de servicio (QOS) requerido.

Existen dos tipos de cabeceras ATM.

- UNI (User-Network Interface)
- NNI (Network-Network Interface)

*La capa de adaptación ATM:*

Provee las funciones orientadas al usuario no comprendidas en la Capa ATM.

Permite a la Capa ATM transportar diferentes protocolos y servicios de capas superiores.

Tiene dos subcapas:

- CS (Convergence Sublayer)
- SAR (Segmentation and Reassembly Sublayer)

Las capas superiores:

Las capas superiores en el modelo de referencia dependen de cada aplicación específica que utilice las capas inferiores del protocolo ATM para el transporte de información por la red. Para facilitar la estandarización de las capas del modelo de referencia ATM, se distingue sólo entre cuatro clases de aplicaciones de las capas superiores:

1. Clase A
2. Clase B
3. Clase C
4. Clase D

### 2.1.4.2 Conexiones lógicas en ATM

Las conexiones lógicas en ATM están relacionadas con las conexiones de canales virtuales (VCC), ver **figura 2.11**. Una VCC es como un circuito virtual en X.25 o como una conexión de enlace de datos en retransmisión de tramas, siendo la unidad básica de conmutación en la red ATM. Una VCC se establece entre dos usuarios finales a través de la red, proporcionando un flujo full-duplex de celdas del mismo tamaño a una velocidad determinada.

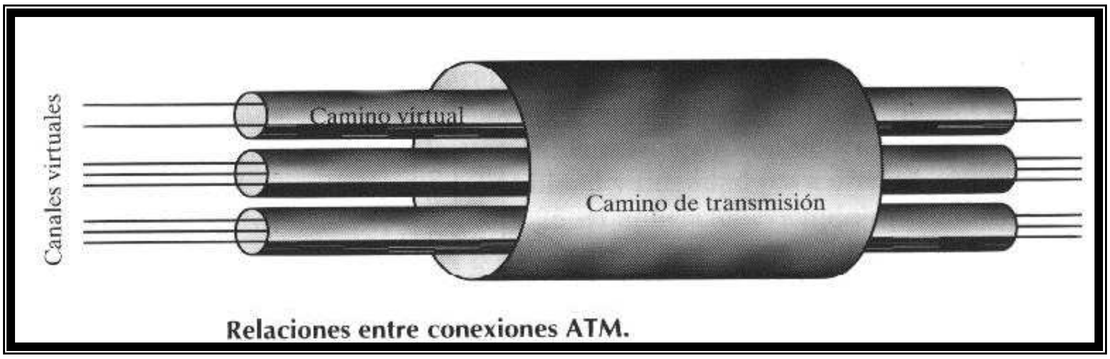



**Figura 2.11** Relaciones entre conexiones ATM[12]

Una conexión de camino virtual (VPC) es un haz de VCC con los mismos extremos, tal que las celdas que fluyen en las VCC de una misma VPC se conmutan conjuntamente. Los caminos virtuales sirven para simplificar y facilitar el control de la red agrupando en una sola unidad a conexiones que comparten el mismo camino a través de la red.

### 2.1.4.3.- Celdas ATM

Las celdas en ATM son de tamaño fijo, con 5 bytes de cabecera y 48 bytes de información (53 bytes por celda). El empleo de este tipo de celdas, pequeñas y de tamaño fijo se debe a:

- El uso de celdas pequeñas puede reducir el retardo de cola para celdas de alta prioridad.

[12] Tomado de libro: Tecnologías y redes de transmisión de datos Autor: Enrique Herrera

- Las celdas de tamaño pequeño pueden ser conmutadas más eficientemente.

- La implementación física de los sistemas de conmutación es más sencilla para celdas de tamaño fijo.

**Formato de cabecera**

En la **figura 2.12**, la de la izquierda muestra el formato de cabecera en el interfaz usuario-red. La figura de la derecha muestra el formato de cabecera en el interfaz red-red, en el cual no se especifica el campo *control de flujo genérico* (GFC), ampliando en su lugar el campo *identificador de camino virtual* (VPI) de 8 a 12 caracteres, lo que permite un gran número de VPC internos de la red, para dar cabida a los de los usuarios y a los internos de la red.

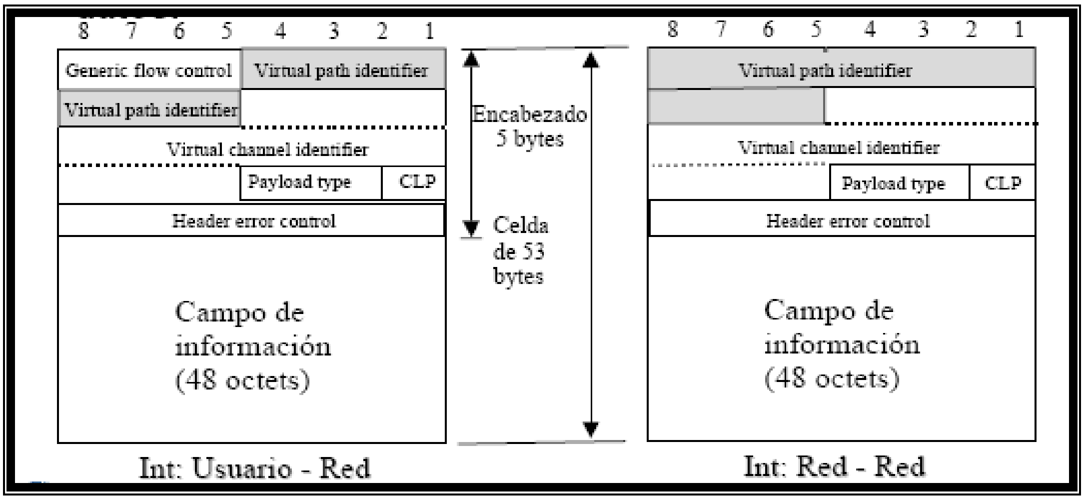



**Figura 2.12** Formato de cabecera

El campo de control de flujo genérico (GFC) sólo tiene sentido en la interfaz local usuario-red, y podría utilizarse para ayudar al usuario en el control de flujo del tráfico para las distintas calidades de servicio.

Los campos de identificador de camino virtual (VPI) e identificador de canal virtual (VCI) contienen entradas a la tabla de ruteo del siguiente conmutador de caminos virtuales o canales virtuales que visitará la celda. Cabe destacar que el protocolo ATM siempre suministra a las capas superiores las celdas en orden de secuencia correcto.

El campo tipo de carga útil (Payload type) indica el tipo de información contenida en el campo de información.

La prioridad de pérdida de celdas (CLP) se emplea para orientar a la red en caso de congestión:

- Un bit 0 indica que la celda es de prioridad superior y que no debe descartarse.
- Un bit 1 indica que la celda es de prioridad baja y que puede descartarse en caso de ser necesario.

El campo de HEC (Header Error Control) contiene un código redundante cíclico (CRC) que permite detectar y corregir errores en el encabezado de la celda ATM.

#### 2.1.4.4.- Señalización en ATM

En ATM es necesario un mecanismo para establecer y liberar las VPC y VCC, de modo que llamamos señalización de control a la información involucrada en ese proceso, la cual se transmite a través de conexiones distintas de las gestionadas.

Los distintos modos de establecer/liberar VCC son:

1. Las VCC semipermanentes pueden usarse en el tráfico usuario-usuario, para lo cual no es necesaria la señalización de control.

2. Si no existe un canal de señalización de control, será necesario establecer uno. Para ello, se intercambiará una serie de señales de control entre usuario y red a través de un canal específico. Por ello, es necesario un canal permanente que pueda ser usado para establecer las VCC para el control de llamadas. Este canal permanente se llama canal de meta-señalización, dado que se emplea para establecer canales de señalización.

3. El canal de meta-señalización sirve para establecer canales virtuales de señalización usuario-red, el cual se utilizará para establecer las VCC de transmisión de datos.

4. El canal de meta-señalización también permite establecer un canal virtual de señalización usuario-usuario, el cual se utilizará para que dos usuarios finales establezcan y liberen VCC para el transporte de datos, sin intervención de la red.

**Métodos para establecer/liberar VPC:**

1.-Una VPC semipermanente se puede establecer mediante negociación previa, para lo cual no son necesarias señales de control.

2.-El usuario puede establecer/liberar una VPC haciendo uso de la VCC de señalización.

3.-La propia red puede establecer y liberar VPC, en cuyo caso las VPC podrán estar destinadas al tráfico red-red, usuario-red ó usuario-usuario.

### 2.1.4.5.- Transmisión de celdas ATM

BISDN especifíca que las celdas deben transmitirse a 155,52 ó 622,08 Mbps, y será necesario especificar la estructura de transmisión usada para transportar esta carga.

En el caso de la interfaz a 155,52 Mbps se han definido dos aproximaciones: capa física basada en celdas y capa física basada en SDH.

<u>Capa física basada en celdas</u>

La estructura de la interfaz se basa en una secuencia continúa de celdas de 53 bytes, sin fragmentación. Dado que no se imponen tramas externas, para sincronizar se utiliza el campo "control de errores de cabecera" de la cabecera.

<u>Capa física basada en SDH</u>

Alternativamente, las celdas ATM pueden transmitirse a través de una línea haciendo uso de SDH (jerarquía digital síncrona) o SONET. En este caso, en la **figura 2.13**, en la capa física se impone la fragmentación utilizando tramas STM-1.

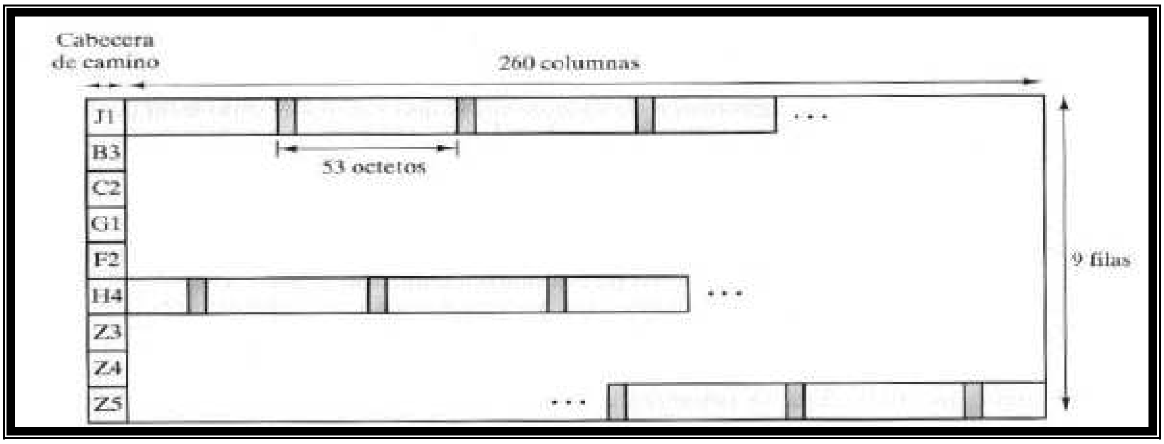



**Figura 2.13** Carga útil STM-1 para transmisión de celdas ATM basada en SDH

La capacidad de carga útil de las tramas STM-1 es de 2430 bytes. La carga útil consta de 9 bytes suplementarios de cabecera del camino y de las propias celdas ATM.

SONET (Synchronous Optical Network, Red Optica Síncrona) y SDH (Synchronous Digital Hierarchy, Jerarquía Digital Síncrona) en terminología UIT-T, es un estándar internacional (ver **tabla 2.7**), desarrollado por el Working Group T1X1 de ANSI para líneas de telecomunicación de alta velocidad sobre fibra óptica (desde 51,84 Mbps a 2,488 Gbps). SONET es su nombre en EE.UU. y SDH es su nombre europeo. Son normas que definen señales ópticas estandarizadas, una estructura de trama síncrona para el tráfico digital multiplexado, y los procedimientos de operación para permitir la interconexión de terminales mediante fibras ópticas, especificando para ello el tipo monomodo.

**Tabla 2.7** Jerarquía digital síncrona

| SONET | SDH | TASA |
|---|---|---|
| STS -1 | STM – 0 | 51,840 Mbps |
| STS - 3 | STM – 1 | 155,520 Mbps |
| STS - 9 | STM – 3 | 466,560 Mbps |
| STS -12 | STM – 4 | 622,080 Mbps |
| STS - 18 | STM – 6 | 933,120 Mbps |
| STS - 24 | STM – 8 | 1.244,160 Mbps |
| STS - 48 | STM – 16 | 2.488,379 Mbps |

### 2.1.4.6.- Funciones de las capas del modelo de referencia ATM

Como mencionamos anteriormente el protocolo ATM está constituido por 4 capas que son:

La capa física, la capa ATM, la capa de adaptación ATM y las capas superiores como se muestra en la **figura 2.14**. En éste subcapítulo explicaremos con más detalle las funciones que realizan cada una de ellas.

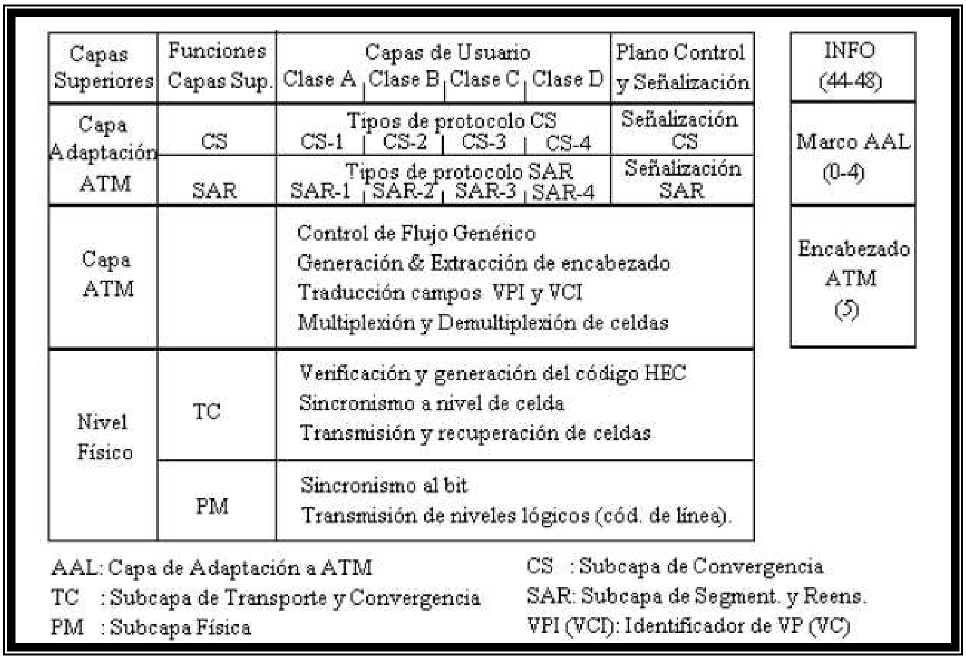



**Figura 2.14** Capas de ATM[13]

### *Capa física o nivel físico*

La capa física está dividida en la subcapa de medio físico (PM) y la subcapa de transmisión y convergencia (TC). La subcapa TC identifica cada celda dentro del flujo de bits o bytes que recibe de la capa PM, y está encargada del transporte y sincronismo de cada celda. Las celdas provenientes del plano de operación, administración y mantenimiento son insertadas en el flujo de información en esta subcapa. Esta subcapa está encargada también de realizar el chequeo de errores en el encabezado de las celdas ATM.

[13] Tomado de http://profesores.elo.utfsm.cl/~walter/varios/Atm.pdf

La subcapa PM está encargada de establecer el acceso físico al medio y suministrar un servicio de transporte para un flujo continuo de bits. Las funciones principales en esta capa son el envío de bits en un código de línea adecuado y sincronismo al bit.

***Capa de adaptación ATM***

El uso de ATM hace necesaria de una capa de adaptación para admitir protocolos de transferencia de información no basado en ATM. En un entorno heterogéneo en el que existen redes ATM interconectadas con redes de transmisión de tramas, una forma adecuada de integrar los dos tipos de redes es realizar una transformación entre tramas y celdas, lo que implica la segmentación de una trama en celdas de transmisión y la agrupación de las celdas en tramas en el receptor.

Esta capa se divide en subcapas, cuyas funciones se describen a continuación:

1. Subcapa de segmentación y reensamblaje (SAR). Segmenta los mensajes de longitud variable de las capas superiores en bloques de tamaño apropiado para ser transportados en el campo de información de una celda ATM, esto 48 bytes. De igual forma, esta capa vuelve a reconstruir los mensajes a su tamaño original en el extremo receptor.

A cada fragmento de mensaje resultante se le agrega un encabezado y cola con información de control de este nivel. Solamente las celdas correspondientes al mismo mensaje están garantizadas de seguir la misma ruta.

2. Subcapa de Convergencia (CS). Las funciones asociadas a este nivel son por ejemplo detección y recuperación de celdas perdidas, recuperación del sincronismo a nivel de mensaje, ecualización del retardo variable incurrido por las celdas, etc. Cada mensaje del nivel de convergencia va precedido de un encabezado y se le agrega información de término de mensaje apropiada.

***Capas superiores***

Clase A: Emulación de Circuitos. Esto corresponde a establecer un enlace con flujo continuo de bits entre el transmisor y el receptor. La variación del tiempo entre arribos de información en paquetes es compensada con un buffer de llegada, y la pérdida de información tiene que ser reducida al mínimo. Deben sincronizarse asimismo los relojes de los extremos entre los que se envía la información.

Clase B: Servicios con tasa de transmisión de bits variable, con sincronismo entre el transmisor y el receptor. Los servicios de voz, video y sonido de tasa de transmisión variable son un ejemplo de estos servicios, en que se aprovecha la multiplexión estadística que ofrece ATM.

Clase C: Servicios de transmisión de datos con establecimiento de conexión. Este servicio puede establecerse con o sin la garantía de una transmisión libre de errores, así como también con mensajes de largo fijo o variable (la capa ATM transporta un fragmento de tamaño fijo de mensaje en cada celda). Por ejemplo, se suele establecer una conexión (o sesión) entre dos computadores cuando la cantidad de datos que se requiere intercambiar en forma interactiva es grande.

Clase D: Servicio de transmisión de datos sin establecimiento de conexión. Los mensajes de esta clase de servicio son enrutados en forma independiente a través de la red ATM usando direcciones explícitas del destino. Los servicios de correo electrónico y aplicaciones de tipo cliente-servidor son típicamente de esta clase.

### 2.1.4.6.1.- Protocolos AAL

Con el fin de minimizar el número de protocolos AAL diferentes que pueden ser especificados, se han definido cuatro clases de servicios que cumplen un amplio rango de requisitos:

Existe un tipo de protocolo para cada clase de servicio por lo tanto hay cuatro tipos que han sido definidos tipos 1, 2, 3/4 y 5 como se muestra en la **figura 2.15**.

| | CLASE A | CLASE B | CLASE C | CLASE D |
|---|---|---|---|---|
| Sincronización origen-destino | Requerido | | No Requerido | |
| Tasa de bits | Constante | Variable | | |
| Modo de conexión | Orientado a conexión | | | Sin conexión |
| Protocolo AAL | Tipo 1 | Tipo 2 | Tipo 3,4,5 | Tipo 3,4 |

**Figura 2.15** Clases de servicios en ATM

Tipo 1: Emulación de circuitos.

Tipo 2: Video, con tasa de transmisión variable.

Tipo 3,4 y 5: Transmisión de datos.

Cada tipo de protocolo consiste de dos subcapas: CS y SAR.

**AAL Tipo 1**

Aquí la subcapa SAR antes de transmitir organiza los bits en celdas; en recepción recupera los bits de las celdas.

Cada celda consiste de:

• Un número de secuencia para poder detectar pérdidas de información (SN).

• Un campo de protección del número de secuencia (SNP) para poder detectar errores y corregirlos; como se puede ver en la **figura 2.16**.

La subcapa CS es para temporización y sincronización.

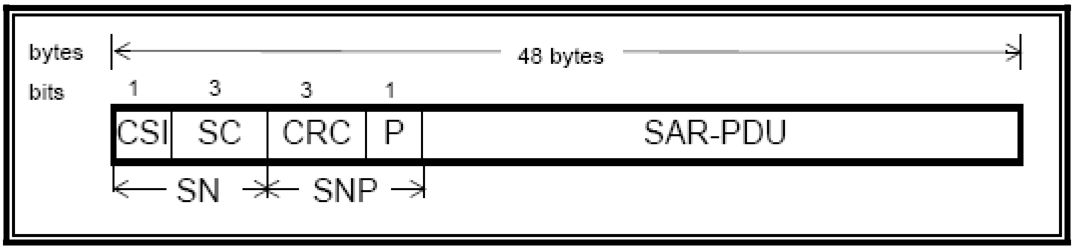



**Figura 2.16** PDU SAR-AAL1[14]

**AAL Tipo 2**

- Transferencia de unidades de datos de servicio (SDUs) a tasa de transmisión variable (VBR).
- Transferencia de información de temporización entre el transmisor y el receptor.
- No ofrece la posibilidad de detectar errores o pérdidas de información.

[14] Tomado de http://www.trendtest.com

**AAL Tipos 3/4**

El servicio puede ser con o sin conexión.

El servicio puede ser proporcionado en modo mensaje o en modo stream (secuencia continua)

- Modo mensaje: un protocolo de línea puede ser usado.
- Modo stream: transferencia de información a baja velocidad de manera continua pero con un tiempo corto de respuesta.

**AAL Tipo 5**

Mínimo “overhead” en procesamiento.

Mínimo “overhead” durante la transmisión.

Promete la interconexión con protocolos de transporte ya existentes.

Dentro del PDU de esta capa se tienen varios campos detallados a continuación y mostrados en la **figura 2.17**:

- Pad: La subcapa de convergencia agrega rellena con ceros para que el PDU sea múltiplo de 48bytes.
- Los campos UU y CPI actualmente no son usados y se llenan de ceros.
- LI: Este campo indica la longitud de los datos de usuario.

- CRC: Este campo provee chequeo de errores al PDU de la subcapa de convergencia.

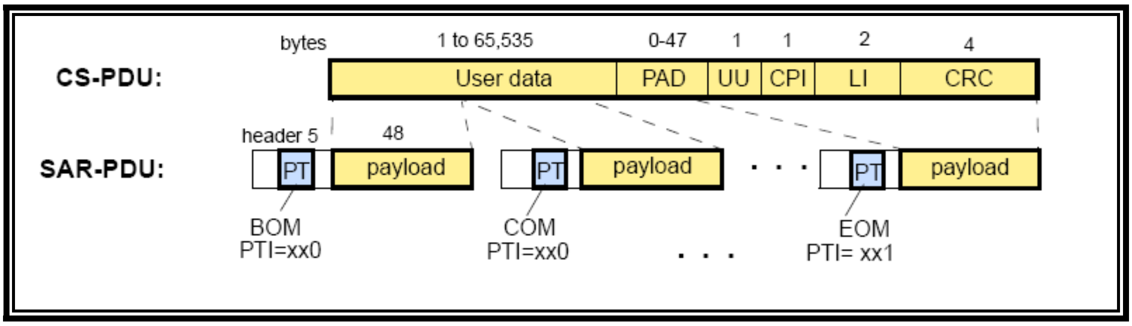



**Figura 2.17** Ensamblado de PDU AAL5[15]

### 2.1.4.7.- Beneficios

Una única red ATM dará cabida a todo tipo de tráfico (voz, datos y video). ATM mejora la eficiencia y manejabilidad de la red.

Capacita nuevas aplicaciones, debido a su alta velocidad y a la integración de los tipos de tráfico, ATM capacita la creación y la expansión de nuevas aplicaciones como la multimedia.

Compatibilidad, porque ATM no está basado en un tipo especifíco de transporte físico, es compatible con las actuales redes físicas que han sido

[15] Tomado de http://www.trendtest.com

desplegadas. ATM puede ser implementado sobre par trenzado, cable coaxial y fibra óptica.

Simplifica el control de la red. ATM está evolucionando hacia una tecnología estándar para todo tipo de comunicaciones. Esta uniformidad intenta simplificar el control de la red usando la misma tecnología para todos los niveles de la red.

Largo periodo de vida de la arquitectura. Los sistemas de información y las industrias de telecomunicaciones se están centrando y están estandarizado el ATM. ATM ha sido diseñado desde el comienzo para ser flexible en:

- Distancias geográficas
- Número de usuarios
- Acceso y ancho de banda (hasta ahora, las velocidades varían de Megas a Gigas).

## 2.2.- Protocolo de Capa 3

### 2.2.1.- IP

El protocolo de Internet (IP) es un protocolo de la capa de Red (Capa 3 del modelo OSI) que contiene información de dirección y control que permite al paquete ser encaminado o enrutado; este es el principal protocolo en el Modelo TCP/IP.

IP tiene dos funciones principales: prever la entrega de paquetes en un sistema no orientado a conexión y best effort (técnica del mejor esfuerzo) a través de una red y suministrar fragmentación y reensamblar datagramas para dar soporte a la capa 2.

#### 2.2.1.1.- Estructura de un paquete IP

Un paquete IP contiene varios campos de información mostrados en la siguiente **figura 2.18**.

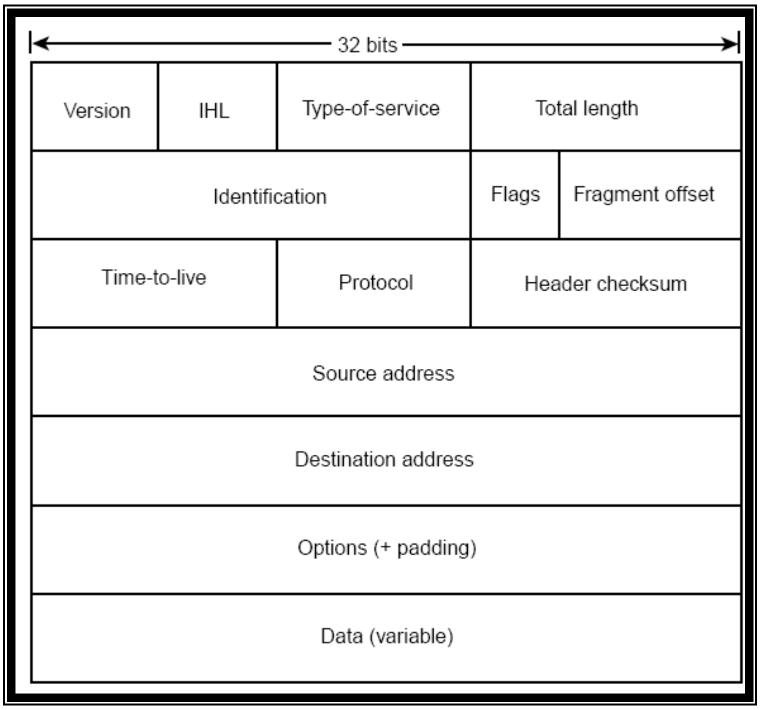



**Figura 2.18** Formato estructura IP

**Versión:** Indica la versión del protocolo ip actualmente utilizado.

**Longitud de cabecera IP (IHL):** Indica la longitud de la cabecera del datagrama en palabras de 32bits.

**Tipo de servicio:** Específica cual es el tipo de servicio de capa superior que va manejar el datagrama, esto se refiere a que algunos paquetes pueden tener prioridad sobre otros.

**Longitud total:** Especifica la longitud de en bytes de todo el paquete ip, incluida la cabecera y datos.

**Identificación:** Contiene un entero que identifica el datagrama actual. Este campo es utilizado para ayudar a unir fragmentos en un datagrama completo.

**Banderas:** Consiste de un campo de 3bit de los cuales los dos menos significativos son bits de control, el bit menos significativo especifica si el paquete esta fragmentado, el Segundo bit especifica si es el último bit de todos los fragmentos.

**Posición del fragmento:** Indica la posición del fragmento relativa al paquete original.

**Time-to-Live:** Mantiene un contador con decremento gradual hasta cero para evitar lazos, hasta el punto de descartar el paquete.

**Protocolo:** Indica cual protocolo de capa superior recibe el paquete.

**Cabecera Checksum:** Ayuda a asegurar la integridad de la cabecera del paquete.

**Dirección fuente:** Detalla la dirección IP fuente.

**Dirección destino:** Detalla la dirección IP destino.

**Opciones:** Permite al paquete IP soportar otras opciones como seguridad.

**Datos:** Contiene la información de capa superior.

### 2.2.1.2.- Direccionamiento IP

En el modelo TCP/IP cada host tiene una identificación o dirección de 32bits que se divide en dos partes: la que identifica a la red y la del host.

La dirección IP está conformada por cuatro octetos, separados por un punto y representados en notación decimal; el valor máximo que puede alcanzar un octeto es 255 y el mínimo es 0. En la siguiente figura 2.18 se aprecia la dirección 172.16.122.204.

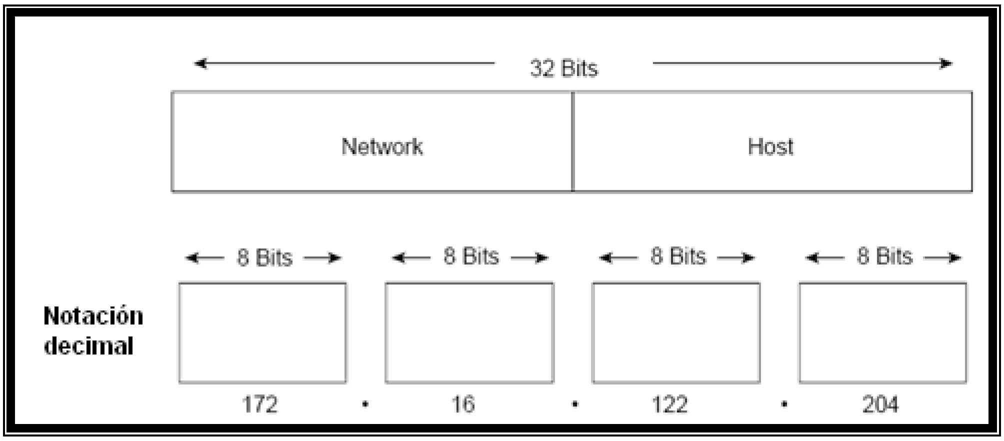



**Figura 2.19** Dirección IP

### 2.2.1.3.- IPv4

Es la primera versión del protocolo Internet en si, fue desarrollado por el IETF (Internet Engineering Task Force), IPv4 ha demostrado por su duración un diseño flexible y poderoso, pero está empezando a tener problemas, siendo el más importante el crecimiento en poco tiempo de la necesidad de direcciones IP.

### 2.2.1.4.- IPv4 en comparación con IPv6

IPv6 es la nomenclatura abreviada de "Internet Protocol Versión 6".

Es el protocolo de la próxima generación de Internet, por lo que a veces también se denomina IPng que viene de "Internet Protocol Next Generation".
Es, por tanto, la actualización del protocolo de red de datos en el que se fundamenta Internet. El IETF desarrolló las especificaciones básicas durante los 90 para sustituir la versión actual del protocolo de Internet, IP versión 4 (IPv4), que vio la luz a finales de los 70.
IPv6 aumenta el tamaño de las direcciones IP, creando un nuevo formato de dirección IP con 128bits en vez de 32bits en su modelo original.
Se espera que IPv6 reemplace gradualmente a IPv4.

Las ventajas del protocolo IPv6 se las resume en las siguientes:

- **Escalabilidad:** IPv6 tiene direcciones de 128 bits frente a las direcciones de 32 bits de IPv4.
- **Seguridad:** IPv6 incluye seguridad en sus especificaciones como es la encriptación de la información y la autentificación del remitente de dicha información.
- **Especificaciones más claras y optimizadas:** IPv6 seguirá las buenas prácticas de IPv4 y eliminará las características no utilizadas u obsoletas de IPv4, con lo que se conseguirá una optimización del protocolo de Internet.

# CAPÍTULO 3

## 3. Herramientas de Simulación de Protocolos de comunicaciones

### 3.1.- Software de simulación

La Simulación de una red es una técnica para obtener modelos de comportamientos simplificados de elementos de una red o de la red en si, se analiza la interacción entre distintos equipos que componen la red. También es usada para evaluar el rendimiento de tecnologías de red en escenarios de laboratorio.

Las herramientas de simulación pueden venir en forma de hardware y software. Las herramientas más utilizadas son software de eventos discretos. Este software es un modelo computarizado de un sistema físico. Una de las principales actividades de esta es el proceso de una lista de eventos que se realizan con orden cronológico.

Actualmente las desventajas de éste son que al agregar más componentes al modelo, su procesamiento será más lento, siendo dependiente de la capacidad de procesamiento de la computadora en la cual se encuentra instalado. El listado de estas herramientas de eventos discretos las tenemos en la **tabla 3.1**.

**TABLA 3.1** Software de eventos discretos.

| **Herramienta** | **Pagina Web** |
| --- | --- |
| Packet Tracer | http://www.cisco.com/web/learning/netacad/ |
| Ns-2 | http://www.isi.edu/nsnam/ns/ |
| OPnet | http://www.opnet.com/ |
| OMnet++ | http://www.omnetpp.org/ |
| Dynamips | www.dynamips.com |

### 3.2.- Otras herramientas de análisis y simulación de redes

En otras herramientas de análisis tenemos los analizadores de red (analizadores de protocolos o sniffers), estos realizan el proceso de capturar el tráfico de la red. Este a su vez decodifica la información, generalmente, tramas o paquetes de varios protocolos de comunicaciones y lo presenta de una manera comprensible al usuario. Una de las primeras aplicaciones de captura y análisis del tráfico de red fue Sniffer, de Network General, es por esto que una aplicación de análisis de red es conocida como Sniffer o Packet Sniffer.

Los analizadores tienen por lo general un número de protocolos soportados y que pueden decodificar, también permiten realizar gráficas de tráfico y filtros para organizar la información.

Actualmente existen varios Analizadores de red como se muestra en la siguiente **tabla 3.2**.

**TABLA 3.2** Analizadores de red.

| Herramienta | Pagina Web |
|---|---|
| Wireshark | http://www.wireshark.org/ |
| Sniffer Portable | http://www.networkgeneral.com/ |
| WinDump | http://www.winpcap.org/windump/ |
| Etherpeek | http://www.wildpackets.com/ |

De estas aplicaciones o herramientas (dado a su uso en troubleshooting) se presenta un resumen de Wireshark debido a que es uno de los más utilizados, es gratuito y soporta más de 800 protocolos para análisis.

### 3.2.1.- Wireshark

Wireshark es uno de los analizadores de protocolos más utilizados para realizar análisis y troubleshooting en redes LAN, es considerada una aplicación Packet Sniffer. Es una aplicación gratuita y tiene todas las características de un analizador de protocolos comercial.

Wireshark es una aplicación que posee la estructura de alrededor 800 protocolos de red, haciéndolo capaz en su entorno gráfico de presentarlo y hacer más fácil su análisis.

Algunas ventajas las detallamos a continuación:

- Los datos pueden ser capturados online y guardados para posterior análisis, desde Ethernet, IEEE802.11, Token Ring, FDDI, PPP, IPoATM, Frame Relay y otros.
- Es multiplataforma, es decir funciona en Windows, Linux, Solaris y otros sistemas operativos.
- Realiza análisis VoIP.
- Soporta desencriptación de muchos protocolos que poseen como: Kerberos, IPSec, SNMPv3, WEP, WAP y otros.
- Soporta lectura y escritura de varios formatos de archivos de otros analizadores de protocolos como RADCOM WAN/LAN Analyzer, Cisco Secure, Novell LANalyzer, Sniffer Pro, Tektronix Analyzer y otros.

Una desventaja es que al depender de un computador es difícil realizar capturas en interfaces V.35 y E1 debido a la poca disponibilidad de interfaces de este tipo; a pesar de esto si tiene capacidad de analizarlos luego de importarlos de otros analizadores.

Dado a que interfaces ATM utiliza hardware dedicado para el procesamiento de las celdas, es muy poco probable poder capturar las celdas sin ser procesadas por alguna subcapa AAL de ATM. A esto hay que reconocer que para manejar las interfaces ATM se necesitan servidores muy rápidos debidos a las altas velocidades, lo que vuelve muy costosa la solución.

### 3.3.- Herramientas de hardware para simulación de redes

Dada la necesidad de procesamiento las simulaciones en tiempo real utilizan hardware de simulación para servir modelos de protocolos y servicios en tiempo real.

Simulación es una técnica para reemplazar componentes físicos de un sistema complejo. Esta es lograda cuando los componentes de la red no pueden diferenciar entre un componente real y otro simulado, además está definida en tiempo real.

### 3.3.1.- RADCOM RC-100WL

En este subcapítulo se darán a conocer los puntos básicos del equipo RADCOM RC-100WL para análisis y simulación de redes con diferentes protocolos a nivel LAN y WAN. En la actualidad este equipo ha sido reemplazado por la familia de equipos Prism Lite y Performer Analyzer de Radcom. Debido a que este modelo de equipo no soporta interfaz ATM, esta será realizada con la versión demo del equipo Prism Lite de Radcom

#### 3.3.1.1.- Arquitectura interna

El RC-100 WL consiste de un procesador RISC Intel i960 que controla el funcionamiento del modulo de interfaz de línea (LMI), el buffer interno que permite el almacenamiento  hasta 8 Mbyte de RAM y la interfaz de conexión del PC como se muestra en la **figura 3.1**.

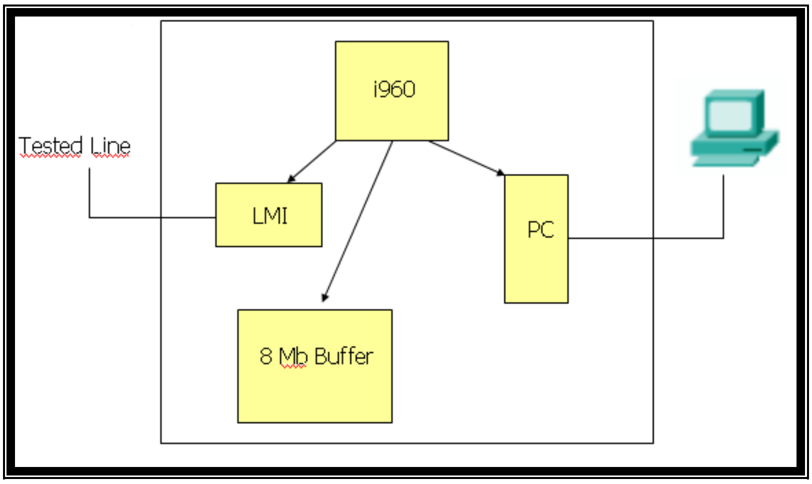



**FIGURA 3.1** Arquitectura interna

La unidad externa del analizador se ocupa de las velocidades de la línea de comunicación, mientras que el PC sirve como interfaz hombre - máquina.

### 3.3.1.2.- Presentación

Este posee varias ventajas que detallamos a continuación:

- Unidad Externa: se conecta a un PC portátil y opera bajo Windows.
- Diseño modular: sistema básico con suplementos de hardware y software opcionales.

El equipo fue diseñado de manera modular para adaptarse a las necesidades de la red, es así, que posee una amplia gama de módulos de interfaz que detallamos a continuación:

- Interfaz MTYP con soporte para V.35, V.24/RS-232, RS-530, X.21/V.11.
- Lan : Ethernet, 100BASE-t, 10BASE-5 (AUI).
- ISDN : E1/T1.

El analizador tiene 2 puertos a los que se conecta cualquier combinación de módulos de interfaz (LAN + WAN, WAN + WAN, LAN + LAN, RDSI/BEI + Ethernet)

La unidad externa posee altas prestaciones, contiene internamente un procesador RISC que permite alto rendimiento y rapidez. La unidad externa opera en conjunto con la línea bajo prueba, recogiendo datos on-line. El usuario visualiza los datos usando el PC.

En la parte frontal posee indicadores como se muestra en la **figura 3.2**:


**FIGURA 3.2** Panel frontal de equipos Radcom.

- Indicador ON esta iluminado cuando el analizador esta funcionado.
- Los indicadores de actividad de la línea RX y TX, indican actividad de Recepción y transmisión sobre la línea para los canales 1 y 2 respectivamente.

- El indicador FAULT se ilumina cuando el programa de auto prueba del analizador detecta un fallo en la unidad o el cable.

El panel posterior contiene los puertos, conectores para el analizador y módulos de la interfaz como se muestra en la **figura 3.3**.

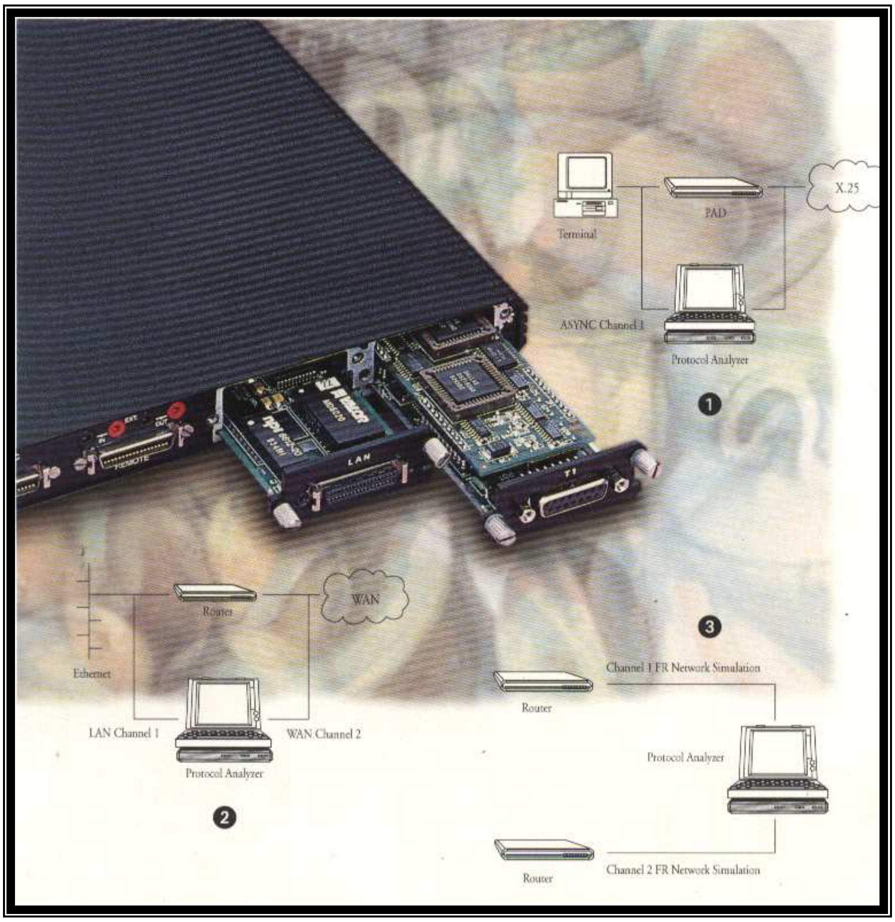



**FIGURA 3.3** Panel posterior

#### 3.3.1.3.- Conexión del equipo

La unidad externa se conecta al PC usando el puerto paralelo y a la línea usando cables monitor o de simulación, según la línea que sea analizada y la tarjeta interfaz seleccionada.

##### 3.3.1.3.1.- Cable Monitor

En el modo monitor, el analizador se puede usar para probar la velocidad y tráfico en la línea, disponibilidad de la línea, tasa de error y otros. El tráfico en la línea puede ser capturado para un análisis inmediato. Los cables monitor suministrados con el analizador utilizan buffer incorporados para aislar la línea bajo prueba desde el analizador de protocolos. Estos buffer permiten el funcionamiento de la línea bajo prueba incluso cuando el analizador de protocolo no está siendo usado.

##### 3.3.1.3.2.- Cable Simulación

En el modo de simulación, el analizador puede probar dispositivos del usuario o de la red mediante la generación de datos en la línea. Las opciones de simulación incluyen definición de datos del usuario y varios parámetros relativos a la línea; control sobre la distribución de la longitud de la trama; inyección de errores de trama, y un simulador de ráfagas con un alto rendimiento. El analizador permite un completo monitoreo durante las operaciones de simulación.

#### 3.3.1.4.- Software de interfaz con el usuario (GUI)

La instalación del Software del equipo RC-100WL es simple, pero se necesitan algunos requerimientos mínimos del computador para una instalación exitosa:

- Microsoft Windows 2000, XP.
- Se necesitan 100Mbyte de espacio en disco duro.
- Se necesita mínimo de 50Mbyte en disco duro para adquisición y almacenamiento de datos de usuario.
- Microprocesador Pentium III o superior.

A continuación se detallará de manera breve algunos aspectos de los procesos para su utilización, los cuales se han escogido debido a que son procesos genéricos y utilizados en casi todos los protocolos que el equipo RADCOM RC-100WL permite analizar y simular, otros se detallarán en el momento de la simulación en el siguiente capítulo en su protocolo especifico.

#### 3.3.1.4.1.- Ventana principal

La pantalla de análisis está dividida en dos áreas principales: el área de estado y el área de trabajo como en la **figura 3.4**.

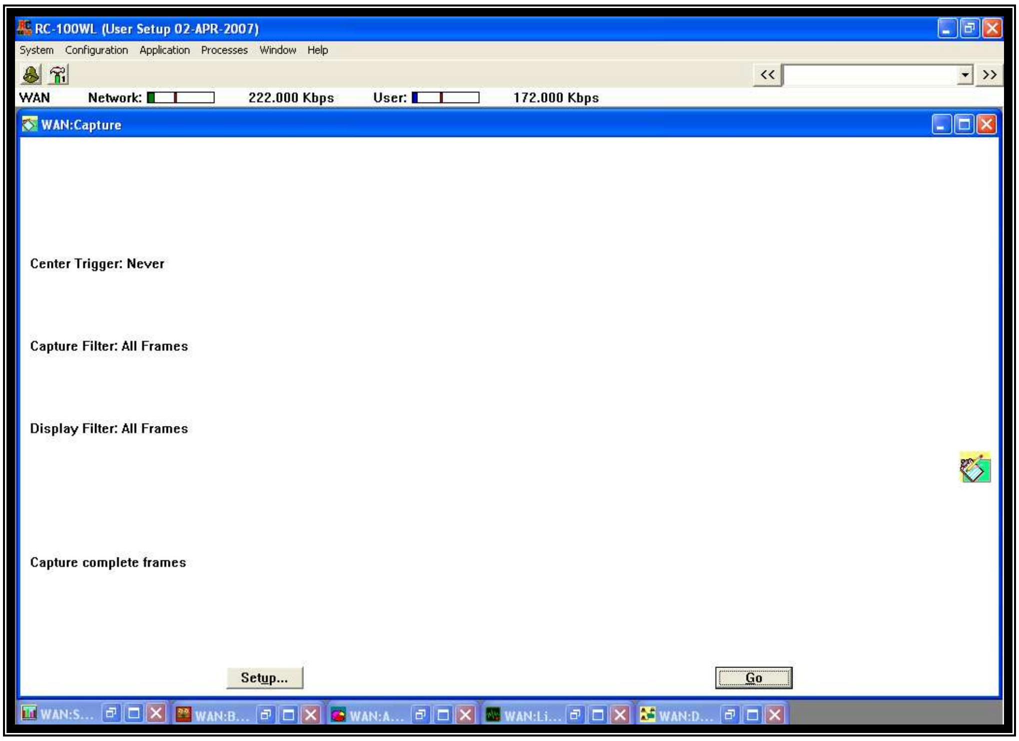



**FIGURA 3.4** Ventana principal

Área de Estado: Contiene información de estado referente a la velocidad de transferencia de la línea.

Área de Trabajo: Constituye la parte inferior de la pantalla y contiene los iconos y presentación de datos de cada uno de los procesos. Los procesos que no estén en uso se muestran como iconos minimizados y se activan haciendo doble clic con el botón izquierdo del ratón. Se hace clic en "Go" para activar el proceso o se hace clic en "Setup" para definir la configuración del proceso.

### 3.3.1.4.2.- Asignación de canal

En la **figura 3.5** se muestra como llevar a cabo la asignación de un canal, se hace clic en "Configuration" en la barra de menús y se elige "Channel Assignment". Realizar la asignación de canal la primera vez que use el analizador, o siempre que las conexiones hardware cambien.

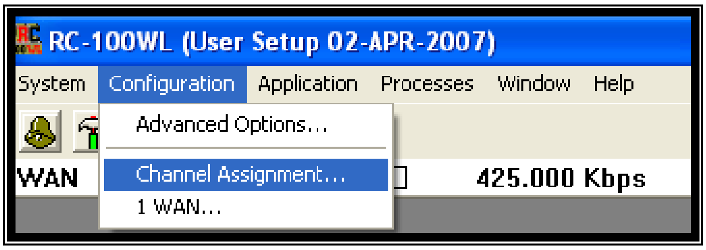



**FIGURA 3.5** Asignación de canal

Pasos para configurar el analizador en el cuadro de diálogo asignación de canal, ver **figura 3.6**:

- Verifique que el canal conectado está correctamente identificado (Puerto) y especificado como activo.
- Configure el modo de trabajo requerido para cada canal.

- Haga clic en el botón Martillo “Configuración” a la derecha del canal activo para abrir la ventana de diálogo configuración.
- Los siguientes modos de trabajos están disponibles: monitor (Para monitorear uno o ambos extremos), Frame Simulation y pruebas de BER.

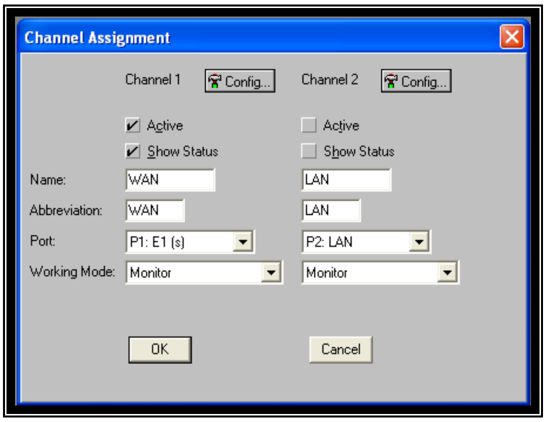



**FIGURA 3.6** Asignación de canal (2)

El cuadro de dialogo configuración (**figura 3.7**) para una configuración del canal de forma avanzada, donde se especifica el tipo de interfaz, modo de funcionamiento y protocolo a usar para el canal; esta consiste de varias opciones detalladas a continuación:

- Port: Puerto seleccionado en la ventana de diálogo Channel Assigment (P1 representa Puerto 1 y es el interfaz situado a la izquierda).
- Interface: Configura las opciones hardware del interfaz. Especifique el tipo exacto de interfaz que se va analizar.

* Frame level: Para Wan elija HDLC; para LAN elija Ethernet.
* Protocolo Stack: Protocolo de comienzo; realice la selección según la línea que está siendo analizada.

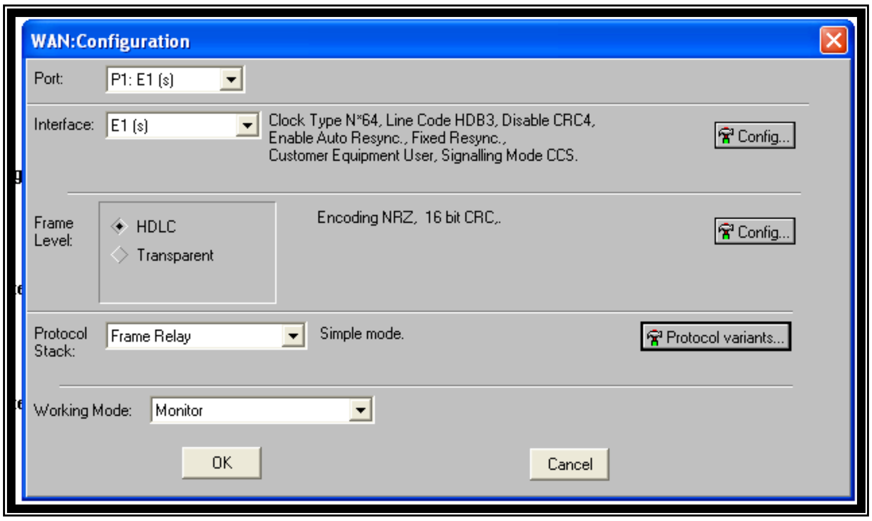



**FIGURA 3.7** Configuración del canal 1

### 3.3.1.4.3.- Proceso de captura

El proceso de captura permite la decodificación on-line de los datos de la línea de más de 200 protocolos de comunicaciones. La selección cuidadosa de filtros permite capturar tramas específicas. La visualización actual puede ser observada en varios niveles de detalle: completa parcial o resumida. Los datos se pueden almacenar en el disco duro del PC para análisis posteriores.

El proceso de captura tiene tres estados posibles:

- Ready / Listo: El proceso está listo para ejecutarse. En este estado podemos configurar los parámetros de captura definiendo filtros y triggers.

- Run / Ejecutar: El proceso está ejecutándose, capturando datos en tiempo real. La visualización es una muestra de los datos guardados en la RAM interna.

- View / Ver: Se para el proceso. Podemos visualizar, imprimir, registrar y analizar los datos almacenados en la RAM (incluyendo guardarlos en el disco duro).

**Proceso de captura Ready / Listo**

En este cuadro de diálogo mostrado en la **figura 3.8**, permite iniciar la captura de tramas (Go) o cambiar parámetros de captura, filtros, triggers o el modo de presentación de las tramas (Setup).

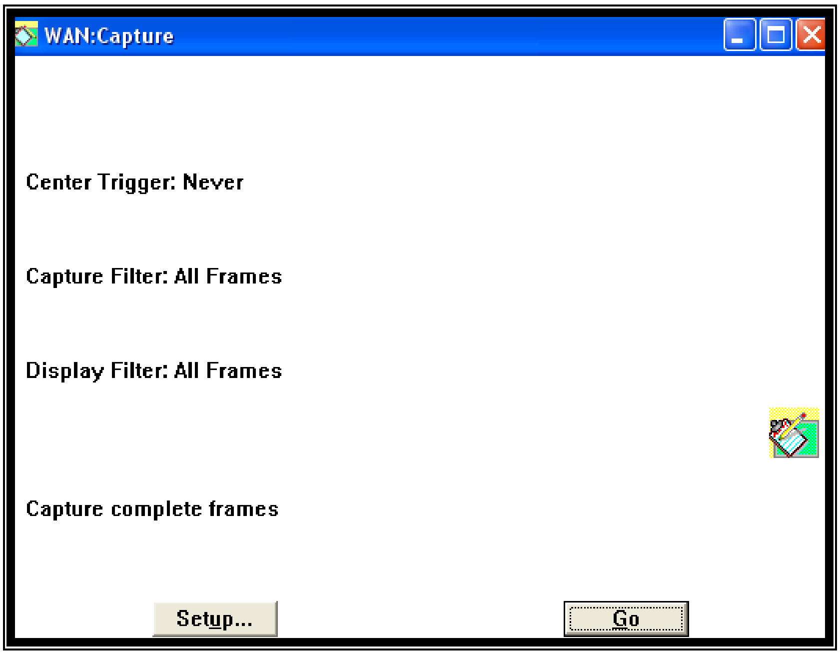



**FIGURA 3.8** Cuadro de diálogo del proceso de captura

Al seleccionar la opción Setup permite visualizar el cuadro de diálogo de Configuración de Captura (Capture Setup) como se detalla en la **figura 3.9**; donde se encuentran opciones como:

- Capture Filter: para realizar una limitación selectiva de los datos capturados y almacenados en el buffer RAM.
- Display Filter: para realizar una limitación selectiva de los datos enviados a la pantalla, es decir presentados.
- Capture Triggers: para determinar cuando comenzará o finalizará un proceso.
- Capture mode: para capturar continuamente, según triggers o cuando el buffer esté lleno.

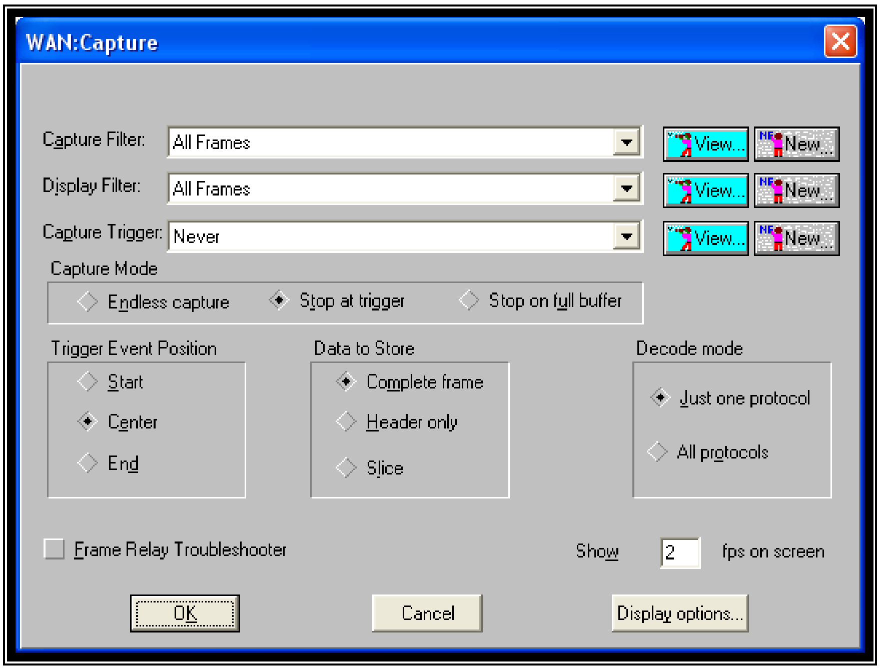



**FIGURA 3.9** Cuadro de diálogo de configuración del proceso de captura

**Proceso de captura View / Visualizar**

El proceso de captura visualizar y ejecutar son muy similares, debido que al comenzar una captura la ventana cambia mostrando las tramas de manera continua mientras va capturando y el proceso visualizar empieza cuando se finaliza la captura cuando se llena la RAM, cuando se alcanza la condición de trigger o cuando hacemos clic en el botón stop. Entonces se muestra la ventana de Presentación del Buffer de captura como en la **figura 3.10**.

- Search: Este botón nos permite buscar una trama específica en la pantalla, el criterio de búsqueda puede ser según una cadena de caracteres (String match), un patrón (pattern match) o incluso definido de acuerdo con los campos de protocolos

- Restart: para finalizar el estado actual y abrir la ventana de configuración de captura (Capture Setup).
- Done: para salir del proceso de captura.
- Options: para acceder a las opciones de visualización disponibles.

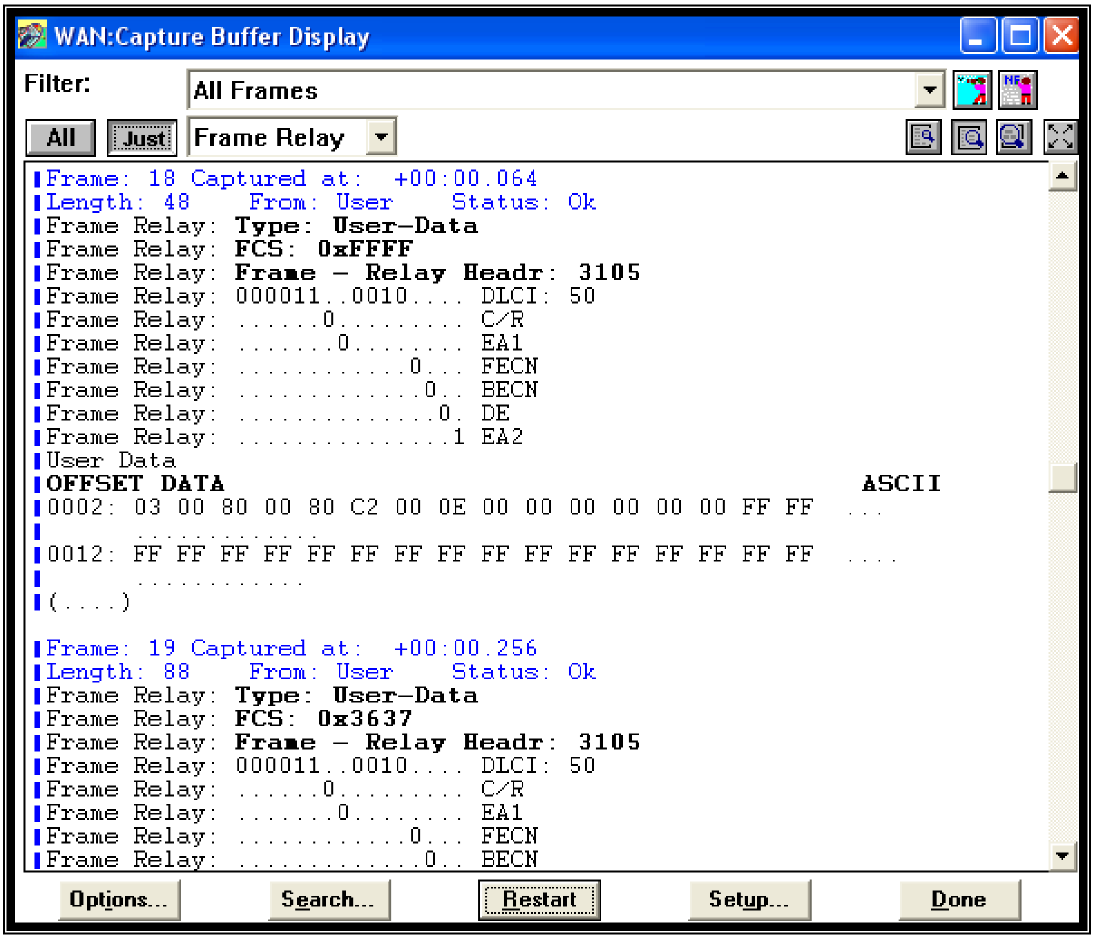



**FIGURA 3.10** Ventana del proceso de captura visualizar

Las capacidades de post captura están diseñadas para facilitar el análisis de datos y exportar los datos capturados a otras aplicaciones externas como:

- Decodificación de un único protocolo.
- Decodificación de múltiples protocolos.
- Visualización de pantalla dual.
- Funciones de grabación e impresión.
- Temporización relativa y absoluta.
- Búsqueda de datos específicos.
- Exportar Datos a archivos ASCII o aplicaciones MS-Windows.

En la figura anterior al seleccionar el botón de opciones permite acceder a las opciones de visualización disponibles. La misma operación se puede realizar haciendo clic en el botón derecho del ratón en cualquier punto de la ventana de captura, esto facilita algunas opciones mostradas a continuación; ver **figura 3.11**:

- Summary: Muestra información resumida de los datos capturados.
- Views: Muestra el fichero de datos en una o dos ventanas separadas.
- Record: Guarda los datos capturados en un fichero, externamente o internamente para análisis off-line.
- Timing: Determina el formato de visualización de tiempos en la ventana de captura.
- Print: Imprime usando la impresora MS-Windows definida por defecto.

- Marks: Inserta un marcador en un punto específico o salta a un marcador.
- Filter: Define un filtro para visualizar un subconjunto de tramas del fichero de datos.
- Analysis: Realiza análisis de datos.
- Preferente: Define el modo de visualización por niveles del protocolo.

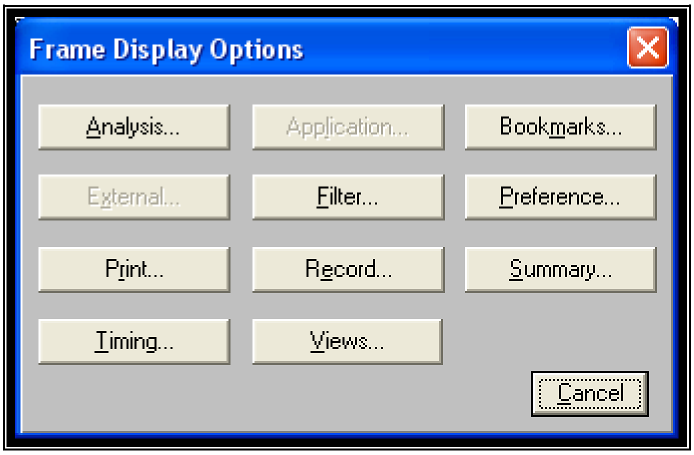



**FIGURA 3.11** Opciones de post captura

**Análisis de Datos Capturados**

Al seleccionar el botón Analysis en la ventana Frame Display Options para analizar los datos capturados.

- Subject: Define el asunto a analizar.
- Analysis: La ventana desplegable de análisis contiene una lista de análisis disponibles para un asunto en particular.

- Filter: Define un filtro para realizar el análisis en tramas determinadas.
- Graphic: Especifica el formato de presentación de datos.

El análisis seleccionado se realiza sobre los datos almacenados en el buffer. A continuación un ejemplo de un análisis de datos capturados en el buffer RAM, se puede visualizar en formato torta (ver **figura 3.12**) o en gráfico de barras, en esta figura en formato torta.

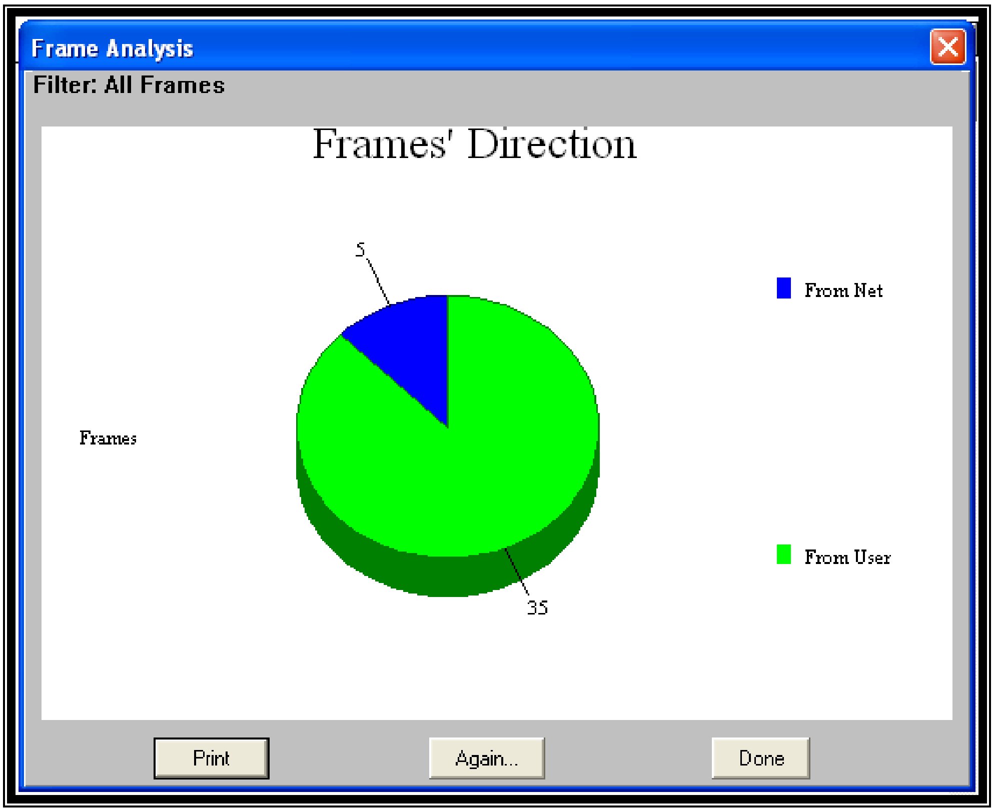



**FIGURA 3.12** Análisis de datos capturados

### 3.3.1.4.4.- Proceso de captura (Background Record)

Es un proceso de captura que se recomienda usar cuando se necesite más cantidad de memoria de almacenamiento que la proporcionada por el buffer RAN interno. La forma más eficiente para usar este proceso es mediante la definición de filtros.

El botón "Setup" muestra el cuadro de dialogo de configuración (ver **figura 3.13**) es utilizado para definir los parámetros de captura. Los parámetros de la grabación subordinada definen que datos guardar en el disco. Se recomienda definir filtros para centrarnos en una sección de los datos en particular, y para definir que partes específicas de las tramas de datos van a ser guardados.

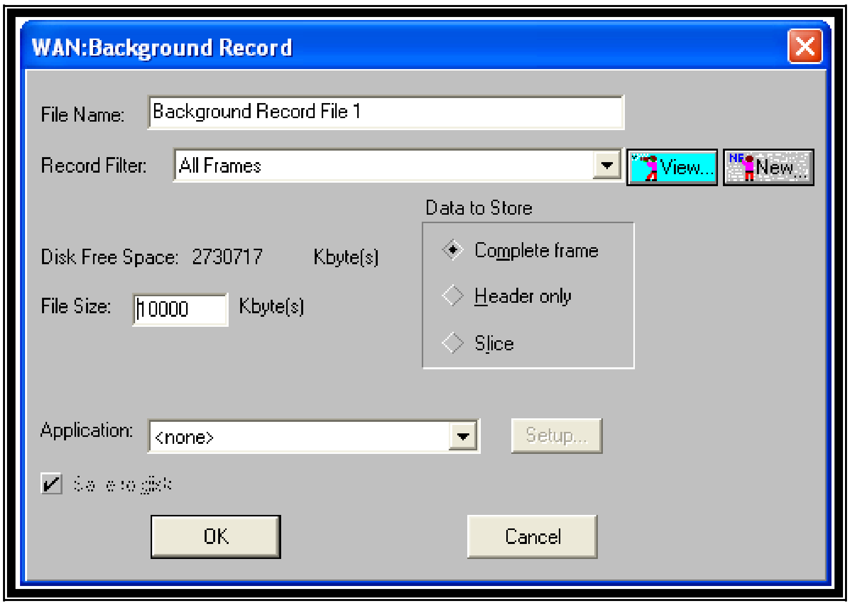



**FIGURA 3.13** Diálogo de configuración del Background

#### 3.3.1.4.5.- Proceso de simulación

- Dos vías de comunicación.
- El analizador transmite y/o recibe datos.
- Definición de parámetros de Simulación.
- Útil para probar equipos de comunicaciones.

El usuario determina las propiedades de la simulación. Los ejemplos típicos incluyen la determinación de la velocidad, tamaño y contenido de tramas transmitidas las cuales hacen útil la simulación para probar equipos de comunicaciones.

Existen dos tipos de simulación como se muestra en la **figura 3.14**:

**Simulación de tramas**: Se define una trama específica para una transmisión continua de hasta 2 Mbps. Alternativamente, es posible elegir una generación de datos aleatorios desde el analizador y, por lo tanto simular el comportamiento de una red real.

**Simulación de Ráfagas:** La transferencia de tráfico es por ráfagas. Esto permite el realizar pruebas al límite de las capacidades de la línea. El usuario controla el espacio entre tramas. Este modo, se pueden transmitir 40.000 tramas cortas por segundo.

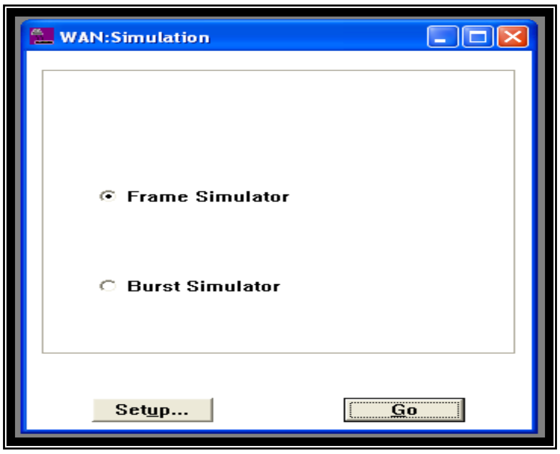



**FIGURA 3.14** Diálogo del proceso de simulación

Para seleccionar el modo de simulación:

Abra la ventana “Channel Configuration” y seleccione el nombre y número del canal deseado.

En la ventana de la lista desplegable “Working mode”, seleccione “Frame Simulation” y haga clic en OK. El icono “Frame Simulation” aparecerá en la parte inferior de la pantalla. Haga doble clic en el icono para abrir la ventana “Simulation” en su estado “Ready”.

Elija el tipo de simulación deseada; Frame Simulator o Burst Simulator.

El proceso de simulación está basado en ciclos. La pantalla de configuración (ver **figura 3.15**) controla todos los parámetros relevantes del ciclo. En la ventana “Simulator Parameters” se puede seleccionar “User Frame” o “Simulator Generated”.

Seleccione “Simulator Generated” para transmitir tramas cuyo contenido es generado por el analizador.

A partir de este momento puede definir el rango de longitudes de la trama. El analizador de protocolos realiza una generación aleatoria de valores dentro del rango definido. Use Data para definir el contenido de la trama. Seleccione “Don’t care” para generar datos de forma aleatoria o Ascending para generar valores de bytes ascendentes.

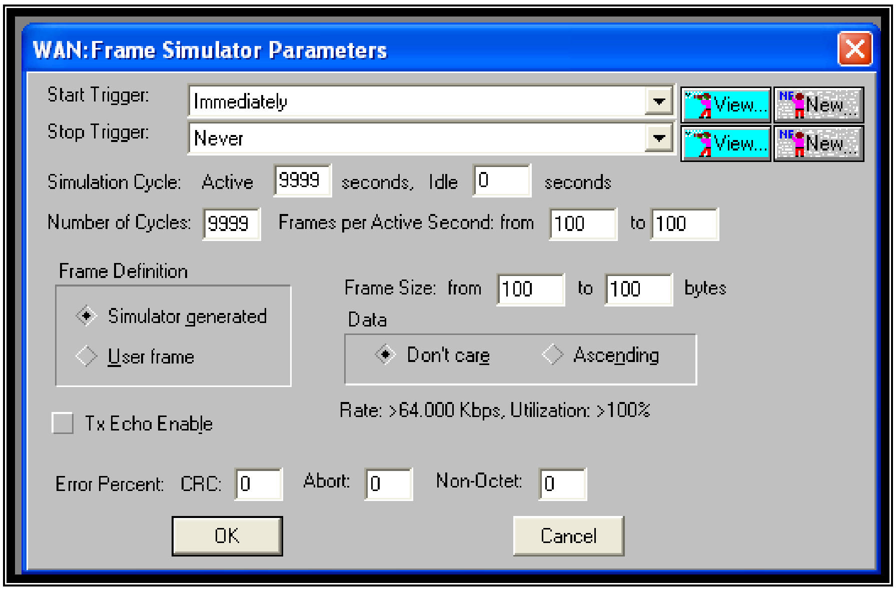



**FIGURA 3.15** Diálogo del proceso de simulación

### Definicion de Tramas de Usuario

Seleccione “**User Frame**” en la ventana de “Frame Simulator Parameters” (ver **figura anterior 3.15**) para definir una trama fija para transmisiones continuas. Haga clic en el botón de “User Frame Definition” se muestra la ventana permitiendo definir todos los bytes de la trama simulada como se muestra en la **figura 3.16**.

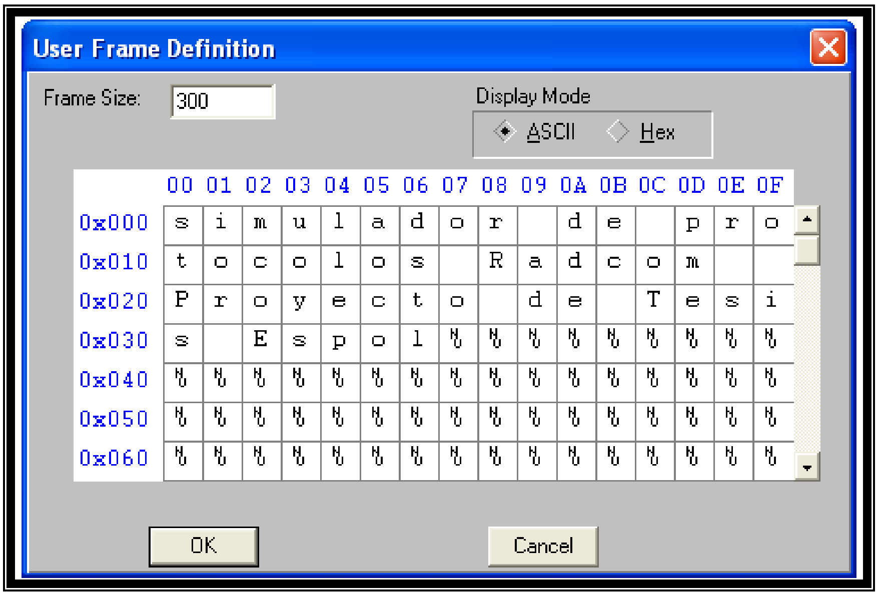



**FIGURA 3.16** Ventana para definir trama específica

Defina los bytes de la trama haciendo clic en la ventana que corresponde al byte y escribiendo el valor.

### Simulación de Ráfagas - Ready

Para usar la Simulación de ráfagas, seleccione “Burst Simulator” en la ventana de simulación (ver **figura 3.14**) y haga clic en el botón “Setup”. La ventana del “Burst Simulator Parameters” está abierta para que defina el número de tramas transmitidas por segundo, su longitud y espacio entre ellas.

El modo de “Burst Simulator” es particularmente efectivo cuando se usa para cargar la unidad bajo prueba con muchas pequeñas tramas y por eso origina una elevada sobrecarga en el procesamiento de datos.

# CAPÍTULO 4

## 4. Proyecto

Para el desarrollo de este capitulo se ha visto la necesidad de implementar varias topologías de red para los distintos protocolos que se van a analizar. Además como se ha disminuido la complejidad de la red para aumentar la comprensión de la utilidad del equipo Radcom se han utilizado 3 ruteadores Cisco, dos serie 805 y un router 1601 con una interfaz WIC-1T.

Como se detalló en el capitulo anterior se va utilizar el analizador Radcom RC-100WL el cual posee una interfaz multitype y una interfaz Ethernet.

### 4.1.- Pruebas realizadas

En cada laboratorio se procedió con la configuración de equipos ruteadores para obtener la red que se desea implementar, las pruebas de conectividad luego de lo cual se procede con la captura de datos en tiempo real y su respectivo análisis de las primeras tramas y graficación de todos los datos capturados con gráficos pre-establecidos.

## 4.2.- Implementación de una red de datos

Se van a desarrollar cuatro laboratorios en este capítulo los cuales son en el siguiente orden:

- Práctica de laboratorio de simulación del protocolo HDLC
- Práctica de laboratorio de simulación del protocolo Mac/Ip
- Práctica de laboratorio de simulación del protocolo Frame Relay
- Práctica de laboratorio de simulación del protocolo ATM.

Para los tres primeros laboratorios mencionados anteriormente se utilizó un procedimiento que se detalla en el Anexo 1, mientras que para el laboratorio de ATM se detalla en el Anexo 2.

La estructura de la red del laboratorio HDLC va servir como base para el análisis del laboratorio de Mac/Ip.

En el laboratorio de Frame Relay se utilizó tres ruteadores Cisco, uno se configuró como switch Frame Relay; mientras que los dos restantes se destinaron como dispositivos de acceso Frame Relay (FRAD).

En el laboratorio de ATM debido a la no disponibilidad de equipos ATM se va realizar el análisis con el software demo del Radcom Prism-Lite, el cual realiza una simulación de tráfico real para realizar la captura de datos.

### 4.3.- Práctica de Laboratorio de Simulación de HDLC

#### 4.3.1.- Descripción general

Esta práctica permite que el estudiante se familiarice con la estructura de la trama HDLC, con su variante cHDLC; además de la configuración y funcionamiento de la misma. Se utilizará un analizador de Protocolos para poder visualizar la estructura de la trama.

#### 4.3.2.- Equipos requeridos

- ✓ Dos ruteadores Cisco con una interfaz ethernet y una interfaz serial cada uno.
- ✓ Un switch no administrable.
- ✓ Dos computadores con tarjeta de red y puerto serie
- ✓ Un Analizador Radcom Rc-100wl con interfaz multitype y cable monitor V.35; además necesitamos tener instalado el software del equipo en un computador.

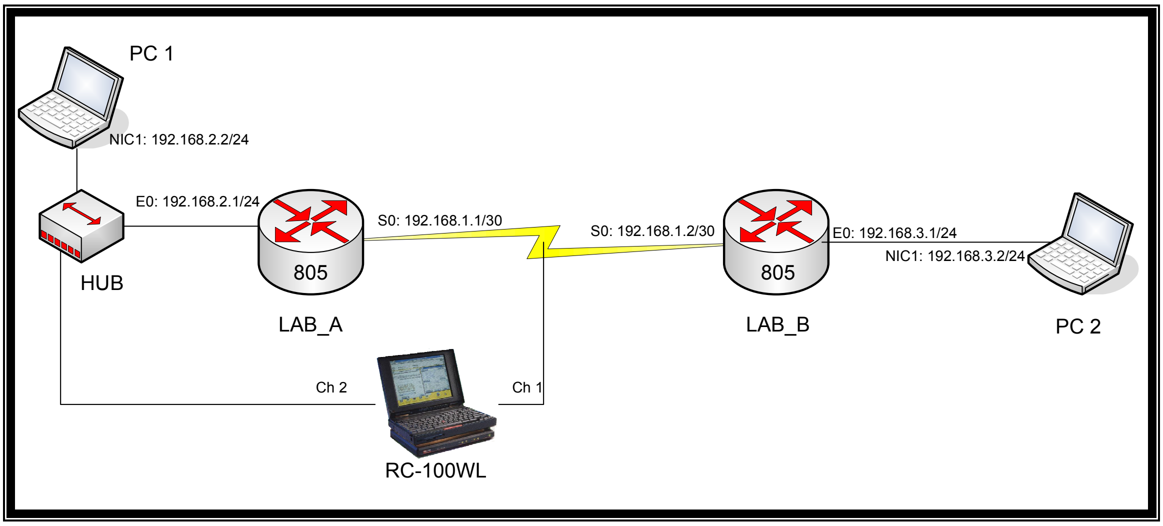



**Figura 4.3.1** Diagrama de red

### 4.3.3.- Descripción del contenido de la práctica.

Se capturarán las tramas HDLC con el analizador de Protocolos Radcom Rc-100wl, se analizara la estructura de la trama cHDLC.

### 4.3.4.- Desarrollo de la práctica

El diseño de la práctica es la interconexión de dos ruteadores Cisco 805 con protocolo de encapsulación HDLC en el enlace serial.

#### 4.3.4.1.- Esquema de conexión

Conectamos el analizador de protocolos RC-100 WL en la interfaz serial del enlace como se muestra en la figura **4.3.1**.

#### 4.3.4.2.- Conexiones de los equipos

Se deben conectar los router entre si, esto es:

- ✓ Interfaz serial 0 de ruteador Lab_A con el cable monitor V.35 (conector Macho) del equipo Radcom
- ✓ Interfaz serial 0 del ruteador Lab_B con el cable monitor V.35 (conector hembra) del equipo Radcom.
- ✓ Recordar que el cable V.35 DCE va de lado del LAB_A.
- ✓ Conectar en los puertos disponibles del Hub la interfaz Ethernet 0 del ruteador Lab_A, la PC1 y la interfaz AUI del analizador de protocolos.
- ✓ Proceder a conectar los computadores en la interfaz Ethernet 0 del ruteador respectivo. Además proceder con la conexión de los cables consola del ruteador según la necesidad.

#### 4.3.4.3.- Configuración de los ruteadores

Se configura los ruteadores con la información de la siguiente **tabla 4.3.1**:

**Tabla 4.3.1** Configuración de direcciones IP

| **Designación del Ruteador** | **Nombre del Ruteador** | **Tipo de Interfaz** | **Dirección serial** | **Dirección ethernet 0/Mascara de Subred** | **Encapsulación Capa 2** |
|---|---|---|---|---|---|
| Router 1 | Lab_A | DCE | 192.168.1.1/30 | 192.168.2.1/24 | HDLC |
| Router 2 | Lab_B | DTE | 192.168.1.2/30 | 192.168.3.1/24 | HDLC |

**Paso 1: Configuración de los password**

**Ruteador 1:**

```
Router>enable
Router#configure terminal
Router(config)#hostname Lab_A
Lab_A(config)#enable secret cisco
Lab_A(config)#line console  0
Lab_A(config-line)#password cisco
Lab_A(config-line)#login
Lab_A(config-line)#exit
Lab_A(config)#line vty 0 4
Lab_A(config-line)#password cisco
Lab_A(config-line)#login
Lab_A(config-line)#exit
```

**Ruteador 2:**

```
Router>
Router>enable
Router#configure  terminal
Router(config)#hostname Lab_B
Lab_B(config)#enable secret cisco
Lab_B(config)#line console  0
Lab_B(config-line)#password cisco
Lab_B(config-line)#login
Lab_B(config-line)#exit
Lab_B(config)#line vty 0 4
Lab_B(config-line)#password cisco
Lab_B(config-line)#login
Lab_B(config-line)#exit
```

**Paso 2: Configurar las interfaces seriales**

La configuración del protocolo de encapsulación HDLC es por default en los ruteadores cisco

Para el ruteador Lab_A:

Lab_A(config)#interface serial 0
Lab_A(config-if)#encapsulation hdlc
Lab_A(config-if)#ip address 192.168.1.1 255.255.255.252
Lab_A(config-if)#clok rate 64000
Lab_A(config-if)#no shutdown
Lab_A(config-if)#exit

Para el ruteador Lab_B:

Lab_B(config)#interface serial 0
Lab_B(config-if)#encapsulation hdlc
Lab_B(config-if)#ip address 192.168.1.2 255.255.255.252
Lab_B(config-if)#no shutdown
Lab_B(config-if)#exit

**Paso 2: Configurar las interfaces Ethernet 0**

Para el ruteador Lab_A:

Lab_A(config)#interface ethernet 0
Lab_A(config-if)#ip address 192.168.2.1 255.255.255.0
Lab_A(config-if)#no shutdown
Lab_A(config-if)#exit

Para el ruteador Lab_B:

Lab_B(config)#interface ethernet 0
Lab_B(config-if)#ip address 192.168.3.1 255.255.255.0
Lab_B(config-if)#no shutdown
Lab_B(config-if)#exit

**Paso 3: Configurar el enrutamiento EIGRP**

Para configurar el Protocolo de Enrutamiento de Gateway Interior Mejorado use la siguiente sintaxis:

Para el ruteador Lab_A:

```
Lab_A(config)#router eigrp 100
Lab_A(config-router)#network 192.168.1.0
Lab_A(config-router)#network 192.168.2.0
Lab_A(config-router)#exit
Lab_A(config)#
```

Para el ruteador Lab_B:

```
Lab_B(config)#router eigrp 100
Lab_B(config-router)#network 192.168.1.0
Lab_B(config-router)#network 192.168.3.0
Lab_B(config-router)#exit
Lab_B(config)#
```

Nota: Utilizar el siguiente comando en cada uno de los ruteadores router#copy running-config startup-config, para guardar su configuración.

#### 4.3.4.4 Verificación de la configuración HDLC

**PASO 1: Verificar la encapsulación**

Use el comando show interface s0 para mostrar el protocolo de encapsulación en la interfaces serial como se muestra en la **figura 4.3.2**.

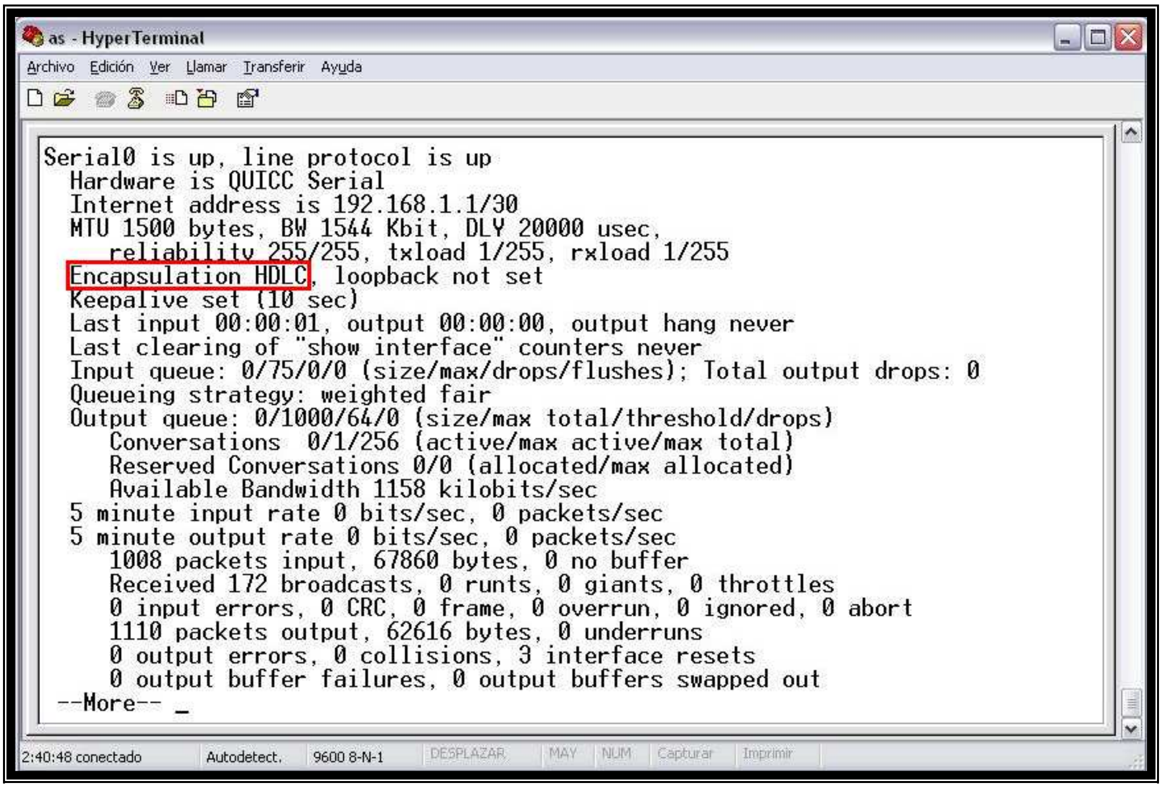
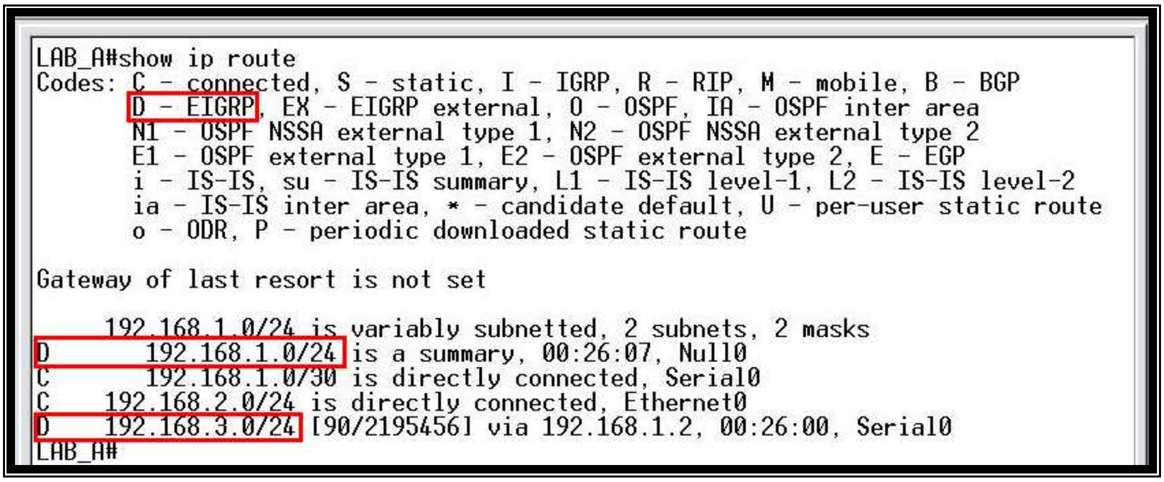



**Figura 4.3.2** Verificación de protocolo de encapsulación.

**PASO 2: Verificar el protocolo de enrutamiento**

Utilice el comando **show ip route** para mostrar las adyacencias del protocolo de enrutamiento como se muestra en la pantalla captura de la **figura 4.3.4**.

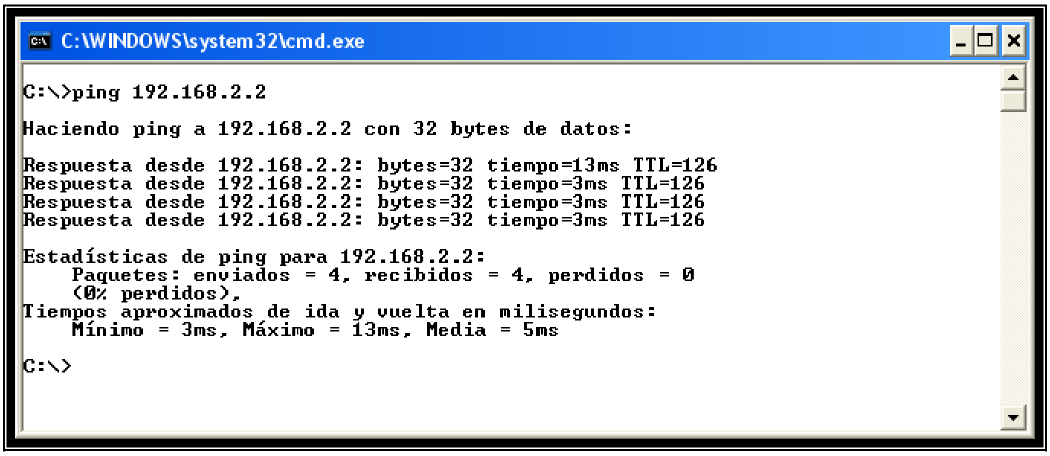


```
LAB_A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
D       192.168.1.0/24 is a summary, 00:26:07, Null0
C       192.168.1.0/30 is directly connected, Serial0
C    192.168.2.0/24 is directly connected, Ethernet0
D    192.168.3.0/24 [90/2195456] via 192.168.1.2, 00:26:00, Serial0
LAB_A#
```

**Figura 4.3.3** Verificación de protocolo de enrutamiento.

## PASO 3: Verificar la conectividad

Haga Ping a las interfaces Ethernet del ruteador Lab_B como se muestra en la **figura 4.3.4** y ruteador Lab_A como en **figura 4.3.5**.



```
C:\WINDOWS\system32\cmd.exe

C:\>ping 192.168.2.2

Haciendo ping a 192.168.2.2 con 32 bytes de datos:

Respuesta desde 192.168.2.2: bytes=32 tiempo=13ms TTL=126
Respuesta desde 192.168.2.2: bytes=32 tiempo=3ms TTL=126
Respuesta desde 192.168.2.2: bytes=32 tiempo=3ms TTL=126
Respuesta desde 192.168.2.2: bytes=32 tiempo=3ms TTL=126

Estadísticas de ping para 192.168.2.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 3ms, Máximo = 13ms, Media = 5ms

C:\>
```

**Figura 4.3.4** Ping hacia la interfaz Ethernet del ruteador Lab_B.


**Figura 4.3.5** Ping hacia la interfaz Ethernet del ruteador Lab_A.

### 4.3.4.5.- Captura de la trama cisco HDLC

Para capturar la estructura de la trama, se procederá a utilizar el analizador de protocolos RC-100WL.

### Paso 1: Ejecutar el programa RC-100WL

Activar solo la interfaz Multi Type, en working mode, se seleccionará Monitor. Luego OK como se detalla en la siguiente figura.

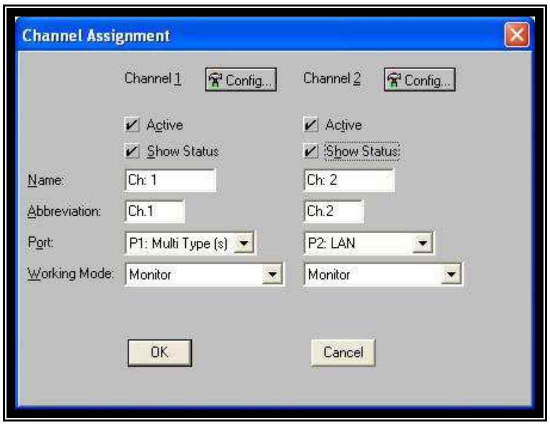



**Figura 4.3.6** Selección de canal a realizar análisis

**Paso 2: Seleccionar el protocolo utilizado**

En el menú Channel Assigment seleccionar en CH 1 Config para seleccionar el protocolo a utilizar como se muestra en la **figura 4.3.7**.

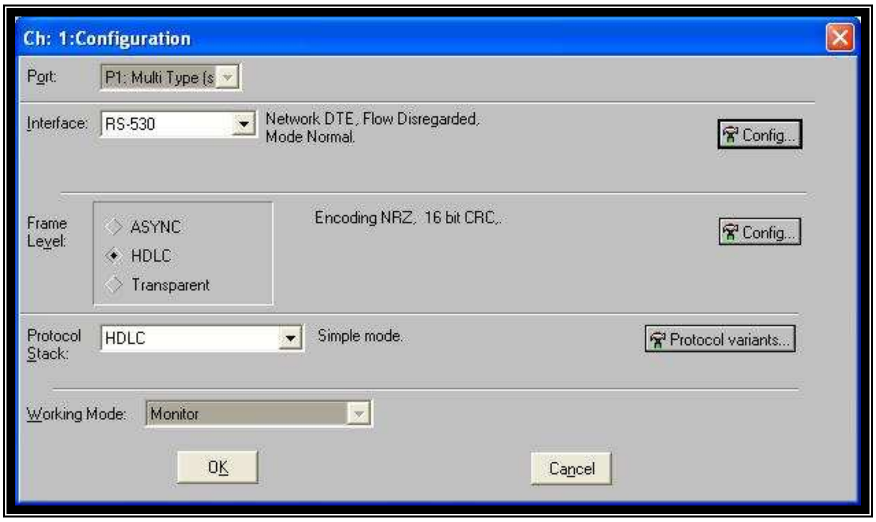



**Figura 4.3.7** Selección de protocolo de pila

**Paso 3: Capturar las tramas**

Luego en el menú Window seleccionar Ch #: capture

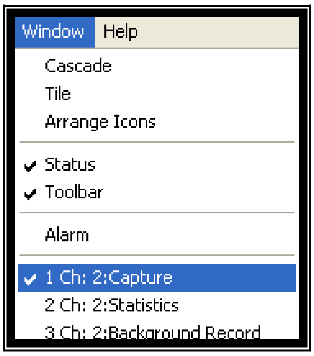



**Figura 4.3.8** Selección de la ventana de captura.

Posteriormente en la ventana Ch2: Capture se da clic en Go para empezar la captura de tramas en la interfaz serial. Luego para finalizar la captura se procederá a dar clic en el botón Stop y obtenemos las tramas como se muestra en la **figura 4.3.9**.

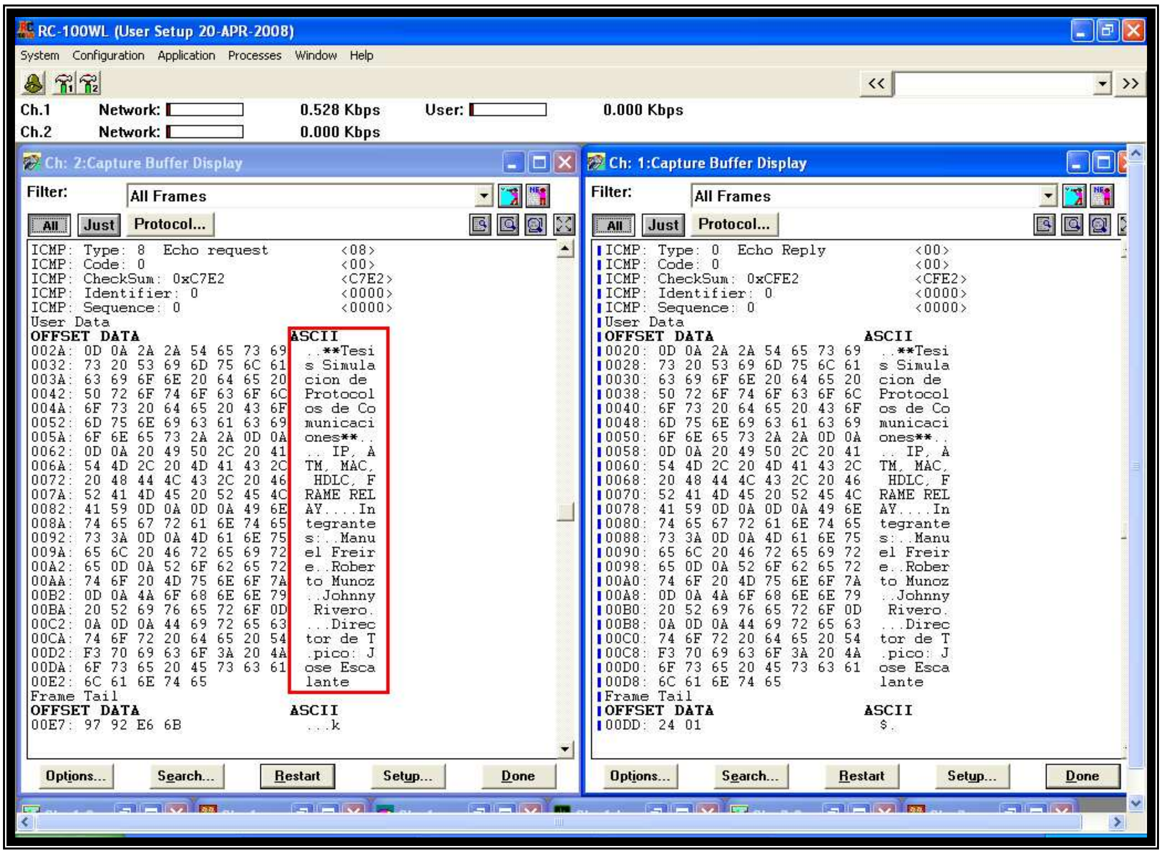


**Figura 4.3.9** Vista de la ventana de captura

### 4.3.4.6.- Análisis de la trama cisco HDLC

Una vez capturada las tramas se procederá a realizar el análisis correspondiente.

#### 4.3.4.6.1.- Análisis de la trama 0

En la siguiente **tabla 4.3.2** se muestra la trama 0 donde se observa que el primer octeto corresponde al campo de dirección 0x8F que indica una trama broadcast, el siguiente octeto corresponde al campo de control 0x00, recordar que este campo de control no está implementado en cHDLC.

**Tabla 4.3.2** Análisis de la trama 0

```
Frame: 0 Captured at:  +00:00.000
Length: 286    From: User    Status: Ok
OFFSET DATA                                         ASCII
0000: 8F 00 20 00 02 B4 DD 81 00 01 00 09 4C 41 42 5F  .. .........LAB_
0010: 42 00 02 00 11 00 00 00 01 01 01 CC 00 04 C0 A8  B...............
0020: 01 02 00 03 00 0B 53 65 72 69 61 6C 30 00 04 00  ......Serial0...
0030: 08 00 00 00 01 00 05 00 D9 43 69 73 63 6F 20 49  .........Cisco I
0040: 6E 74 65 72 6E 65 74 77 6F 72 6B 20 4F 70 65 72  nternetwork Oper
0050: 61 74 69 6E 67 20 53 79 73 74 65 6D 20 53 6F 66  ating System Sof
0060: 74 77 61 72 65 20 0A 49 4F 53 20 28 74 6D 29 20  tware .IOS (tm)
0070: 43 38 30 35 20 53 6F 66 74 77 61 72 65 20 28 43  C805 Software (C
0080: 38 30 35 2D 53 59 36 2D 4D 57 29 2C 20 56 65 72  805-SY6-MW), Ver
0090: 73 69 6F 6E 20 31 32 2E 30 28 37 29 54 2C 20 20  sion 12.0(7)T,
00A0: 52 45 4C 45 41 53 45 20 53 4F 46 54 57 41 52 45  RELEASE SOFTWARE
00B0: 20 28 66 63 32 29 0A 43 6F 70 79 72 69 67 68 74   (fc2).Copyright
00C0: 20 28 63 29 20 31 39 38 36 2D 31 39 39 39 20 62   (c) 1986-1999 b
00D0: 79 20 63 69 73 63 6F 20 53 79 73 74 65 6D 73 2C  y cisco Systems,
00E0: 20 49 6E 63 2E 0A 43 6F 6D 70 69 6C 65 64 20 4D   Inc..Compiled M
00F0: 6F 6E 20 30 36 2D 44 65 63 2D 39 39 20 31 36 3A  on 06-Dec-99 16:
0100: 35 38 20 62 79 20 70 68 61 6E 67 75 79 65 00 06  58 by phanguye..
0110: 00 0E 43 69 73 63 6F 20 43 38 30 35 33 9A        ..Cisco C8053.
```

El tercer y cuarto octeto corresponde al protocolo de nivel superior CDP= 0x2000.

Como se conoce que el protocolo de descubrimiento cisco (CDP) envía paquetes broadcast; esto confirma que los campos de la trama HDLC están correctos.

#### 4.3.4.6.2.- Análisis de la trama SLARP

En la **tabla 4.3.3** se observa que el primer octeto corresponde al campo de dirección 0x8F que indica una trama broadcast, el siguiente octeto corresponde al campo de control 0x00. El tercer y cuarto octeto corresponde al protocolo SLARP = 0x8035, los siguientes 4 octetos definen si es una trama de request(0x00), de replica (0x01) o una trama Keep-alive (0x02).

**Tabla 4.3.3** Trama 1

```
Frame: 1 Captured at:  +00:00.691
Length: 26    From: User    Status: Ok
OFFSET DATA
ASCII
0000: 8F 00 80 35 00 00 00 02 00 00 00 01 00 00 00 00     ...5............
0010: FF FF B0 C2 EA 72 00 0A F8 5A                             .....r...Z
```

En este caso en una trama keep-alive enviada del usuario y posteriormente tenemos los números de secuencias enviados (0x01) y números de secuencia recibidos (0x00).

La siguiente **tabla 4.3.4** es una trama keep-alive enviada de la red con los números de secuencias enviados (0x01) y números de secuencia recibidos (0x01). Las **tablas 4.3.5** y **4.3.6** siguen la secuencia anteriormente descrita, dado a que es un intercambio de datos para comprobar que está activo el enlace.

**Tabla 4.3.4** Trama 5

```
Frame: 5 Captured at:  +00:04.668
Length: 24    From: Network    Status: Ok
OFFSET DATA                                                          ASCII
0000: 8F 00 80 35 00 00 00 02 00 00 00 01 00 00 00 01              ...5............
0010: FF FF 60 47 B1 A0 1E AD                                  ..`G....
```

**Tabla 4.3.5** Trama 16

```
Frame: 16 Captured at:  +00:10.691
Length: 26    From: User    Status: Ok
OFFSET DATA
      ASCII
0000: 8F 00 80 35 00 00 00 02 00 00 00 02 00 00 00 01      ...5............
0010: FF FF B0 C3 11 83 00 0A 60 73                              ........`s
```

**Tabla 4.3.6** Trama 23

```
Frame: 23 Captured at:  +00:14.588
Length: 24    From: Network    Status: Ok
OFFSET DATA                                                      ASCII
0000: 8F 00 80 35 00 00 00 02 00 00 00 02 00 00 00 02      ...5............
0010: FF FF 60 47 D8 B1 86 48                                  ..`G...H
```

### 4.3.4.6.3.- Análisis de la red

Este es un ejemplo de decodificación de ip encapsulado sobre cHDLC. Esta decodificación permite al usuario identificar de forma inmediata los protocolos encapsulados y si los datos recibidos son los esperados.

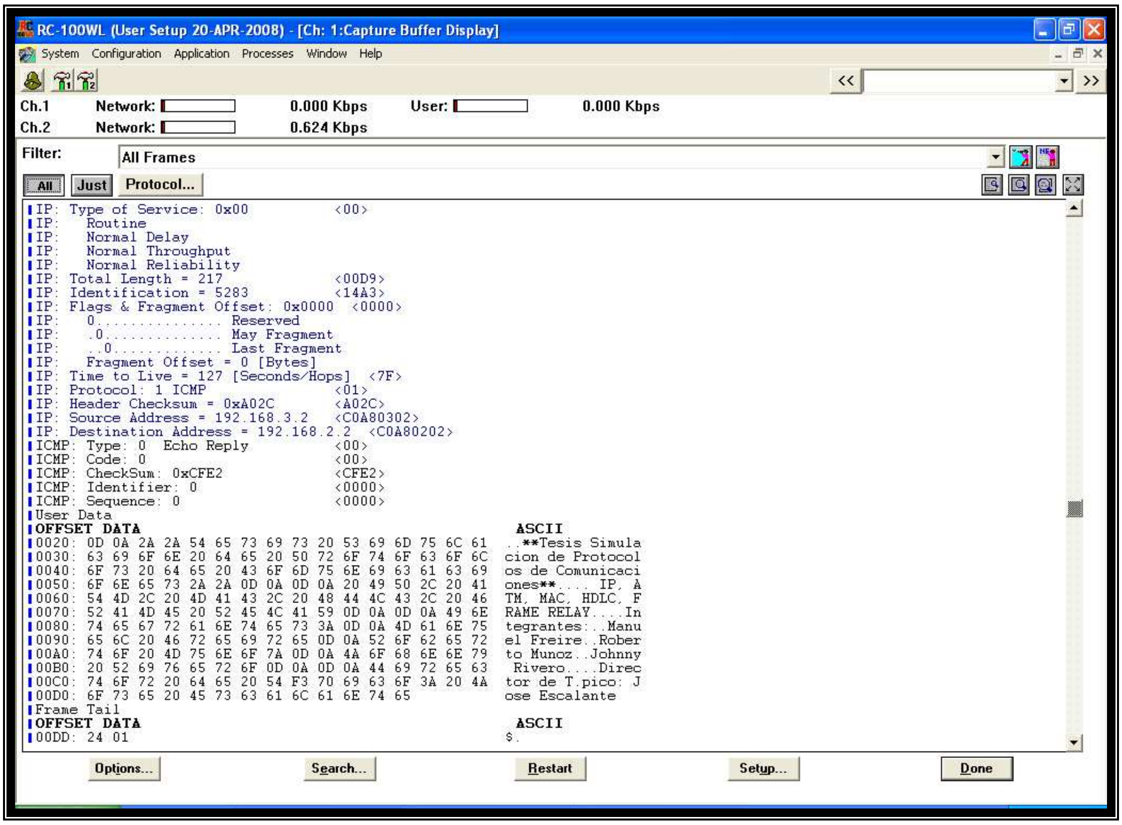



**Figura 4.3.10** Vista de la ventana de captura (2)

En la trama capturada de datos podemos observar el protocolo ip y el protocolo ICMP, que indica el mensaje generado.

**Paso 1: Análisis de las tramas ICMP**

Para observar el análisis preconfigurado del equipo Radcom, dentro de la ventana de captura dar click derecho y se obtiene una lista con opciones, escoger “Analysis”. Luego en “Subject” escoger ”ICMP”.ver **figura 4.3.11**.

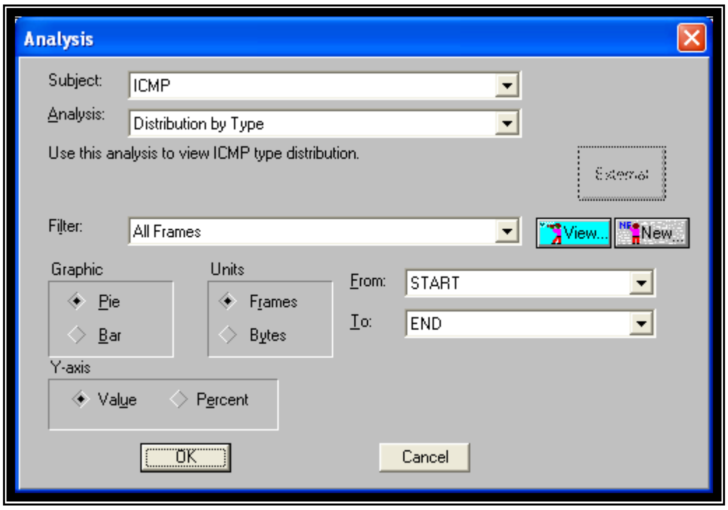



**Figura 4.3.11** Selección de parámetros de análisis

**Distribución por tipo.** Se muestra la **figura 4.3.12** con el análisis de distribución por tipo de las tramas ICMP. Esta figura indica el tipo de código ICMP dentro del paquete, en este caso se tienen 55 paquetes tipo petición de eco y 48 de respuesta de eco.

Además se visualizan otros tipos que no son válidos como tipo 97, 105, 113, 98, 106,114,99 y 107. Estos aparecen pues al realizar un ping con un tamaño mayor a la unidad máxima de transferencia (MTU = 1500bytes) el paquete IP se fragmenta. Por lo tanto en la cabecera IP el campo Protocolo=ICMP pero la cabecera ICMP solo está en el primer paquete y no en todos los fragmentos como se aprecia en la **figura 4.3.13**

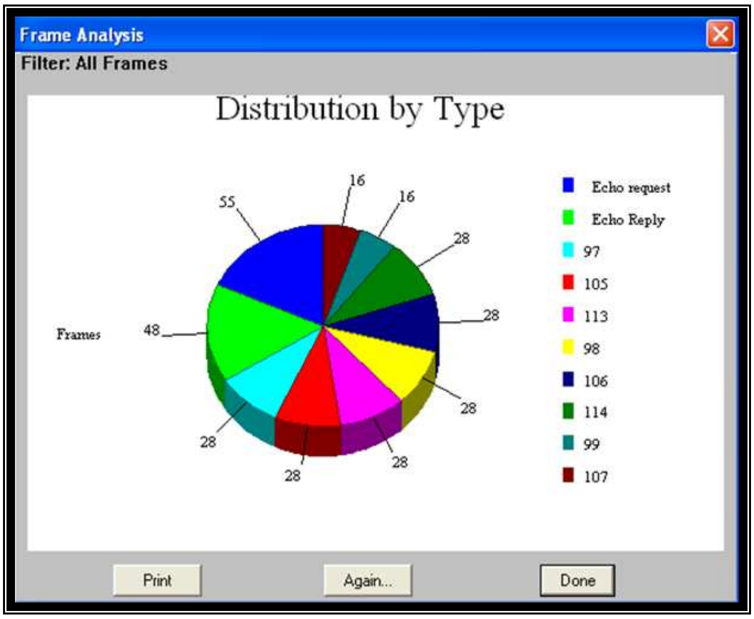



**Figura 4.3.12** Análisis por ICMP

```
Frame: 0 Captured at:  +02:30.258
Length: 1506     From: User     Status: Ok
Cisco Router: Protocol is IP           <0800>
IP: Version = 4                        <45>
IP: IHL = 20 [Bytes]
IP: Type of Service: 0x00              <00>
IP:    Routine
IP:    Normal Delay
IP:    Normal Throughput
IP:    Normal Reliability
IP: Total Length = 1500                <05DC>
IP: Identification = 31761             <7C11>
IP: Flags & Fragment Offset: 0x2172   <2172>
IP:    0.............. Reserved
IP:    .0............. May Fragment
IP:    ..1............ More Fragment
IP:    Fragment Offset = 2960 [Bytes]
IP: Time to Live = 127 [Seconds/Hops]  <7F>
IP: Protocol: 1 ICMP                   <01>
IP: Header Checksum = 0x1249           <1249>
IP: Source Address = 192.168.3.2       <C0A80302>
IP: Destination Address = 192.168.2.2   <C0A80202>
ICMP: ERROR: Unknown message type
ICMP: Type: 105
User Data
OFFSET DATA                                           ASCII
0019: 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 61 62   jklmnopqrstuvwab
0029: 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72   cdefghijklmnopqr
0039: 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6A 6B   stuvwabcdefghijk
```

**Figura 4.3.13** Fragmento de paquete ICMP

**Paso 2: Análisis de la trama IP**

Se tienen varias opciones (ver **figura 4.3.14**) relacionadas con el campo tipo de servicio en la cabecera IP y actividad de tráfico que se detallan a continuación:

- Retardo (Delay).
- Precedencia (Precedence).
- Fiabilidad (Reliability).
- Rendimiento (Throughput).
- Actividad de tráfico de red (tráfico entre pares).
- Distribución de Tráfico por dirección destino.
- Distribución de Tráfico por dirección fuente.
- Distribución por protocolo.

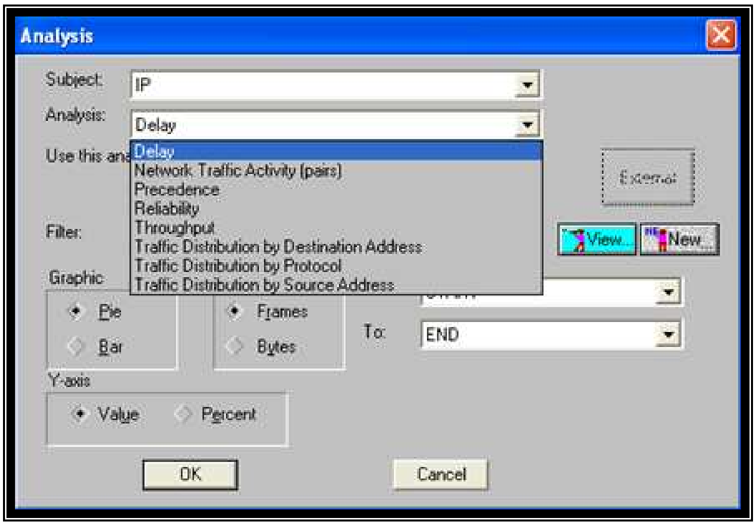



**Figura 4.3.14** Análisis de IP

**Retardo.** Estas estadísticas son obtenidas desde el campo tipo de servicio en la cabecera IP. Se observa que todos los paquetes IP tiene un retardo normal como se muestra en la **figura 4.3.15**.

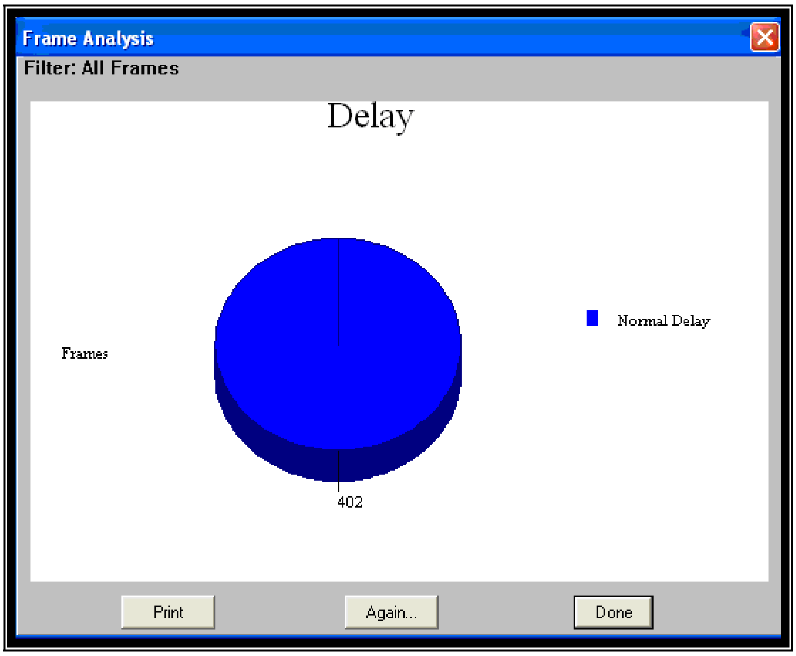



**Figura 4.3.15** Análisis por Retardo

**Precedencia.** Estas estadísticas son obtenidas desde el campo tipo de servicio en la cabecera IP que establece la prioridad del paquete. En la **figura 4.3.16** se observan 306 paquetes de tipo rutina y 96 de tipo control de Internet, se debe tener en cuenta que control de Internet tiene mayor prioridad y es usado por los protocolos de enrutamiento. Cuando se aplican políticas de calidad de servicio este campo es controlado para definir prioridad de los paquetes.

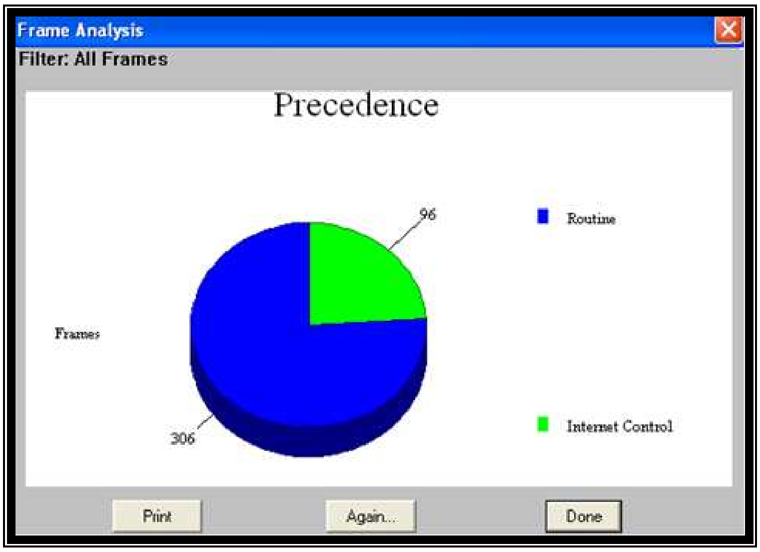



**Figura 4.3.16** Análisis por Precedencia

**Fiabilidad.** Estas estadísticas son obtenidas desde el campo tipo de servicio en la cabecera IP. Se observa que todos los 402 paquetes IP tienen el campo Fiabilidad=normal como se muestra en la **figura 4.3.17**.

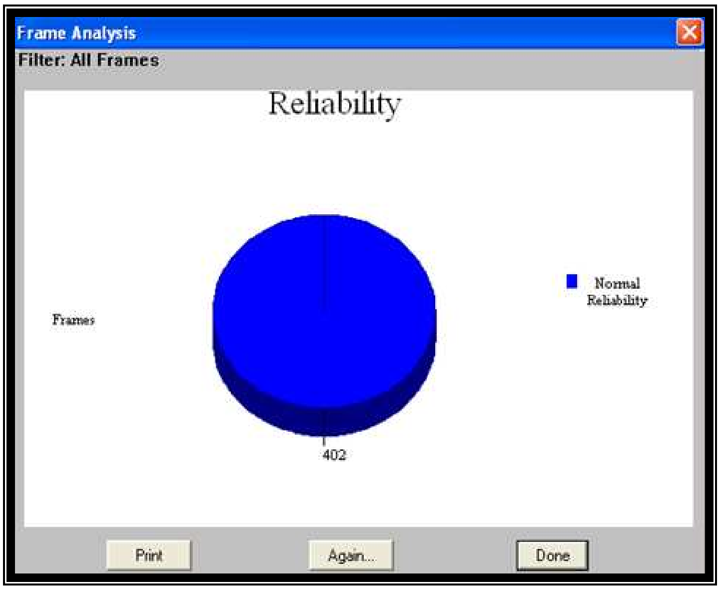



**Figura 4.3.17** Análisis por Fiabilidad

**Rendimiento.** Estas estadísticas son obtenidas desde el campo tipo de servicio en la cabecera IP. Se observa que todos los paquetes IP tiene un rendimiento normal como se muestra en la **figura 4.3.18**.

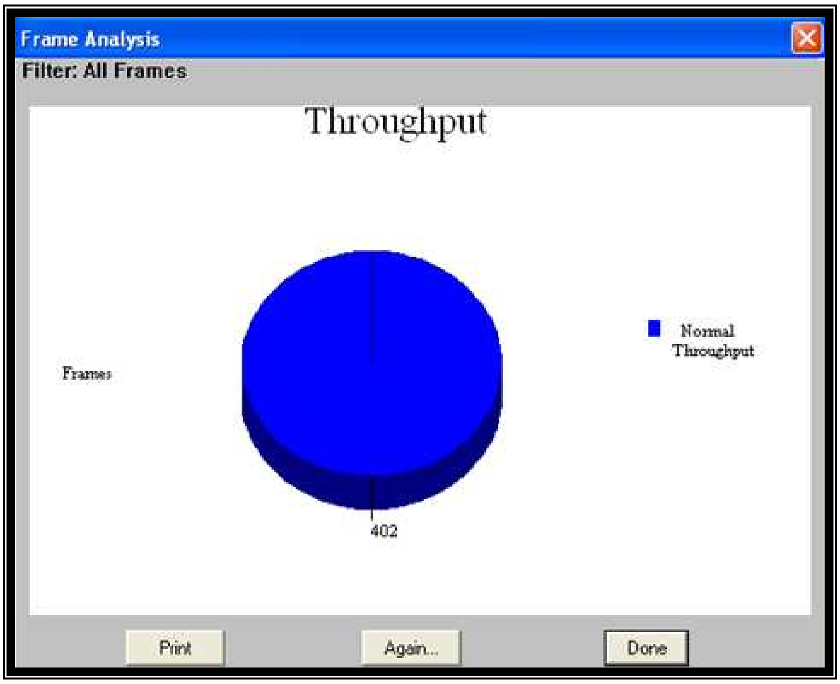



**Figura 4.3.18** Análisis por Rendimiento

**Actividad de tráfico de red (tráfico entre pares).** La **figura 4.3.19** muestra la tabla de la actividad de tráfico entre direcciones IP y sumando todos los paquetes IP da un total de 402 paquetes IP en la red.

El Host 192.168.1.2 ha enviado 45 paquetes a la dirección 224.0.0.10 correspondientes a paquetes Hello del protocolo EIGRP.

El Host 192.168.1.1 ha enviado 43 paquetes a la dirección 224.0.0.10 correspondientes a paquetes Hello del protocolo EIGRP.

El Host 192.168.2.2 ha enviado 147 paquetes a la dirección 192.168.3.2 y este ha enviado 140 a la primera dirección.

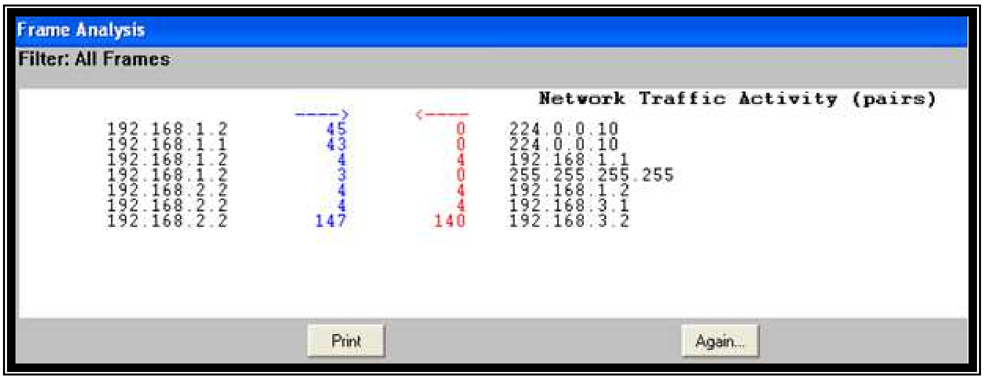



**Figura 4.3.19** Tráfico entre pares

**Distribución de tráfico por dirección destino.** En esta **figura 4.3.20** se puede observar que la dirección IP 192.168.2.2 ha recibido 148 paquetes IP. La dirección IP 192.168.3.2 ha recibido 147 paquetes IP.

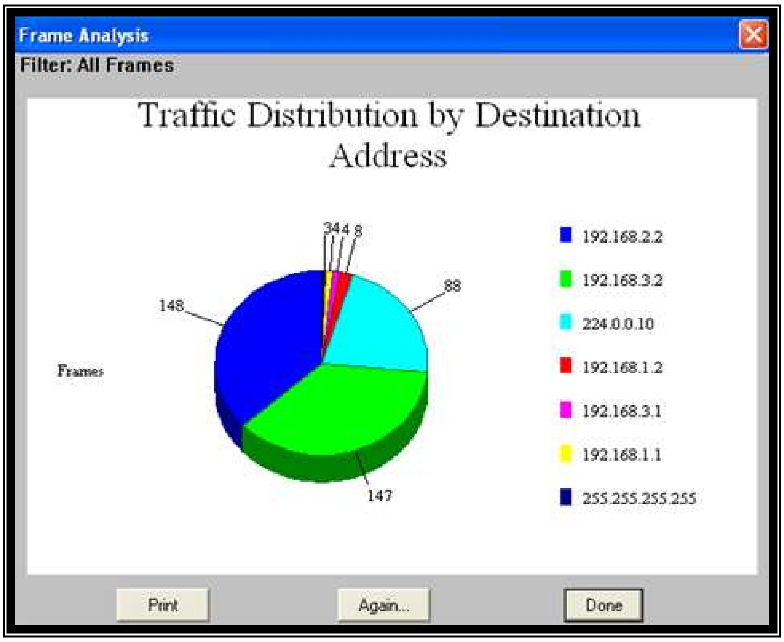



**Figura 4.3.20** Distribución de Tráfico por dirección destino

**Distribución de tráfico por dirección fuente.** La siguiente **figura 4.3.21** indica que la ip 192.168.2.2 ha enviado la mayor cantidad de paquetes IP.

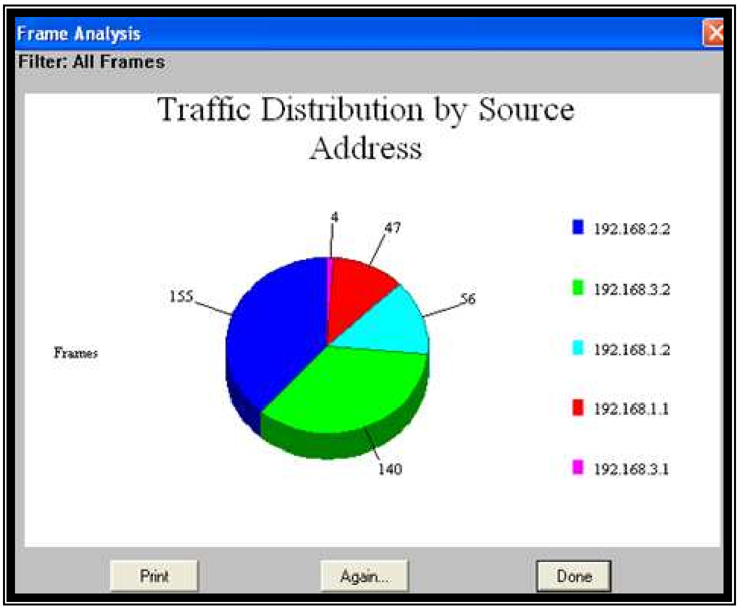



**Figura 4.3.21** Distribución de Tráfico por dirección fuente

**Paso 3: Análisis por distribución de protocolo**

Se pueden realizar análisis de la distribución de los protocolos en la red. En la **figura 4.3.22** se muestra el gráfico en diagrama de barras y en la **figura 4.3.23** se muestra en forma tabular. Ambas figuras muestran la cantidad de tramas de cada protocolo.

Se observa que se capturaron un total de 452 tramas cHDLC, de las cuales 402 contienen el protocolo IP y 50 contienen el protocolo cisco SLARP.

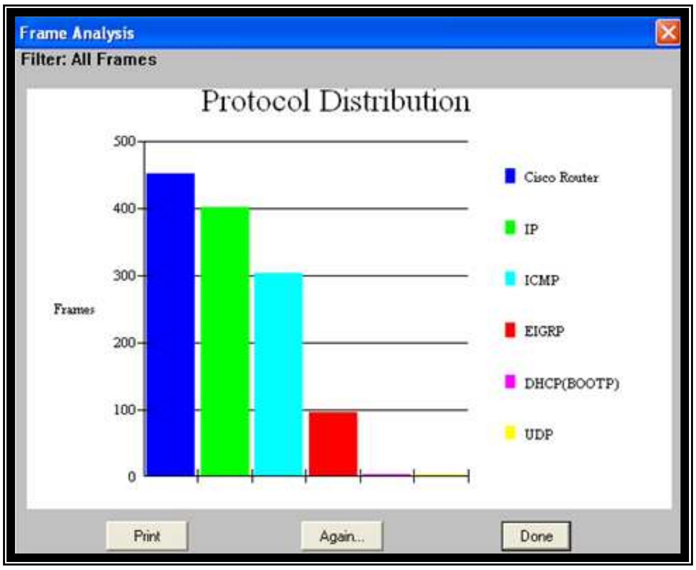
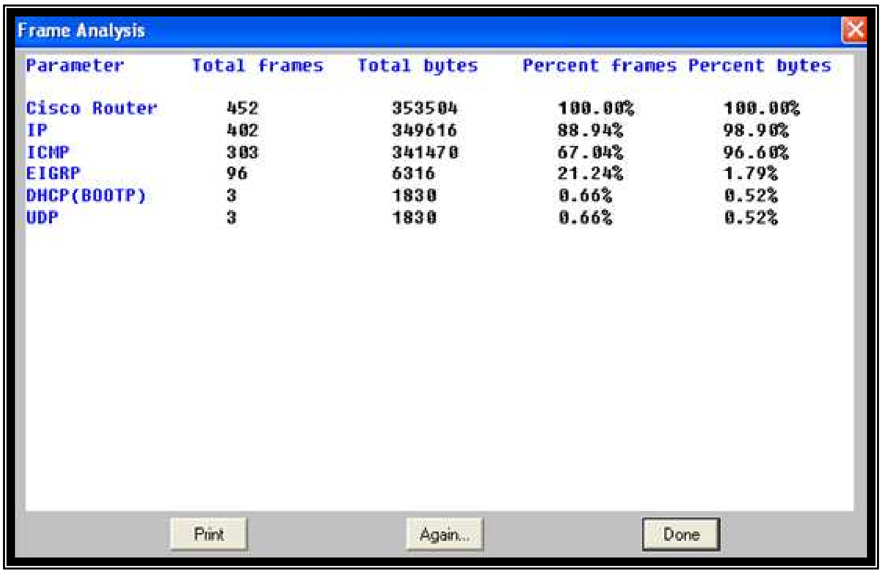



**Figura 4.3.22** Distribución de protocolos (1)




| Parameter | Total frames | Total bytes | Percent frames | Percent bytes |
|---|---|---|---|---|
| Cisco Router | 452 | 353504 | 100.00% | 100.00% |
| IP | 402 | 349616 | 88.94% | 98.90% |
| ICMP | 303 | 341470 | 67.04% | 96.60% |
| EIGRP | 96 | 6316 | 21.24% | 1.79% |
| DHCP(BOOTP) | 3 | 1830 | 0.66% | 0.52% |
| UDP | 3 | 1830 | 0.66% | 0.52% |



**Figura 4.3.23** Distribución de protocolos (2)

## 4.4.- Práctica de Laboratorio de Simulación de Ethernet (Mac), IP

### 4.4.1.- Descripción general

Esta práctica permite que el estudiante se familiarice con la estructura de la trama Ethernet, la descripción de los campos; además se detallará con ejemplos la estructura de la cabecera IP.

### 4.4.2.- Equipos requeridos

- ✓ Dos ruteadores Cisco con una interfaz Ethernet y una interfaz serial.
- ✓ Un Hub.
- ✓ Dos computadores con tarjeta de red y puerto serie
- ✓ Un Analizador Radcom Rc-100wl con la interfaz Multitype (canal 1) con su cable monitor V.35 y la interfaz Ethernet (canal 2); además necesitamos tener instalado el software del equipo en un computador.

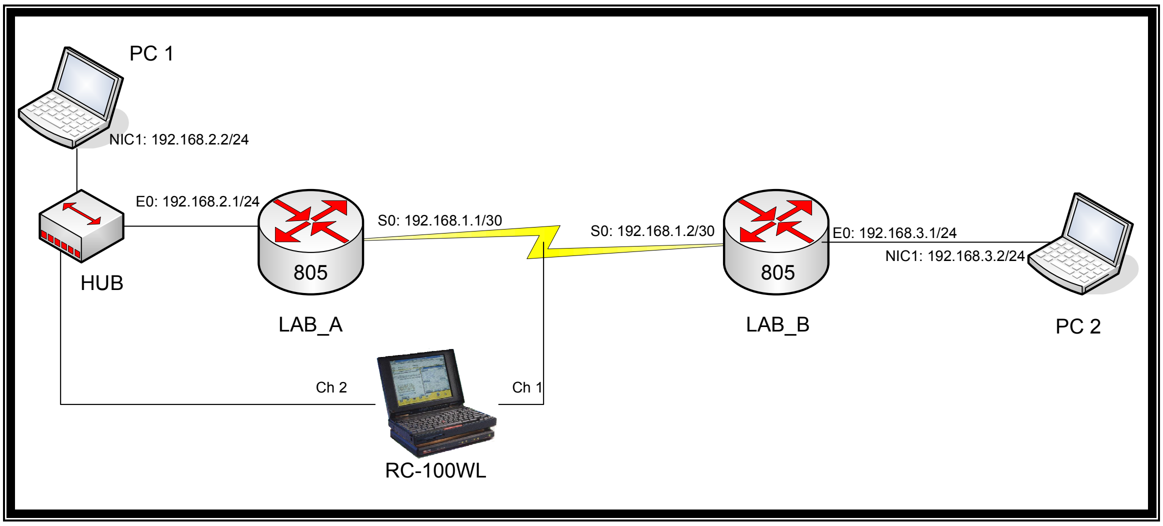



**Figura 4.4.1** Diagrama de red

### 4.4.3.- Descripción del contenido de la práctica.

Para el análisis de las tramas Ethernet e IP se basará en la configuración de los equipos como se detalla en la práctica HDLC.

Se capturan las tramas con el analizador de Protocolos Radcom Rc-100wl, se analizará la estructura de la trama Ethernet y la cabecera IP.

### 4.4.4.- Desarrollo de la práctica

#### 4.4.4.1.- Captura de la trama Ethernet

Para capturar la estructura de la trama, se procederá a utilizar el analizador de protocolos RC-100WL en el canal 2 como se observa en la **figura 4.4.1**.

**Paso 1: Ejecutar el programa RC-100WL**

Activar solo la interfaz Ethernet, en working mode, se seleccionara Monitor. Luego OK.

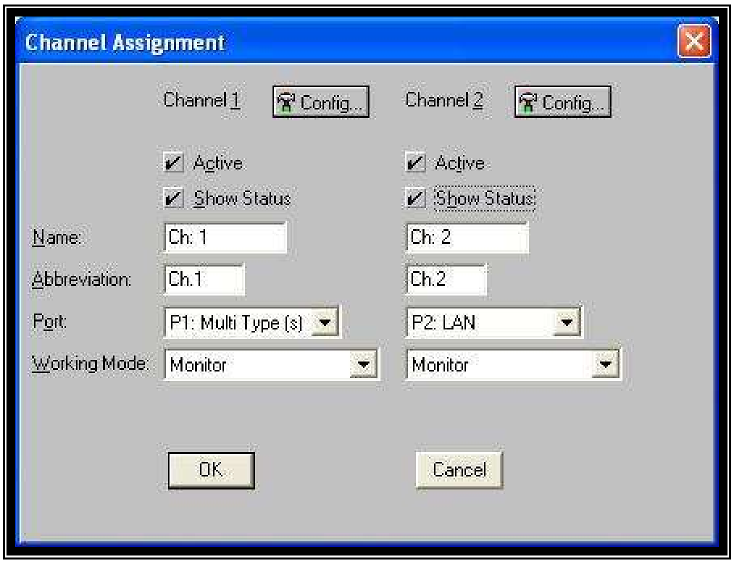



**Figura 4.4.2** Asignación de canales

**Paso 2: Seleccionar el protocolo utilizado**

En el menú "Channel Assigment" seleccionar en CH 2 "Config" para seleccionar el protocol stack seleccionar Ethernet como se detalla en la **figura 4.4.3**.

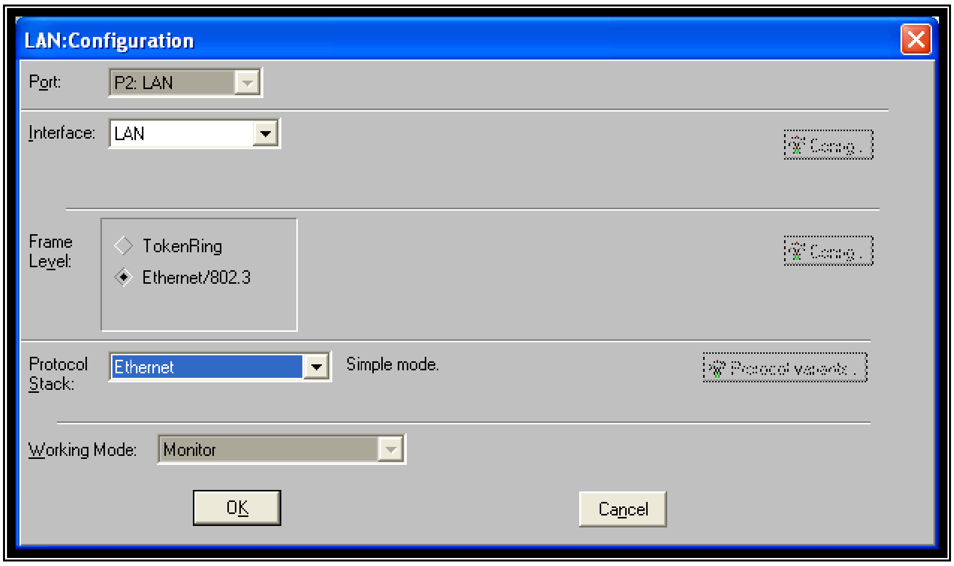



**Figura 4.4.3** Configuración Lan

**Paso 3: Ingresar las direcciones MAC de los equipos**

En el menú "System", seleccionar la opción "Station Names" como se muestra en la siguiente **figura 4.4.4**:

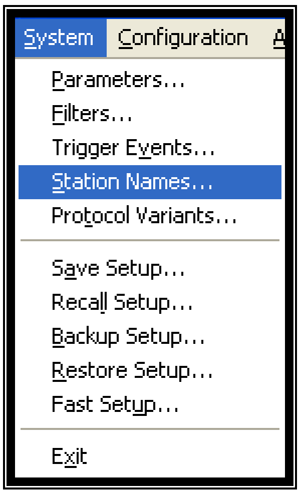



**Figura 4.4.4** Configuración de nombres de equipos

En la ventana “Station Names” seleccionar protocolo Ethernet, luego se ingresa el nombre del equipo y la dirección Mac de este, realizar este paso para cada equipo en la red, ver **figura 4.4.5**. Esto nos permite identificar en el momento de análisis de manera rápida que equipo está enviando o recibiendo tramas Ethernet.

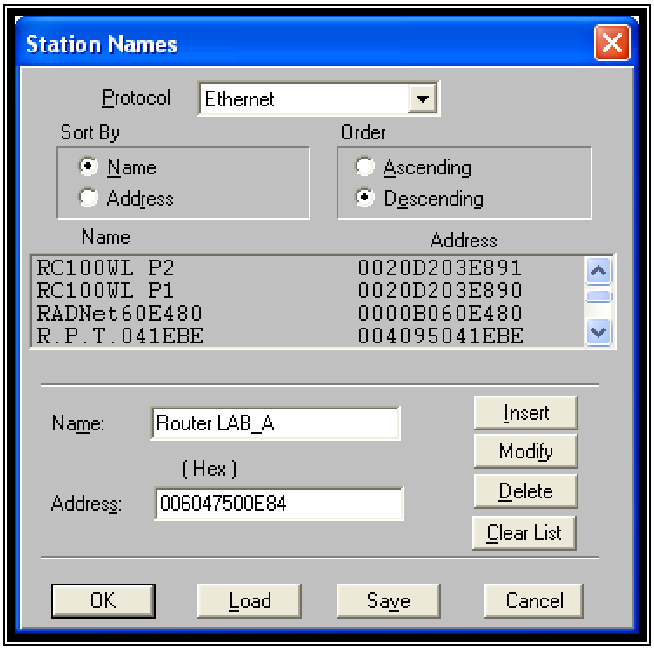



**Figura 4.4.5** Configuración de nombres de equipos (2)

**Paso 3: Capturar las tramas**

Hay que seleccionar la ventana de captura para poder iniciarla; para esto procedemos en el menú Window seleccionar Ch 2: capture, ver **figura 4.4.6**.

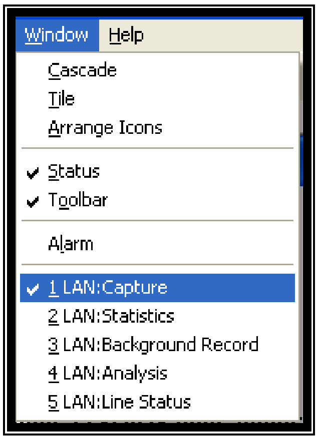



**Figura 4.4.6** Visualizar la ventana de captura

Posteriormente en la ventana Ch2: Capture se da clic en Go para empezar la captura de tramas en la interfaz Ethernet.

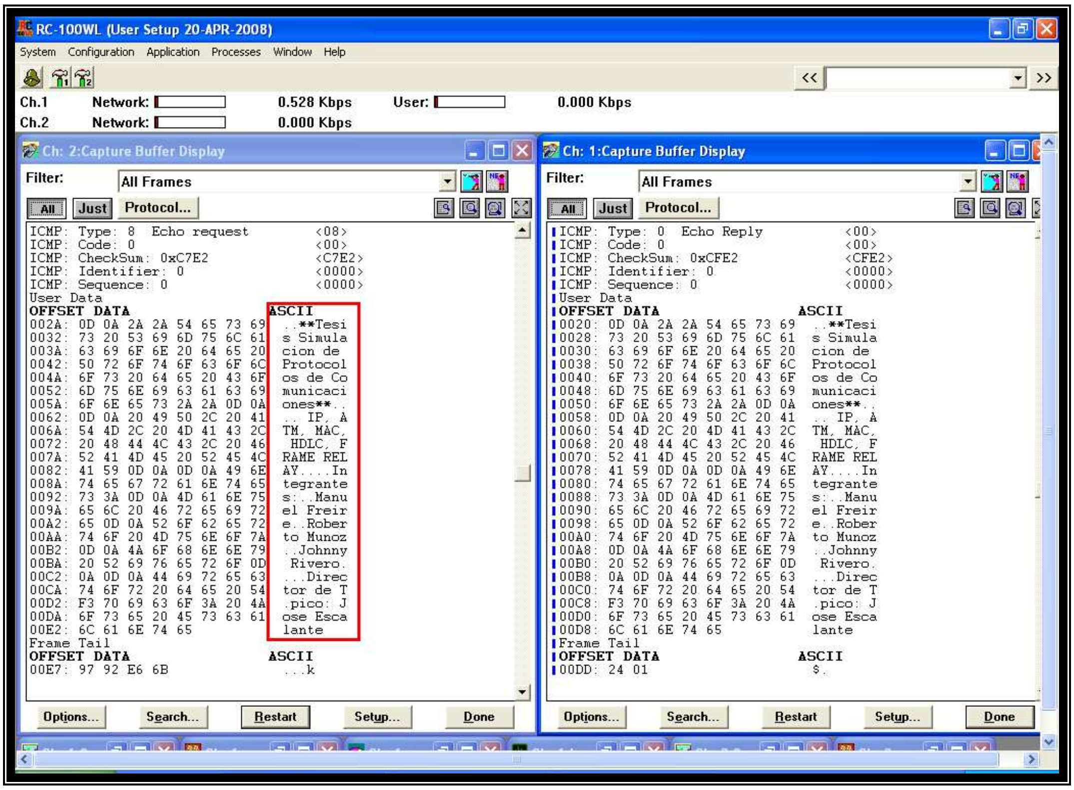



**Figura 4.4.7** Ventana de captura

Luego para finalizar la captura se procederá a dar clic en el botón Stop y se obtienen las tramas como se muestra en la **figura 4.4.7**.

#### 4.4.4.5.- Análisis de la trama Ethernet

Una vez capturada las tramas se procederá a realizar el análisis correspondiente.

##### 4.4.4.5.1.- Análisis de la trama 0

Al encender los equipos el ruteador LabA solo conoce su dirección mac y su dirección ip, como se observa en la trama capturada en la **tabla 4.4.1**, el router Lab A envía un broadcast por el puerto Ethernet, para publicar su dirección ip y mac.

**Tabla 4.4.1** Trama 0

```
Frame: 0 Captured at:  +00:00.000
Length: 64    Status: Ok
Ethernet: Destination Address Broadcast   <FFFFFFFFFFFF>
Ethernet:   Group Address
Ethernet:   Local Address
Ethernet: Source Address 006047500E84  <006047500E84>
Ethernet:   Universally Address
Ethernet: Ethernet V.2, Type ARP (for IP and for CHAOS)   <0806>
ARP/RARP: Hardware Type is Ethernet   <0001>
ARP/RARP: Protocol Type is DOD IP   <0800>
ARP/RARP: Hardware Length = 6      <06>
ARP/RARP: Protocol Length = 4      <04>
ARP/RARP: Operation is ARP Response   <0002>
ARP/RARP: Sender HAddress LAB_A  <006047500E84>
ARP/RARP: Sender PAddress 192.168.2.1  <C0A80201>
ARP/RARP: Target HAddress Broadcast   <FFFFFFFFFFFF>
ARP/RARP: Target PAddress 192.168.2.1  <C0A80201>
User Data
OFFSET DATA                                       ASCII
002A: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003A: 00 00 9F DB 9D A1
```

En la trama 0 se puede notar que el campo del tipo de protocolo en la trama Ethernet es ethertype: 0x806, que es ARP. El protocolo ARP (RFC826) es utilizado parar inicializar el uso del direccionamiento IP en un medio Ethernet. Esta trama en los equipos de comunicaciones es conocida como ARP gratuito dado a que es enviado a cualquier equipo en la red.

En la siguiente trama en la **tabla 4.4.2** correspondiente al lab_A la dirección destino 01000CCCCCCC corresponde a una dirección mac multicast del protocolo Cisco CDP, este protocolo es para descubrimiento de equipos Cisco en la red; aunque en la actualidad lo utilizan muchos fabricantes de equipos de comunicaciones con el mismo fin.

**Tabla 4.4.2** Trama 3

```
Frame: 3 Captured at:  +00:00.184
Length: 308    Status: Ok
Ethernet: Destination Address 01000CCCCCCC  <01000CCCCCCC>
Ethernet:   Group Address
Ethernet:   Universally Address
Ethernet: Source Address LAB_A  <006047500E84>
Ethernet:   Universally Address
Ethernet: 802.3, Length = 290 [Bytes]  <0122>
LLC: DSAP= (SNAP ), Individual SAP   <AA>
LLC: SSAP= (SNAP ), Command         <AA>
LLC: Unnumbered   UI  , Poll        <03>
LLC:                                <00>
LLC: Protocol:SNAP
SNAP: OUI: Cisco Protocols 0x00000C  <00000C>
SNAP: Protocol: 8192 Cisco Discovery (CDP)   <2000>
CDP: Version: 2                     <02>
CDP: Time To Live: 180 (sec)        <B4>
CDP: Checksum: 46275                <B4C3>
CDP: TLV - 1
CDP: Variable Type: 1 Device ID     <0001>
CDP: Length = 9                     <0009>
CDP: Device Id: LAB_A....           <4C41425F41000500D4>
CDP: TLV - 2
CDP: Variable Type: 17257 Unknown    <4369>
CDP: Length = 29539                 <7363>
User Data
OFFSET DATA                                        ASCII
```

```
002B: 6F 20 49 6E 74 65 72 6E 65 74 77 6F 72 6B 20 4F  o Internetwork O
003B: 70 65 72 61 74 69 6E 67 20 53 79 73 74 65 6D 20  perating System
004B: 53 6F 66 74 77 61 72 65 20 0A 49 4F 53 20 28 74  Software .IOS (t
005B: 6D 29 20 31 36 30 30 20 53 6F 66 74 77 61 72 65  m) 1600 Software
006B: 20 28 43 31 36 30 30 2D 59 2D 4C 29 2C 20 56 65   (C1600-Y-L), Ve
007B: 72 73 69 6F 6E 20 31 32 2E 32 28 31 37 61 29 2C  rsion 12.2(17a),
008B: 20 52 45 4C 45 41 53 45 20 53 4F 46 54 57 41 52   RELEASE SOFTWAR
009B: 45 20 28 66 63 31 29 0A 43 6F 70 79 72 69 67 68  E (fc1).Copyrigh
00AB: 74 20 28 63 29 20 31 39 38 36 2D 32 30 30 33 20  t (c) 1986-2003
00BB: 62 79 20 63 69 73 63 6F 20 53 79 73 74 65 6D 73  by cisco Systems
00CB: 2C 20 49 6E 63 2E 0A 43 6F 6D 70 69 6C 65 64 20  , Inc..Compiled
00DB: 54 68 75 20 31 39 2D 4A 75 6E 2D 30 33 20 31 30  Thu 19-Jun-03 10
00EB: 3A 31 32 20 62 79 20 70 77 61 64 65 00 06 00 0E  :12 by pwade....
00FB: 63 69 73 63 6F 20 31 36 30 31 00 02 00 11 00 00  cisco 1601......
010B: 00 01 01 01 CC 00 04 C0 A8 02 01 00 03 00 0D 45  ...............E
011B: 74 68 65 72 6E 65 74 30 00 04 00 08 00 00 00 01  thernet0........
012B: 00 0B 00 05 00 31 0D 83 42                       .....1..B
```

En la siguiente trama 4 que se muestra en la **tabla 4.4.3** correspondiente al Lab_A la dirección destino 01005E00000A corresponde a una dirección mac multicast del protocolo de enrutamiento EIGRP. La cual se puede confirmar con la ip destino 224.0.0.10 que corresponde a una ip multicast del protocolo de enrutamiento.

**Tabla 4.4.3** Trama 4

```
Frame: 4 Captured at:  +00:00.228
Length: 78    Status: Ok
Ethernet: Destination Address 01005E00000A  <01005E00000A>
Ethernet:   Group Address
Ethernet:   Universally Address
Ethernet: Source Address 006047500E84  <006047500E84>
Ethernet:   Universally Address
Ethernet: Ethernet V.2, Type DOD IP   <0800>
IP: Version = 4                     <45>
IP: IHL = 20 [Bytes]
IP: Type of Service: 0xC0           <C0>
IP:   Internet Control
IP:   Normal Delay
IP:   Normal Throughput
IP:   Normal Reliability
IP: Total Length = 60               <003C>
IP: Identification = 0              <0000>
IP: Flags & Fragment Offset: 0x0000  <0000>
IP:   0............... Reserved
IP:   .0.............. May Fragment
IP:   ..0............. Last Fragment
```

```
IP:   Fragment Offset = 0 [Bytes]
IP: Time to Live = 2 [Seconds/Hops]  <02>
IP: Protocol: 88 IGRP/EIGRP        <58>
IP: Header Checksum = 0x14F7       <14F7>
IP: Source Address = 192.168.2.1   <C0A80201>
IP: Destination Address = 224.0.0.10  <E000000A>
EIGRP: Version: 2                  <02>
EIGRP: Opcode: 5 Hello             <05>
EIGRP: Checksum: 0xEECD            <EECD>
EIGRP: Falgs: 0x00000000 Conditional recieve   <00000000>
EIGRP: Sequence number: 0x00000000   <00000000>
EIGRP: Acknowledge number: 0x00000000   <00000000>
EIGRP: Autonomous System Number : 0x00000001   <00000001>
EIGRP: Variable Type: 0x0001 EIGRP Parameters   <0001>
EIGRP: Variable Length: 12         <000C>
EIGRP: K1: 1                       <01>
EIGRP: K2: 0                       <00>
EIGRP: K3: 1                       <01>
EIGRP: K4: 0                       <00>
EIGRP: K5: 0                       <00>
EIGRP: Reserved: 0                 <00>
EIGRP: Hold Time: 15               <000F>
User Data
OFFSET DATA                                      ASCII
0042: 00 04 00 08 0C 02 01 02                         ........
Frame Tail
OFFSET DATA                                      ASCII
004A: C3 84 E6 AD                                     ....
```

En la siguiente **tabla 4.4.4** en el análisis ethernet la dirección fuente con mac 001E8CFBACE8 correspondiente a la PC 1 envía tramas ICMP a la mac destino 006047500E84 correspondiente al router Lab A.

En el análisis IP la dirección fuente 192.168.2.1 (PC 1) envía tramas icmp a la ip destino 192.168.2.2 La PC 1 conoce la IP y la MAC destino debido a que el router Lab A publico su IP y su MAC.

**Tabla 4.4.4** Trama 40

```
Frame: 40 Captured at:  +00:27.899
Length: 78    Status: Ok
Ethernet: Destination Address LAB_A <006047500E84>
Ethernet:   Individual Address
Ethernet:   Universally Address
```

```
Ethernet: Source Address PC1 <001E8CFBACE8>
Ethernet:   Universally Address
Ethernet: Ethernet V.2, Type DOD IP   <0800>
IP: Version = 4                      <45>
IP: IHL = 20 [Bytes]
IP: Type of Service: 0x00            <00>
IP:   Routine
IP:   Normal Delay
IP:   Normal Throughput
IP:   Normal Reliability
IP: Total Length = 60                <003C>
IP: Identification = 12837           <3225>
IP: Flags & Fragment Offset: 0x0000  <0000>
IP:   0............... Reserved
IP:   .0.............. May Fragment
IP:   ..0............. Last Fragment
IP:   Fragment Offset = 0 [Bytes]
IP: Time to Live = 128 [Seconds/Hops]  <80>
IP: Protocol: 1 ICMP                 <01>
IP: Header Checksum = 0x8348         <8348>
IP: Source Address = 192.168.2.2     <C0A80202>
IP: Destination Address = 192.168.2.1  <C0A80201>
ICMP: Type: 8  Echo request          <08>
ICMP: Code: 0                        <00>
ICMP: CheckSum: 0x9E5B               <9E5B>
ICMP: Identifier: 512                <0200>
ICMP: Sequence: 44288                <AD00>
User Data
OFFSET DATA                                       ASCII
002A: 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
003A: 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
Frame Tail
OFFSET DATA                                       ASCII
004A: DD D1 73 41                                      ..sA
```

El ruteador Lab_A recibe tramas ICMP del host PC1, pero el ruteador no conoce su dirección MAC por lo tanto envía una trama ARP request solicitando la MAC destino, conociendo la dirección IP fuente, ver **tabla 4.4.5**.

**Tabla 4.4.5** Trama 41

```
Frame: 41 Captured at:  +00:27.902
Length: 64    Status: Ok
Ethernet: Destination Address Broadcast   <FFFFFFFFFFFF>
Ethernet:   Group Address
Ethernet:   Local Address
Ethernet: Source Address LAB_A  <006047500E84>
```

```
Ethernet:   Universally Address
Ethernet: Ethernet V.2, Type ARP (for IP and for CHAOS)   <0806>
ARP/RARP: Hardware Type is Ethernet   <0001>
ARP/RARP: Protocol Type is DOD IP   <0800>
ARP/RARP: Hardware Length = 6      <06>
ARP/RARP: Protocol Length = 4      <04>
ARP/RARP: Operation is ARP Request   <0001>
ARP/RARP: Sender HAddress 006047500E84  <006047500E84>
ARP/RARP: Sender PAddress 192.168.2.1  <C0A80201>
ARP/RARP: Target HAddress 000000000000  <000000000000>
ARP/RARP: Target PAddress 192.168.2.2  <C0A80202>
User Data
OFFSET DATA                                        ASCII
002A: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003A: 00 00 86 36 DB DC                                 ...6..
```

La PC 1 le envía una ARP reply  para publicar su dirección MAC al ruteador Lab_A, ver **tabla 4.4.6**.

**Tabla 4.4.6** Trama 42

```
Frame: 0 Captured at:  +00:27.902
Length: 64    Status: Ok
Ethernet: Destination Address LAB_A  <006047500E84>
Ethernet:   Individual Address
Ethernet:   Universally Address
Ethernet: Source Address PC1  <001E8CFBACE8>
Ethernet:   Universally Address
Ethernet: Ethernet V.2, Type ARP (for IP and for CHAOS)   <0806>
ARP/RARP: Hardware Type is Ethernet   <0001>
ARP/RARP: Protocol Type is DOD IP   <0800>
ARP/RARP: Hardware Length = 6      <06>
ARP/RARP: Protocol Length = 4      <04>
ARP/RARP: Operation is ARP Response   <0002>
ARP/RARP: Sender HAddress 001E8CFBACE8  <001E8CFBACE8>
ARP/RARP: Sender PAddress 192.168.2.2  <C0A80202>
ARP/RARP: Target HAddress 006047500E84  <006047500E84>
ARP/RARP: Target PAddress 192.168.2.1  <C0A80201>
User Data
OFFSET DATA                                        ASCII
002A: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003A: 00 00 8E D1 F9 32                                 .....2
```

### 4.4.4.5.2.- Análisis de la red

La **tabla 4.4.7** detalla una trama Ethernet, esta ha sido organizada en campos para visualizar estos. Donde la dirección destino es tipo broadcast y la dirección fuente es tipo unicast, específicamente el router LAB_A. Según el campo Tipo/longitud 0x0806 se reconoce que se utiliza el protocolo ARP.

**Tabla 4.4.7**Trama 0

<table>
<tr><td colspan="7">PREAMBULO</td><td>SFD</td></tr>
<tr><td>AA</td><td>AA</td><td>AA</td><td>AA</td><td>AA</td><td>AA</td><td>AA</td><td>AB</td></tr>
<tr><td colspan="6">DIRECCIÓN DESTINO</td><td colspan="2">DIRECCIÓN F</td></tr>
<tr><td>FF</td><td>FF</td><td>FF</td><td>FF</td><td>FF</td><td>FF</td><td>00</td><td>60</td></tr>
<tr><td colspan="4">DIRECCION FUENTE</td><td colspan="2">TIPO/LONGITUD</td><td colspan="2">TIPO HARDWARE</td></tr>
<tr><td>47</td><td>50</td><td>0E</td><td>84</td><td>08</td><td>06</td><td>00</td><td>01</td></tr>
<tr><td colspan="2">TIPO PROTOCOLO</td><td>L.H.</td><td>L.P.</td><td colspan="2">OPERATION</td><td colspan="2">D.H.F.</td></tr>
<tr><td>08</td><td>00</td><td>06</td><td>04</td><td>00</td><td>01</td><td>00</td><td>60</td></tr>
<tr><td colspan="4">D.H.F.</td><td colspan="4">D.P.F.</td></tr>
<tr><td>47</td><td>50</td><td>0E</td><td>84</td><td>C0</td><td>A8</td><td>02</td><td>01</td></tr>
<tr><td colspan="6">D.H.D.</td><td colspan="2">D.P.D.</td></tr>
<tr><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>C0</td><td>A8</td></tr>
<tr><td colspan="2">D.P.D.</td><td colspan="6">DATOS OFFSET</td></tr>
<tr><td>02</td><td>02</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td></tr>
<tr><td colspan="8">DATOS OFFSET</td></tr>
<tr><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td><td>00</td></tr>
<tr><td colspan="4">DATOS OFFSET</td><td colspan="4">FCS</td></tr>
<tr><td>00</td><td>00</td><td>00</td><td>00</td><td>86</td><td>36</td><td>DB</td><td>DC</td></tr>
</table>

A continuación se detalla los campos abreviados:

L.H. = Longitud de dirección de hardware

L.P. = Longitud de dirección de protocolo de capa superior.

D.H.F. = Dirección de hardware fuente

D.P.F. = Dirección de protocolo fuente

D.H.D. = Dirección de hardware destino

D.P.D. = Dirección de protocolo destino

Como se puede observar en la tabla anterior se la realizó en base a los detalles que proporciona el equipo Radcom.

El software tiene ventajas adicionales dado a que muestra los campos de una forma ordenada y detallada de cada protocolo que se encuentra adquirido en la licencia del software.

A continuación en la **figura 4.4.8** un ejemplo de la decodificación de la trama en el software Radcom. Se muestran dos ventanas, la captura del canal 1 que se encuentra conectado a la interfaz serial y la captura del canal 2 que se encuentra en un hub.

El software soporta realizar varios tipos de análisis definidos, entre estos tenemos análisis de tramas Ethernet, protocolo ICMP, IP, Estadísticas a nivel LAN y distribución de protocolos. A continuación se detallan los pasos para realizar los análisis anteriormente descritos.

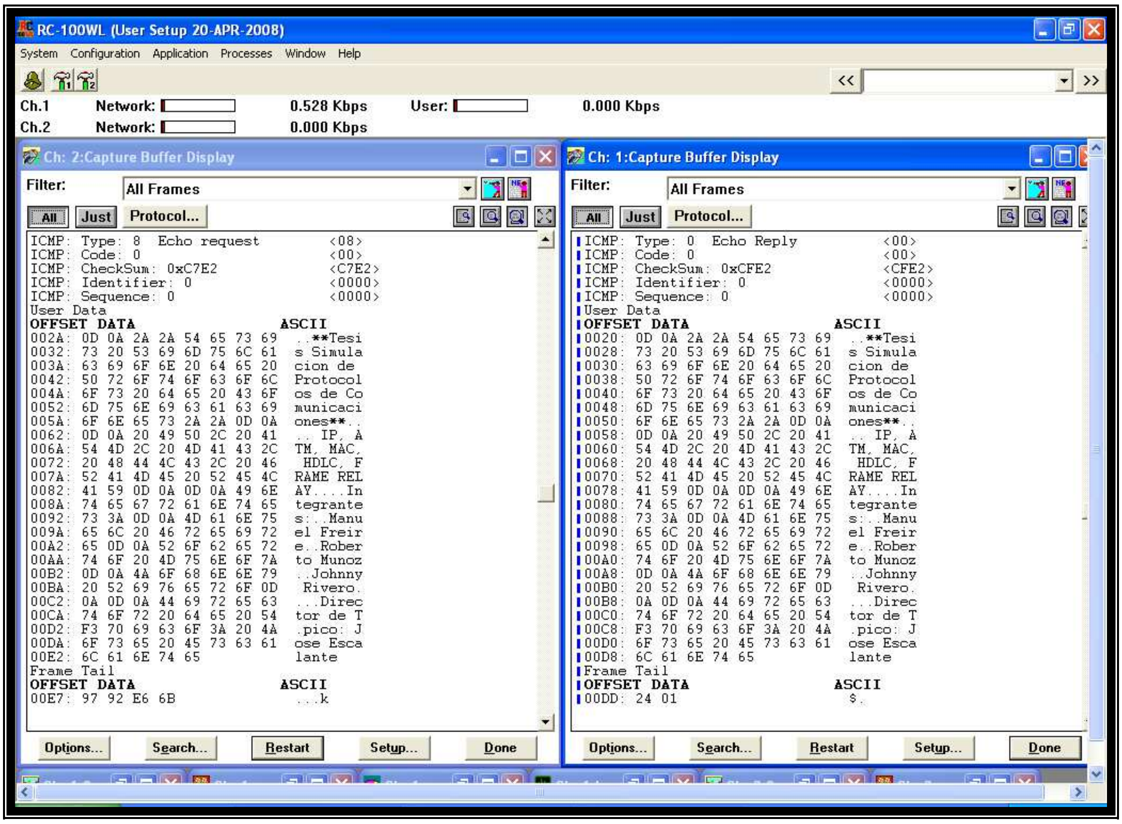



**Figura 4.4.8** Ventana de captura del software Radcom

### Paso 1: Análisis Ethernet

Para realizar el análisis pre-definido se debe hacer click derecho en la pantalla del analizador, y aparecerá una lista desplegable con varias opciones, se escoge análisis. Además seleccionamos en la nueva ventana Ethernet y en análisis se tienen varias opciones detalladas a continuación, ver **figura 4.4.9**:

- Distribución por tipo.
- Actividad de tráfico de red (Ethernet).

- Distribución de tráfico por dirección destino.
- Distribución de tráfico por dirección fuente.

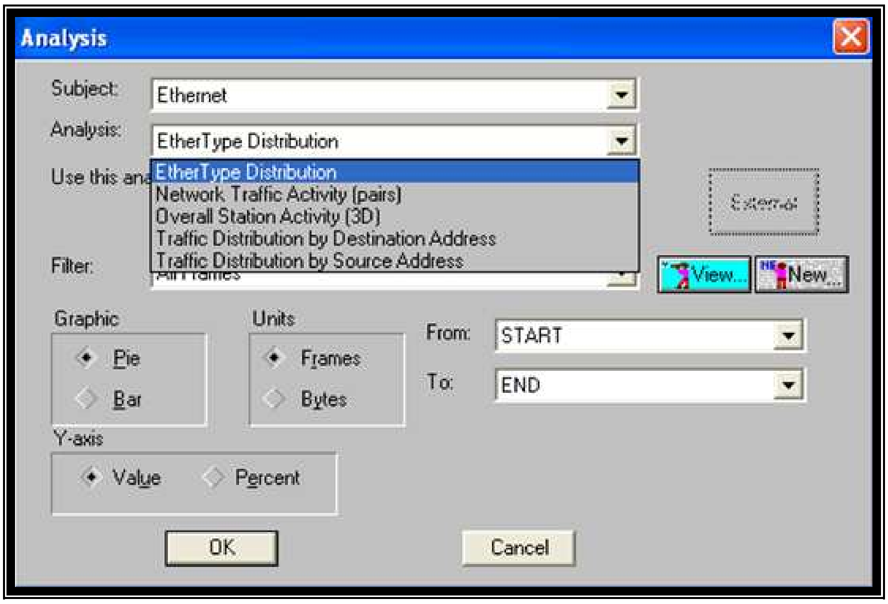



**Figura 4.4.9** Análisis Ethernet

**Distribución por tipo.** Estas estadísticas son obtenidas desde el campo tipo/longitud de la trama Ethernet. Como se comprueba en la **figura 4.4.10** se han capturado 576 tramas Ethernet, de las cuales; 548 corresponde al protocolo de red IP, 4 a las resoluciones ARP y 20 a las tramas loopback que envían los ruteadores para comprobar que sus interfaces están activas. Además se debe incluir 4 tramas con protocolo de Cisco CDP.

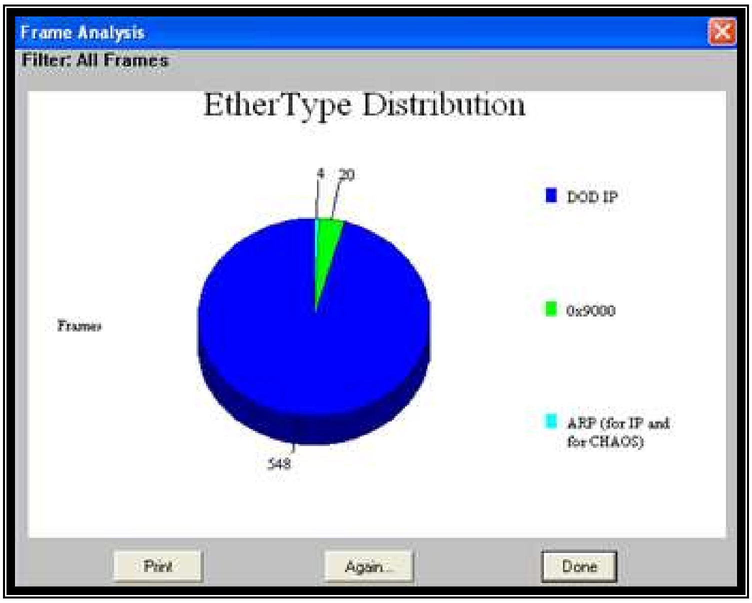



**Figura 4.4.10** Análisis por distribución por campo tipo

**Actividad de tráfico de red.** La **figura 4.4.11** indica la tabla de la actividad de tráfico entre par de direcciones MAC.

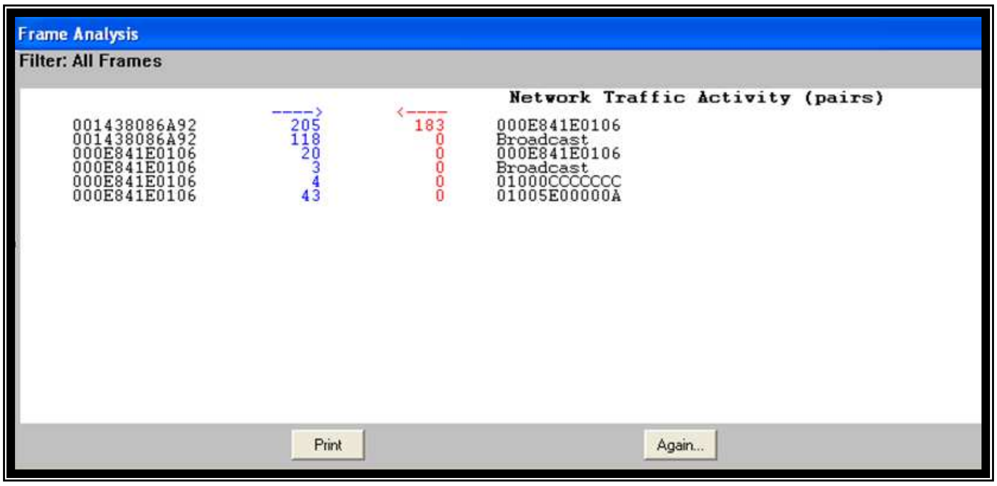



**Figura 4.4.11** Actividad de tráfico de red

En la **figura 4.4.12** se han asociado la dirección MAC con la de cada equipo.

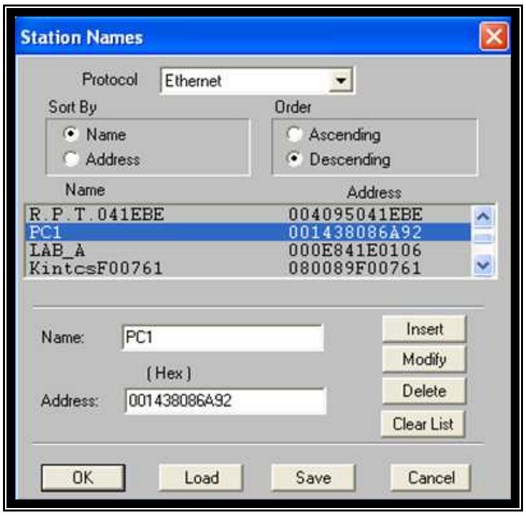



**Figura 4.4.12** Asociación de dirección MAC a equipo

En la **figura 4.4.13** observa la actividad de tráfico en la red pero asociado a cada equipo. Esta muestra que el equipo PC1 ha enviado 183 tramas Ethernet a LAB_A. El ruteador LAB_A ha enviado 4 tramas a la dirección multicast "01000CCCCCCC" que corresponde al protocolo CDP y 43 tramas a la dirección multicast "01005E00000A" que corresponde al protocolo de enrutamiento EIGRP.

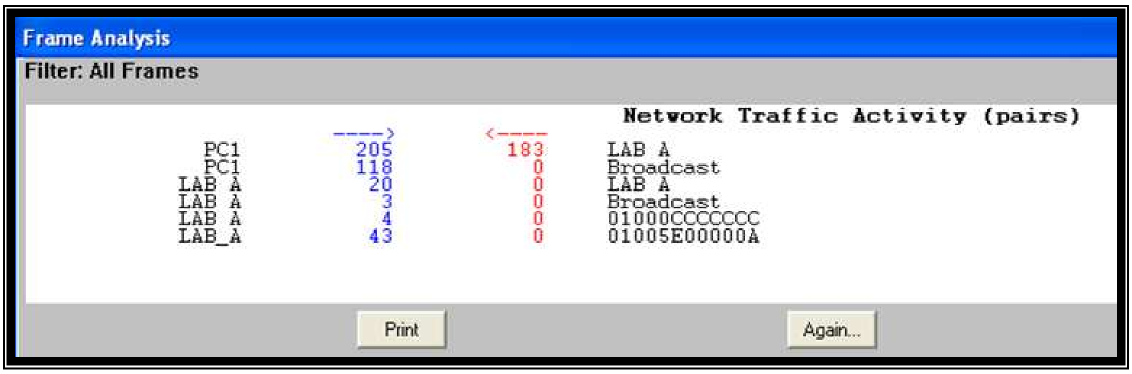



**Figura 4.4.13** Actividad de tráfico de red (2)

**Distribución de tráfico por dirección destino.** En la **figura 4.4.14** se puede observar que la dirección MAC del ruteador LAB_A ha recibido 225 tramas mientras que el equipo PC1 ha recibido 183 tramas.

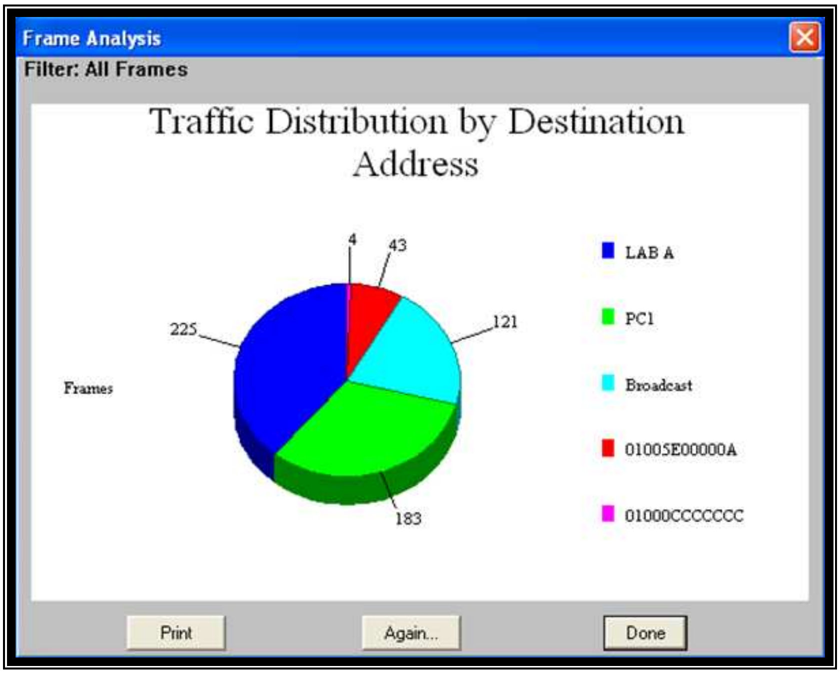



**Figura 4.4.14** Distribución de Tráfico por dirección MAC destino

**Distribución de tráfico por dirección fuente.** En la **figura 4.4.15** se observa que la dirección fuente MAC solo pueden ser direcciones unicast. Se detalla que 323 tramas han sido enviadas por el equipo PC1 y 253 tramas han sido enviadas por el ruteador LAB_A.

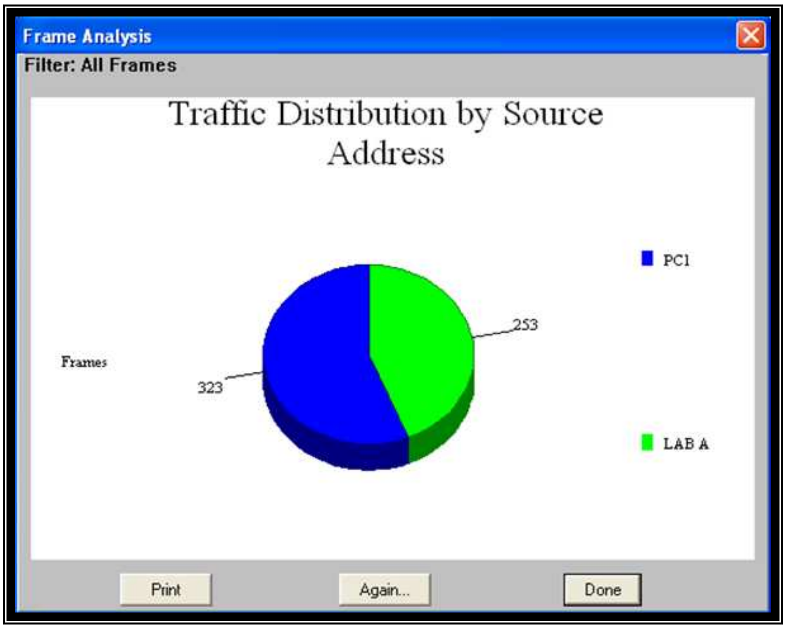



**Figura 4.4.15** Distribución de Tráfico por dirección MAC fuente

**Paso 2: Análisis de las tramas ICMP**

Para realizar el análisis pre-definido como en la **figura 4.4.9** se escoge ICMP y en análisis distribución por tipo.

**Distribución por tipo.** Se muestra la **figura 4.4.16** con el análisis de distribución por tipo de las tramas ICMP. Esta figura recoge estadísticas desde el campo tipo dentro de la cabecera ICMP, en este caso en particularse se tienen 67 tramas tipo=0x08 petición de eco, 57 tramas de tipo =0x00 respuesta de eco, 26 como tipo=0x03 destino no alcanzado.

Además se observan otros tipos no válidos como tipo= 97, 105, 113, 98, 106, 114 y otros, estos se observan cuando el paquete ICMP se fragmenta debido a su tamaño.

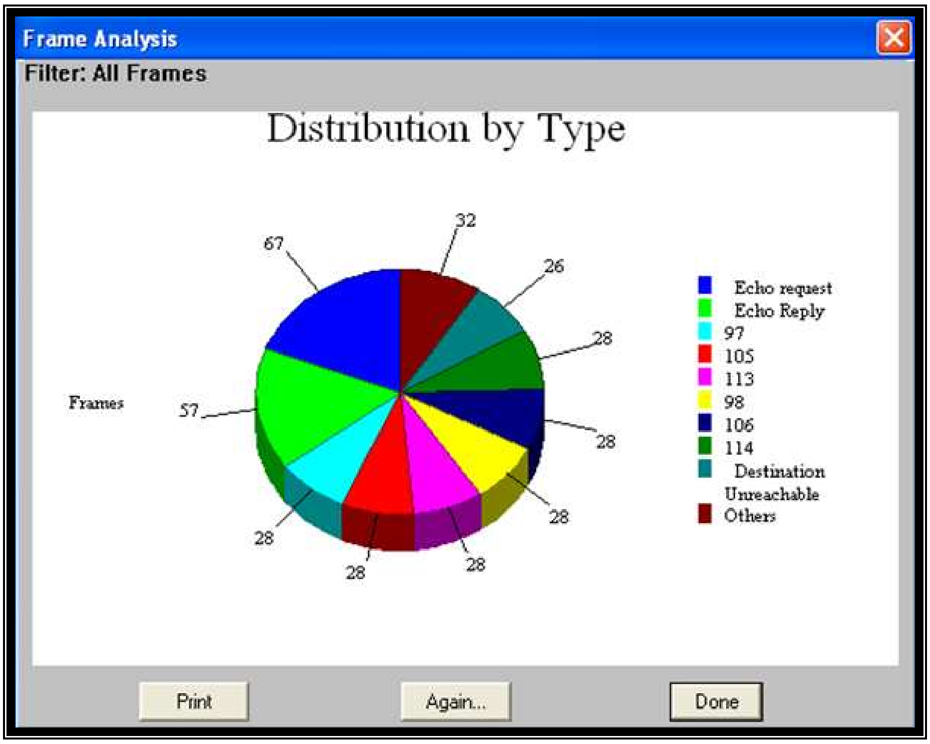



**Figura 4.4.16** Análisis por ICMP

**Paso 3: Análisis de la trama IP**

Se tienen varias opciones relacionadas con el campo tipo de servicio en la cabecera IP y estadísticas de la actividad de tráfico que se detallan a continuación:

- Retardo (Delay).

- Precedencia (Precedence).
- Fiabilidad (Reliability).
- Rendimiento (Throughput).
- Actividad de tráfico de red (tráfico entre pares).
- Distribución de Tráfico por dirección destino.
- Distribución de Tráfico por dirección fuente.
- Distribución por protocolo.

**Retardo.** Estas estadísticas son obtenidas desde el campo tipo de servicio en la cabecera IP. Se observa que todos los paquetes IP tienen seteado retardo normal como se muestra en la **figura 4.4.17**. Además se comprueba la cantidad de paquetes con la **figura 4.4.10**.

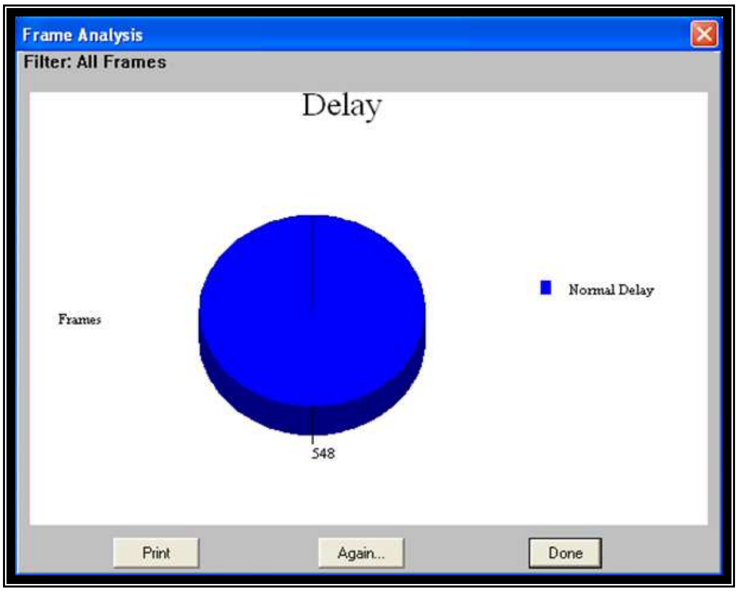



**Figura 4.4.17** Análisis por Retardo

**Precedencia.** En la **figura 4.4.18** se observan 505 paquetes de tipo rutina y 43 de tipo control de Internet, se debe tener en cuenta que control de Internet tiene mayor prioridad y es usado por los protocolos de enrutamiento.

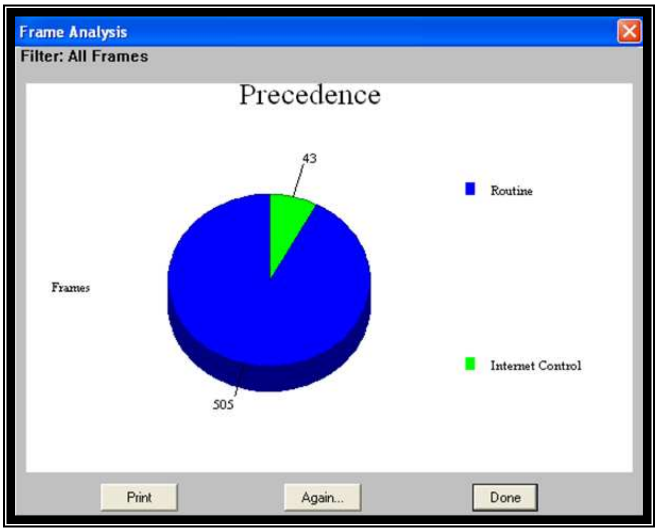



**Figura 4.4.18** Análisis por Precedencia

**Fiabilidad.** Se observa que todos los 548 paquetes IP tienen el campo Fiabilidad=normal como se muestra en la **figura 4.4.19**.

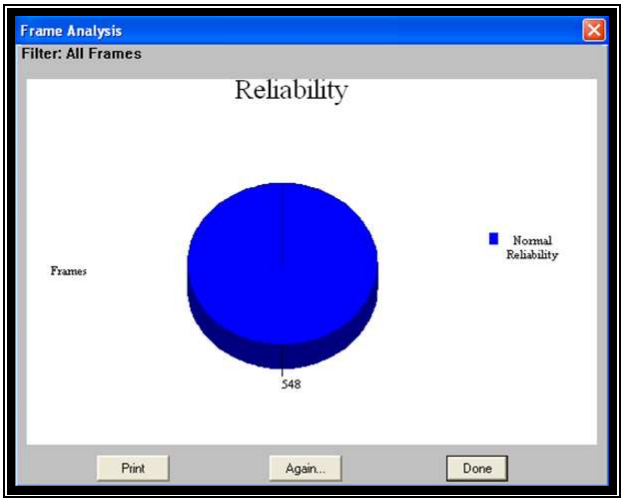



**Figura 4.4.19** Análisis por Fiabilidad

**Rendimiento.** Se observa que todos los paquetes IP tiene un rendimiento normal como se muestra en la **figura 4.4.20**.

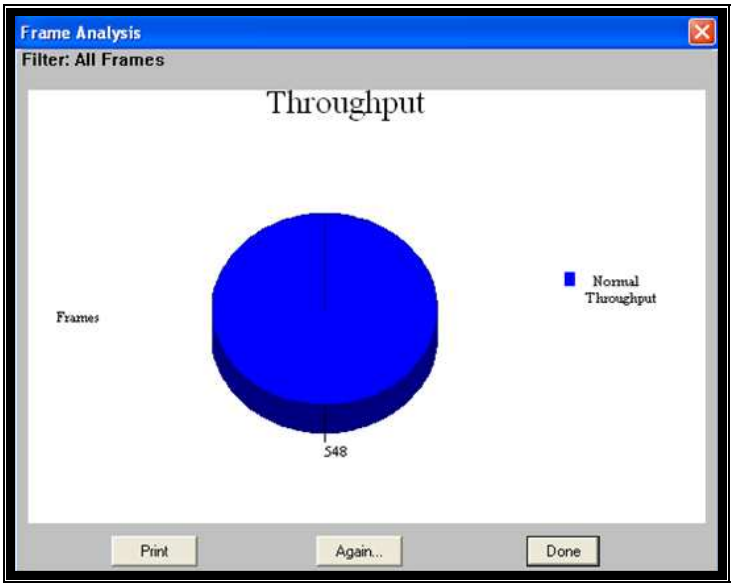



**Figura 4.4.20** Análisis por Rendimiento

**Actividad de tráfico de red (tráfico entre pares).** La **figura 4.4.21** muestra la tabla de la actividad de tráfico entre direcciones IP con un total de 548 tramas que contienen la cabecera IP.

El Host 192.168.2.2 ha enviado 147 paquetes a la dirección 192.168.3.2 y ha recibido 140 paquetes.

El Host 192.168.2.2 ha enviado 8 paquetes a la dirección 192.168.2.1 y ha recibido 31 paquetes.

Además el equipo PC1 (IP: 192.168.2.2) ha enviado paquetes a varias direcciones IP públicas como 75.126.38.75, 75.126.38.76, 190.95.185.98, 190.95.185.99 7 216.12.205.130.

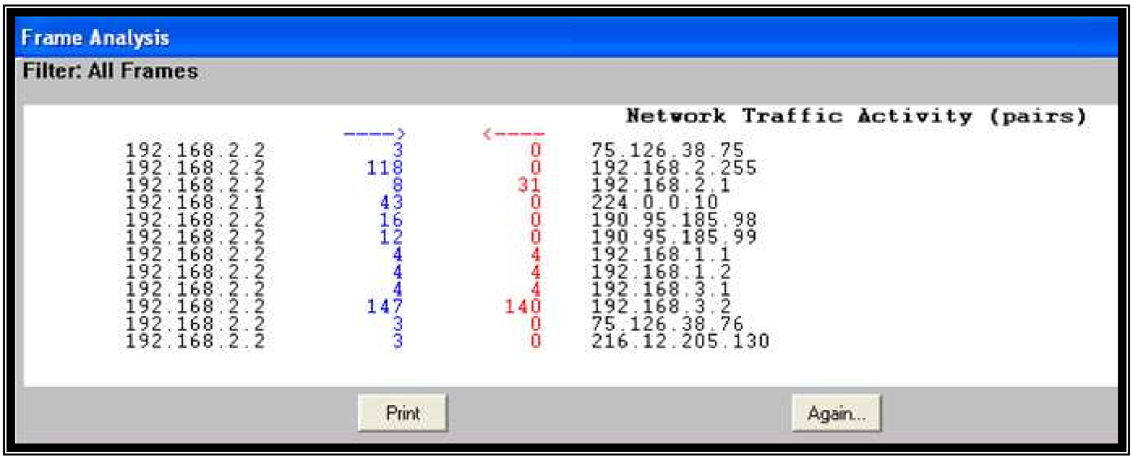



**Figura 4.4.21** Tráfico entre pares

**Distribución de tráfico por dirección destino.** En esta **figura 4.4.22** se puede observar que la dirección IP 192.168.2.2 ha recibido 183 paquetes IP. La dirección IP 192.168.3.2 ha recibido 147 paquetes IP.

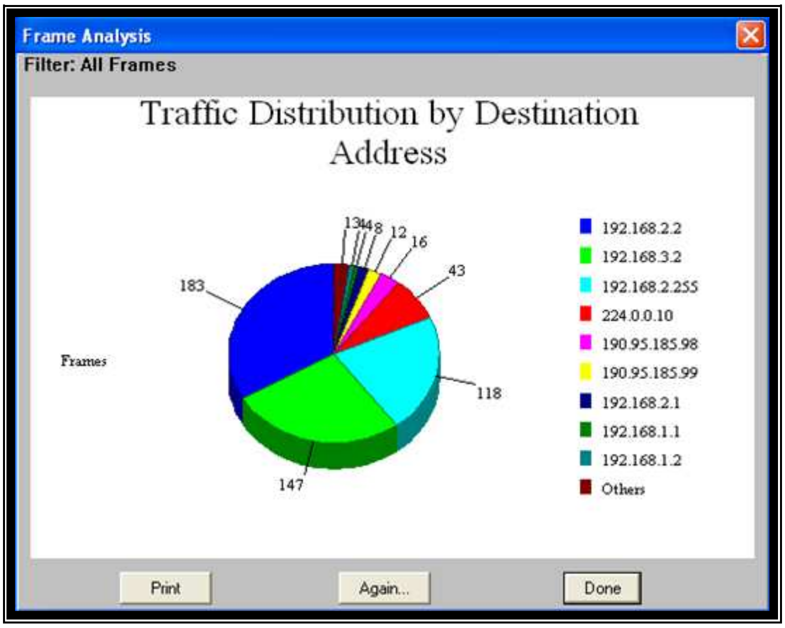



**Figura 4.4.22** Distribución de Tráfico por dirección destino

**Distribución de tráfico por dirección fuente.** La siguiente **figura 4.4.23** indica que la ip 192.168.2.2 ha enviado la mayor cantidad de paquetes IP.

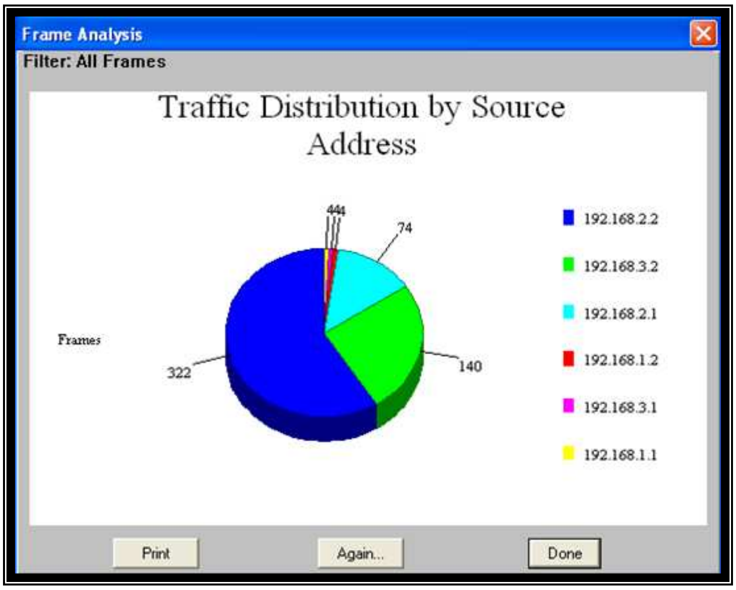



**Figura 4.4.23** Distribución de Tráfico por dirección fuente

**Paso 4: Estadísticas de tramas a nivel LAN**

Se pueden realizar dos estadísticas de distribución de tramas a nivel LAN detalladas a continuación.

- Distribución de tramas por longitud
- Distribución de tramas erróneas

**Distribución de tramas por longitud.** En la **figura 4.4.24** se puede observar que 200 tramas poseen una longitud mayor a 1281bytes, 26 tramas entre 641 bytes y 1280 bytes.

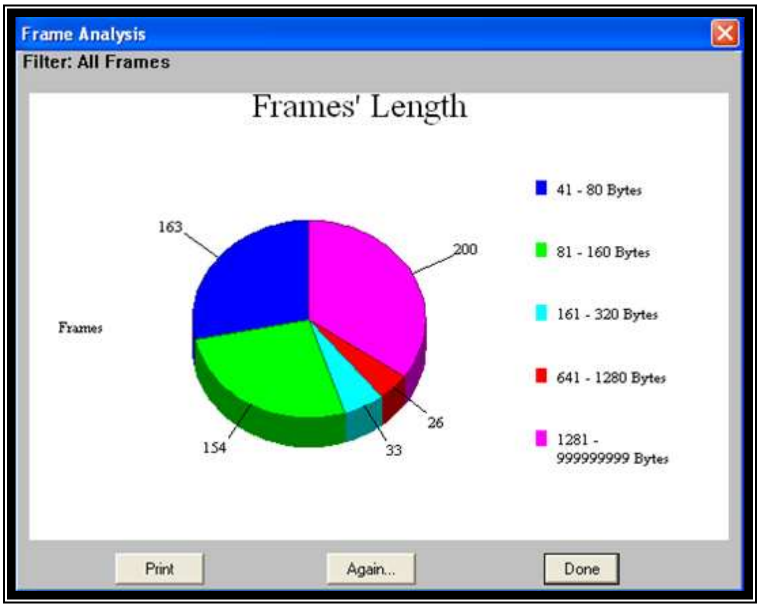



**Figura 4.4.24** Distribución de tramas por longitud

**Distribución de tramas erróneas.** En la **figura 4.4.25** se observa que ninguna trama ha tenido errores, es decir la comprobación del campo FCS ha sido correcta.

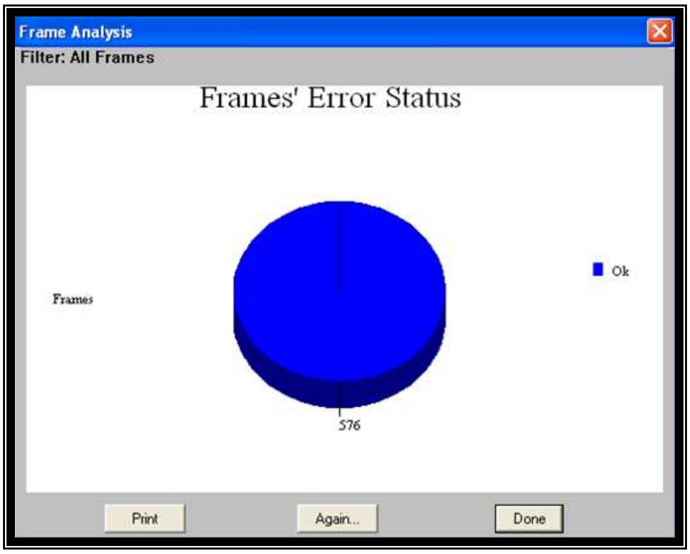



**Figura 4.4.25** Distribución de tramas erróneas

**Paso 5: Análisis por distribución de protocolo**

Se pueden realizar análisis de la distribución de los protocolos en la red. En la **figura 4.4.26** se muestra la el gráfico en diagrama de barras y en la **figura 4.4.27** se muestra en forma tabular. Ambas figuras muestran la cantidad de tramas de cada protocolo. La figura en forma de tabla muestra con más detalle la distribución de protocolos en la red.

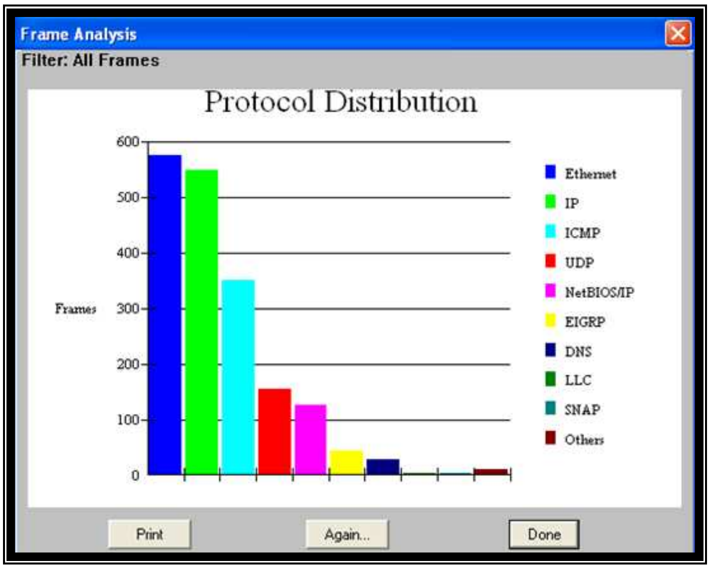
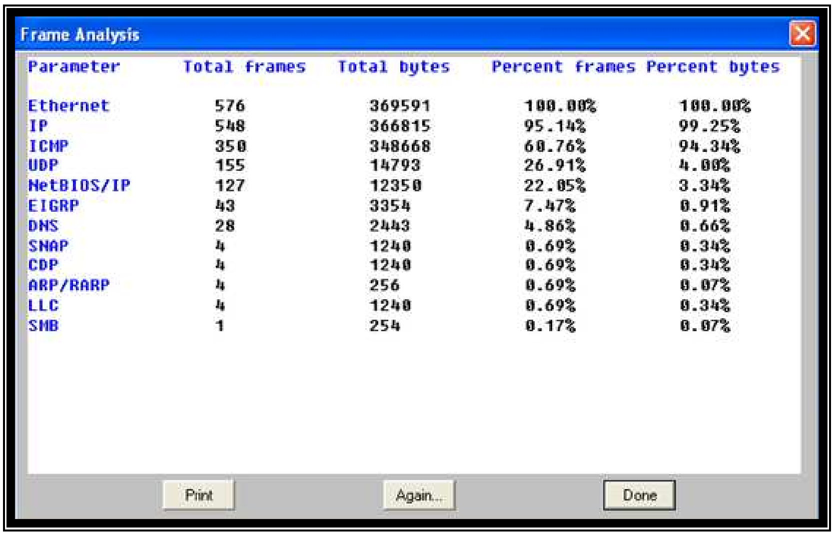



**Figura 4.4.26** Distribución de protocolos (1)

Se observa que se capturaron un total de 576 tramas Ethernet.

Se encuentran encapsulado el protocolo IP en 548 tramas Ethernet.



Frame Analysis

| Parameter | Total frames | Total bytes | Percent frames | Percent bytes |
|---|---|---|---|---|
| Ethernet | 576 | 369591 | 100.00% | 100.00% |
| IP | 548 | 366815 | 95.14% | 99.25% |
| ICMP | 350 | 348668 | 60.76% | 94.34% |
| UDP | 155 | 14793 | 26.91% | 4.00% |
| NetBIOS/IP | 127 | 12350 | 22.05% | 3.34% |
| EIGRP | 43 | 3354 | 7.47% | 0.91% |
| DNS | 28 | 2443 | 4.86% | 0.66% |
| SNAP | 4 | 1240 | 0.69% | 0.34% |
| CDP | 4 | 1240 | 0.69% | 0.34% |
| ARP/RARP | 4 | 256 | 0.69% | 0.07% |
| LLC | 4 | 1240 | 0.69% | 0.34% |
| SMB | 1 | 254 | 0.17% | 0.07% |



**Figura 4.4.27** Distribución de protocolos (2)

## 4.5.- Práctica de Laboratorio de Simulación de Frame Relay

### 4.5.1.- Descripción general

Esta práctica permite que el estudiante se familiarice con la estructura de la trama Frame Relay, con sus variantes LMI (ANSI, Q.933 y el propietario de Cisco); además de la configuración y funcionamiento de la misma. Se utilizará un analizador de Protocolos para poder visualizar la estructura de la trama Frame Relay.

### 4.5.2.- Equipos requeridos

- ✓ Dos ruteadores Cisco con una interfaz ethernet y una interfaz serial cada uno; con software EIGRP en la ios; ambos serán utilizados como dispositivos FRAD.
- ✓ Un ruteador Cisco con 2 interfaces seriales, el cual será configurado como switch Frame Relay.
- ✓ Dos switches no administrables.
- ✓ Dos computadores con tarjeta de red y puerto serie
- ✓ Un Analizador Radcom Rc-100wl con interfaz multitype y cable monitor V.35; además se necesita tener instalado el software del equipo en un computador.

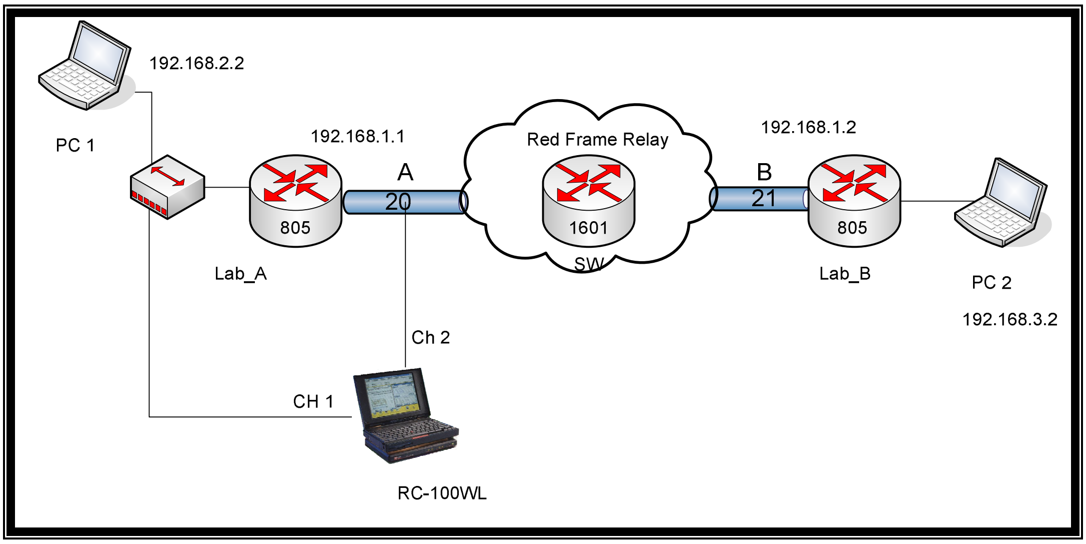



**Figura 4.5.1** Diagrama de red

### 4.5.3.- Descripción del contenido de la práctica.

Se capturarán las tramas Frame Relay con el analizador de Protocolos Radcom Rc-100wl, se analizará la estructura de la cabecera Frame Relay (propietaria de Cisco e Ietf); además se utilizará el estándar de Interfaz de Administración Local (LMI: Ansi, Q.933a y Cisco) para notificar al dispositivo final la información sobre el estado de los DLCI de la red. La topología de la red se muestra en la figura 1.

### 4.5.4.- Desarrollo de la práctica

El diseño de la práctica es la interconexión de dos ruteadores mediante un switch Frame Relay, para esto se procedió a configurar un Router Cisco 1600 como switch Frame Relay.

#### 4.5.4.1.- Esquema de conexión

Conectamos el analizador de protocolos RC-100 WL a una línea en el punto A ó B.

#### 4.5.4.2.- Conexiones de los equipos

Se deben conectar los ruteadores entre si, esto es:

- ✓ Interfaz serial 0 de ruteador Lab_A con el cable monitor V.35 (conector hembra) del equipo Radcom
- ✓ Interfaz serial 1 del ruteador SW con el cable monitor V.35 (conector macho) del equipo Radcom.
- ✓ Interfaz serial 0 de ruteador Lab_B con interfaz serial 0 del ruteador SW.
- ✓ Recordar que el cable V.35 DCE va del lado de SW.
- ✓ Conectar en los puertos disponibles del Hub la interfaz Ethernet 0 del ruteador Lab_A, la PC1 y la interfaz AUI del analizador de protocolos.
- ✓ Proceder a conectar los computadores en la interfaz Ethernet 0 del router respectivo. Además proceder con la conexión de los cables consola del ruteador según la necesidad.

#### 4.5.4.3.- Configuración de los ruteadores

Se configura los ruteadores con la información de la tabla siguiente:

**Tabla 4.5.1** Configuración de los ruteadores

| **Designación del Ruteador** | **Nombre del Ruteador** | **Tipo de Interfaz** | **Dirección serial** | **Numero DLCI** | **Dirección ethernet 0/Mascara de Subred** | **Encapsulación Frame Relay** | **LMI** |
|---|---|---|---|---|---|---|---|
| Router 1 | Lab_A | DTE | 192.168.1.1 /30 | 1023 | 192.168.2.1/24 | Cisco | Cisco |
| Router 2 | SW | DCE | Loopback 0 | 21 | | S 0: Cisco | Cisco |
| | | | Loopback 1 | 20 | | S 1: Cisco | Cisco |
| Router 3 | Lab_B | DTE | 192.168.1.2 /30 | 1023 | 192.168.3.1/24 | Cisco | Cisco |

## Paso 1: Configuración de los password

### Ruteador 1:

Router>enable
Router#configure terminal
Router(config)#hostname Lab_A
Lab_A(config)#enable secret cisco
Lab_A(config)#line console 0
Lab_A(config-line)#password cisco
Lab_A(config-line)#login
Lab_A(config-line)#exit
Lab_A(config)#line vty 0 4
Lab_A(config-line)#password cisco
Lab_A(config-line)#login
Lab_A(config-line)#exit

### Ruteador 3:

Router>
Router>enable
Router#configure terminal
Router(config)#hostname Lab_B

```
Lab_B(config)#enable secret cisco
Lab_B(config)#line console  0
Lab_B(config-line)#password cisco
Lab_B(config-line)#login
Lab_B(config-line)#exit
Lab_B(config)#line vty 0 4
Lab_B(config-line)#password cisco
Lab_B(config-line)#login
Lab_B(config-line)#exit
```

**Paso 2: Configurar las interfaces seriales**

En primer lugar se debe definir el tipo de encapsulamiento Frame Relay que se usará en este enlace mediante los siguientes comandos.

Para el ruteador Lab_A:

```
Lab_A(config)#interface serial 0
Lab_A(config-if)#encapsulation frame-relay cisco
Lab_A(config-if)#ip address 192.168.1.1 255.255.255.252
Lab_A(config-if)#frame-relay lmi-type cisco
Lab_A(config-if)#no shutdown
Lab_A(config-if)#exit
```

Para el ruteador Lab_B:

```
Lab_B(config)#interface serial 0
Lab_B(config-if)#encapsulation frame-relay
Lab_B(config-if)#ip address 192.168.1.2 255.255.255.252
Lab_B(config-if)#frame-relay lmi-type cisco
Lab_B(config-if)#no shutdown
Lab_B(config-if)#exit
```

Se debe configurar el ruteador 2 como switch Frame Relay, para esto use los siguientes comandos.

```
Router>enable
Router#configure terminal
Router(config)#hostname SW
SW(config)#frame-relay switching
SW(config)#interface serial 0
SW(config-if)#ip unnumbered Loopback 0
SW(config-if)# encapsulation frame-relay
SW(config-if)# frame-relay  lmi-type cisco
SW(config-if)#clock rate 64000
SW(config-if)# frame-relay intf-type DCE
SW(config-if)# frame-relay route 20 interface serial 1 21
SW(config-if)# no shutdown
SW(config-if)#exit

SW(config)#interface serial 1
SW(config-if)#ip unnumbered Loopback 1
SW(config-if)# encapsulation frame-relay
SW(config-if)# frame-relay  lmi-type cisco
SW(config-if)#clock rate 64000
SW(config-if)# frame-relay intf-type DCE
SW(config-if)# frame-relay route 21 interface serial 0 20
SW(config-if)# no shutdown
SW(config-if)#exit
```

**Paso 3: Configurar las interfaces Ethernet 0**

Ruteador Lab_A:

```
Lab_A(config)#interface ethernet 0
Lab_A(config-if)#ip address 192.168.2.1 255.255.255.0
Lab_A(config-if)#no shutdown
Lab_A(config-if)#exit


Lab_B(config)#interface ethernet 0
Lab_B(config-if)#ip address 192.168.3.1 255.255.255.0
Lab_B(config-if)#no shutdown
```

Lab_B(config-if)#exit

**Paso 4: Configurar el enrutamiento EIGRP**

Para configurar el Protocolo de Enrutamiento de Gatway Interior Mejorado use la siguiente sintaxis:

Lab_A(config)#router eigrp 100
Lab_A(config-router)#network 192.168.1.0
Lab_A(config-router)#network 192.168.2.0
Lab_A(config-router)#exit

Lab_B(config)#router eigrp 100
Lab_B(config-router)#network 192.168.1.0
Lab_B(config-router)#network 192.168.3.0
Lab_B(config-router)#exit

Nota: Utilizar el siguiente comando en cada uno de los router router#copy running-config startup-config, para guardar su configuración.

**4.5.4.4.- Verificación de la configuración Frame Relay**

**PASO 1: Verificar la Interfaz de Administración Local**

Utilice el comando **show frame-relay** lmi para mostrar las estadísticas de tráfico LMI. Por ejemplo, este comando muestra el número de mensajes de estado intercambiados entre el ruteador local y el switch Frame Relay como se detalla en la **figura 4.5.2**.

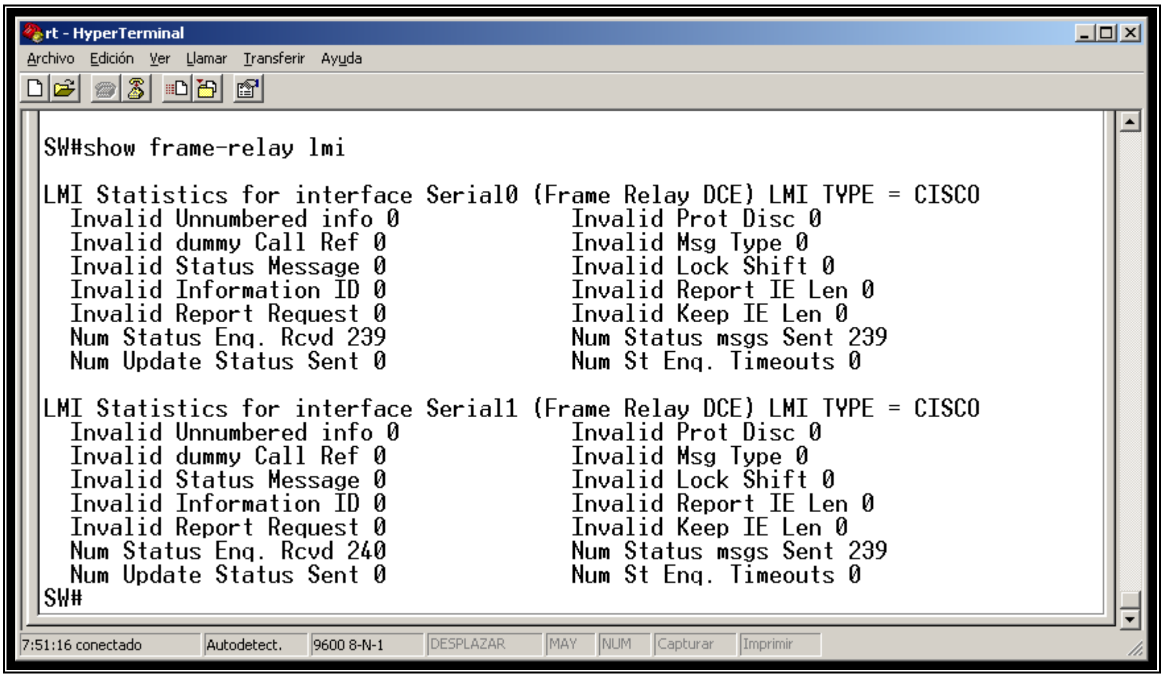
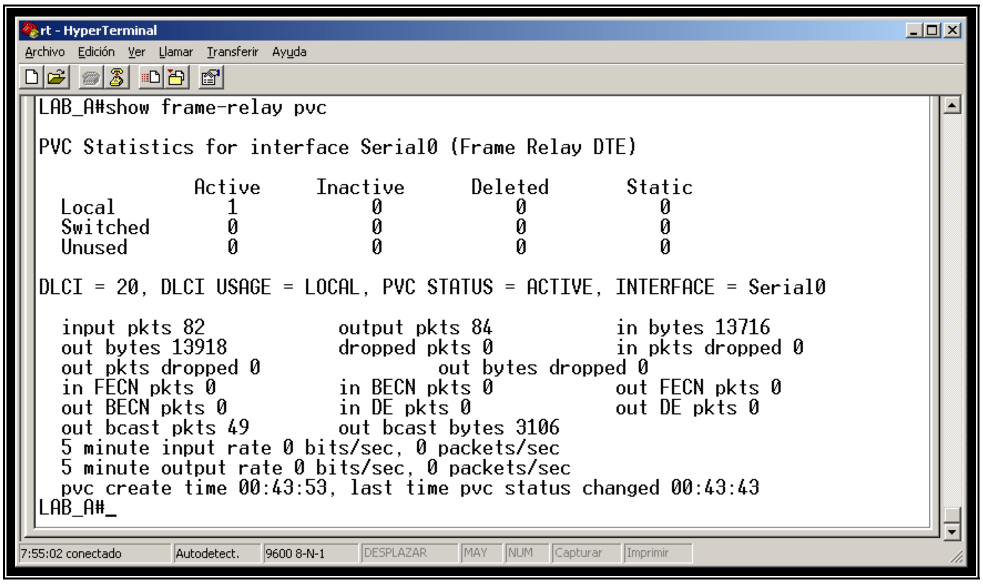



**Figura 4.5.2** Estadísticas de LMI del switch Frame Relay

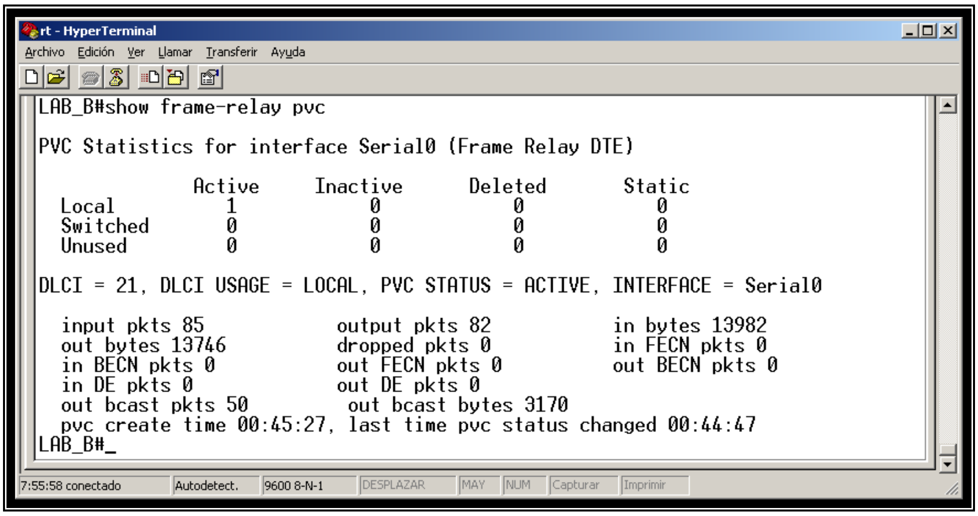
**PASO 2: Verificar el PVC de Frame Relay**

Use el comando show frame-relay pvc para mostrar el estado de todos los PVCs configurados en el ruteador. Este comando resulta útil para ver el número de los paquetes de BECN y FECN que el router recibe. El estado del PVC puede ser activo, inactivo o eliminado. La **figura 4.5.3** corresponde al ruteador Lab_A, la **figura 4.5.4** al ruteador Lab_B y la **figura 4.5.5** al Switch Frame Relay.




```
LAB_A#show frame-relay pvc

PVC Statistics for interface Serial0 (Frame Relay DTE)

              Active     Inactive      Deleted       Static
  Local          1            0            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0

DLCI = 20, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

  input pkts 82            output pkts 84           in bytes 13716
  out bytes 13918          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 49        out bcast bytes 3106
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:43:53, last time pvc status changed 00:43:43
LAB_A#_
```

**Figura 4.5.3** Verificación de PVC del Router Lab_A




```
LAB_B#show frame-relay pvc

PVC Statistics for interface Serial0 (Frame Relay DTE)

              Active     Inactive      Deleted       Static
  Local          1            0            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0

DLCI = 21, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

  input pkts 85            output pkts 82           in bytes 13982
  out bytes 13746          dropped pkts 0           in FECN pkts 0
  in BECN pkts 0           out FECN pkts 0          out BECN pkts 0
  in DE pkts 0             out DE pkts 0
  out bcast pkts 50         out bcast bytes 3170
  pvc create time 00:45:27, last time pvc status changed 00:44:47
LAB_B#_
```

**Figura 4.5.4** Verificación de PVC del Router Lab_B

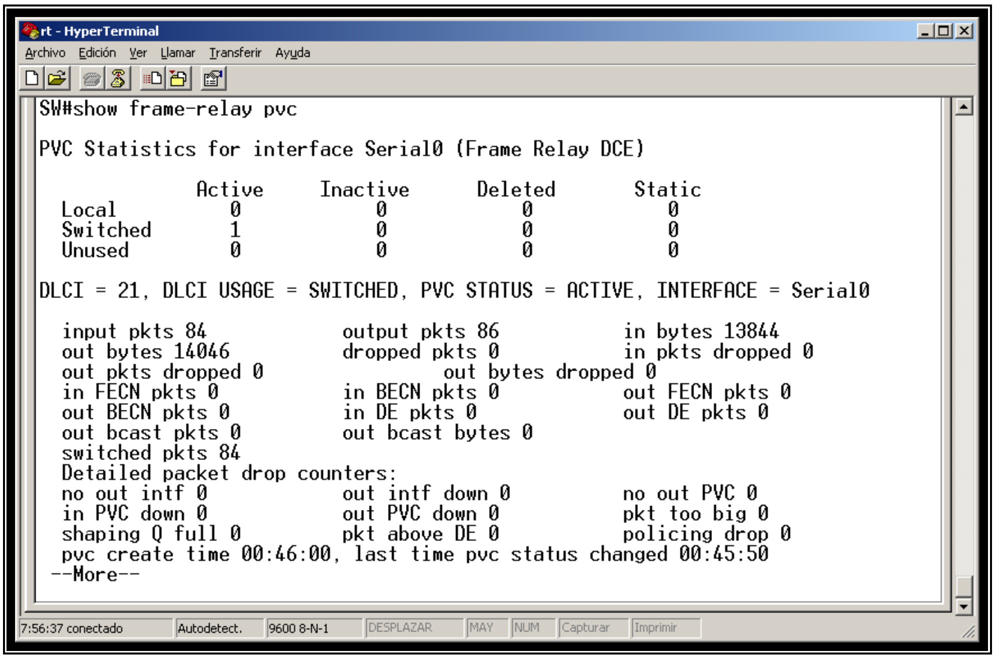



**Figura 4.5.5** Verificación de PVC del switch Frame Relay

## PASO 3: Visualizar el Mapeo de Frame Relay

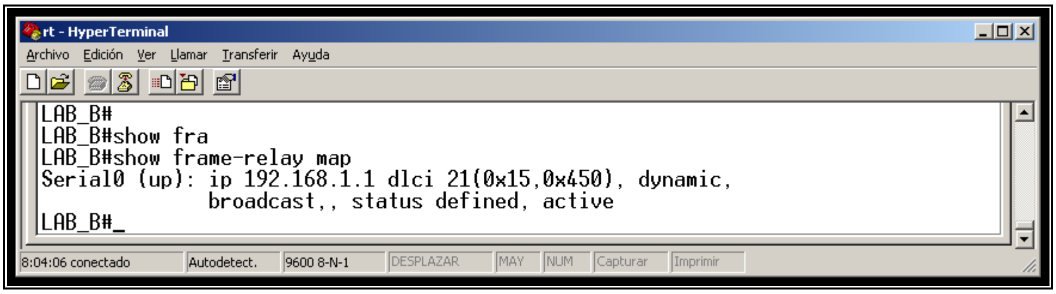



**Figura 4.5.6** Verificación del Mapeo Frame Relay Lab_B

Utilice el comando show frame-relay map para mostrar las asignaciones actuales e información acerca de las conexiones. La siguiente información interpreta el resultado del comando show frame-relay map del ruteador Lab_B que se muestra en la **figura 4.5.6**:

- 192.168.1.1 es la dirección IP de un ruteador remoto, que se aprende de forma dinámica a través de un proceso ARP inverso.
- 21 es el valor decimal del número DLCI local.
- 0x15 es la conversión hexadecimal del número DLCI, , 0x15 = 21 decimal.
- 0x450 es el valor tal como se muestra en la trama debido a la forma en que los bits DLCI se reparten en el campo de dirección de la trama Frame Relay.
- La capacidad broadcast/multicast está habilitada en el PVC.
- El estado del PVC es activo.

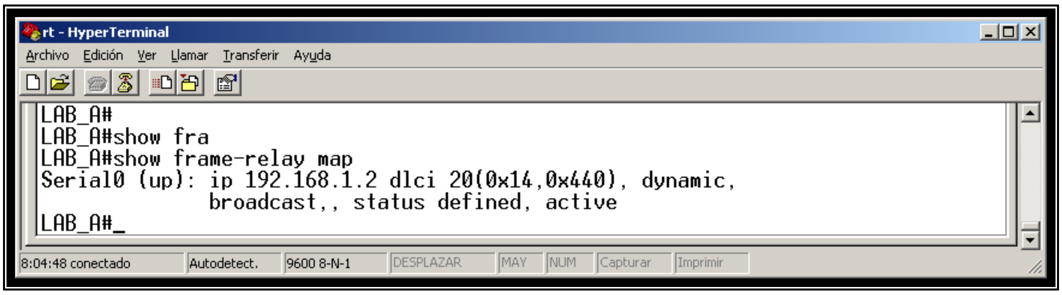



**Figura 4.5.7** Verificación del Mapeo Frame Relay Lab_A

La siguiente información interpreta el resultado del comando show frame-relay map que se muestra en la **figura 4.5.7**:

- 192.168.1.2 es la dirección IP de un router remoto, que se aprende de forma dinámica a través de un proceso ARP inverso.
- 20 es el valor decimal del número DLCI local.
- 0x14 es la conversión hexadecimal del número DLCI, , 0x14 = 20 decimal
- 0x440 es el valor tal como se muestra la trama debido a la forma en que los bits DLCI se reparten en el campo de dirección de la trama Frame Relay.
- La capacidad broadcast/multicast está habilitada en el PVC.
- El estado del PVC es activo.

**PASO 4: Verificar la conectividad**

Las **figura 4.5.8** muestra la realización de ping a las interfaces Ethernet del router Lab_B y la **figura 4.5.9** del router Lab_A.

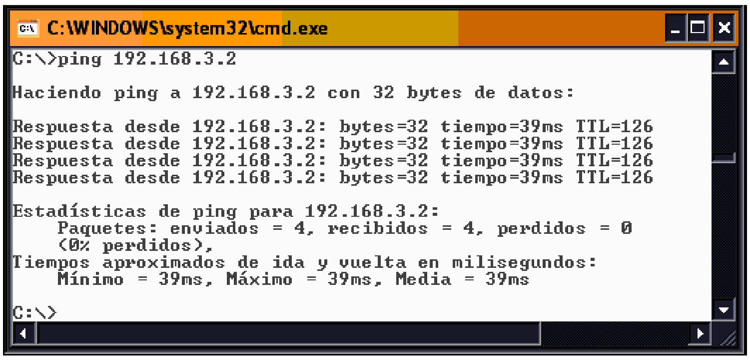



**Figura 4.5.8** Realización de ping Lab_B

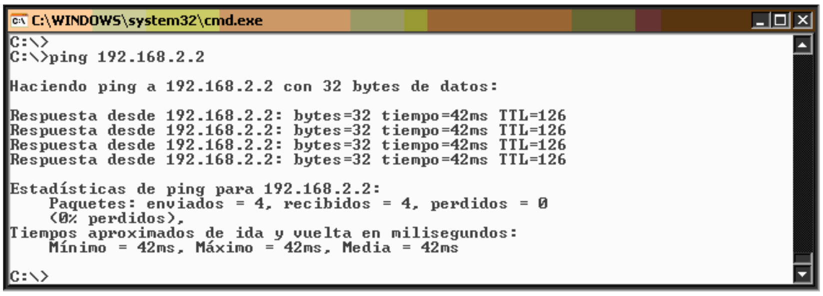



**Figura 4.5.9** Realización de ping Lab_A

### 4.5.4.5.- Captura de la trama de la interfaz de administración local (LMI)

Para capturar la estructura de la trama, se procederá a utilizar el analizador de protocolos RC-100WL.

**Paso 1: Ejecutar el programa RC-100WL**

Activar solo la interfaz Multi Type, en working mode, se seleccionará Monitor. Luego OK, ver **figura 4.5.10**.

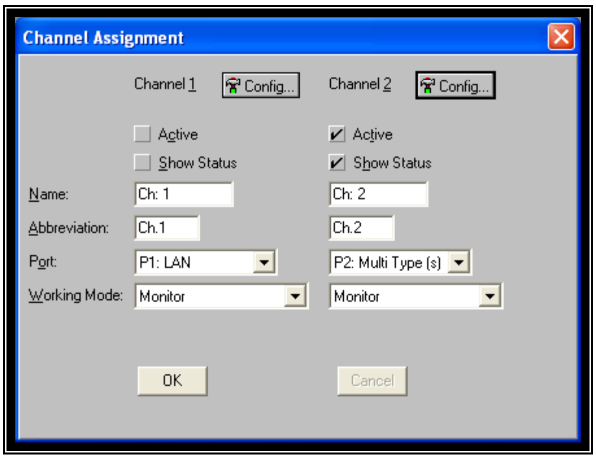



**Figura 4.5.10** Asignación del canal

**Paso 2: Seleccionar el protocolo utilizado**

En el menú "system" seleccionar "Protocols variants" como se detalla en la **figura 4.5.11**.

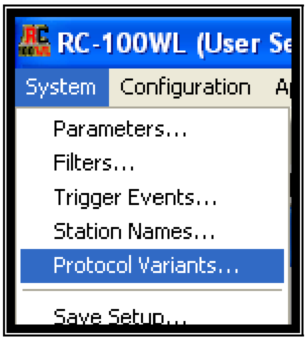



**Figura 4.5.11** Selección del protocolo utilizado

Posteriormente en la ventana protocols variants en la fila 10 columna 3 seleccionar el LMI (Ansi, Q.933 o el propietario de Cisco) según este configurado en la interfaz donde se encuentra el analizador de protocolos, ver **figura 4.5.12**. Luego dar click en OK.

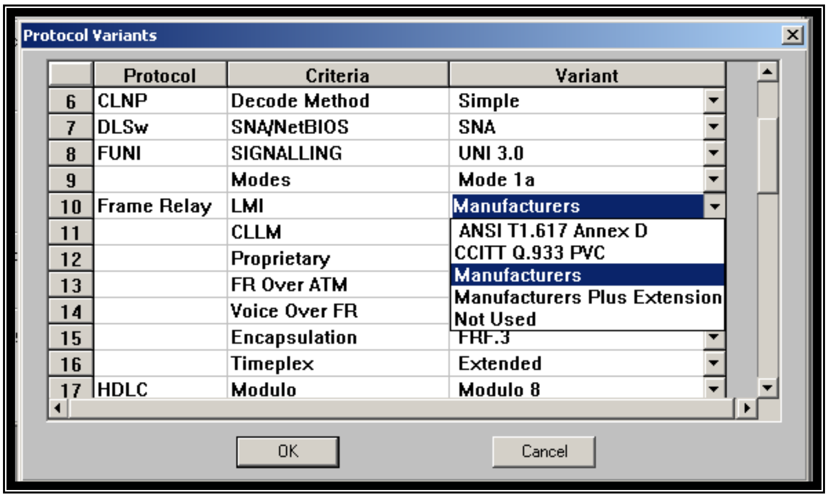



**Figura 4.5.12** Selección de la variante del protocolo

**Paso 3: Capturar las tramas**

Para iniciar el proceso de captura se debe ir a la ventana de captura de la siguiente manera en el menú Window seleccionar Ch #: capture, ver **figura 4.5.13**.

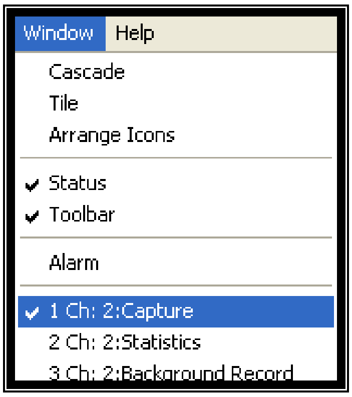



**Figura 4.5.13** Selección de la ventana de captura

Posteriormente en la ventana Ch2: Capture se da clic en Go para empezar la captura de tramas en la interfaz serial. Luego para finalizar la captura se procederá a dar clic en el botón Stop y obtenemos las tramas como se muestra en la **figura 4.5.14**.

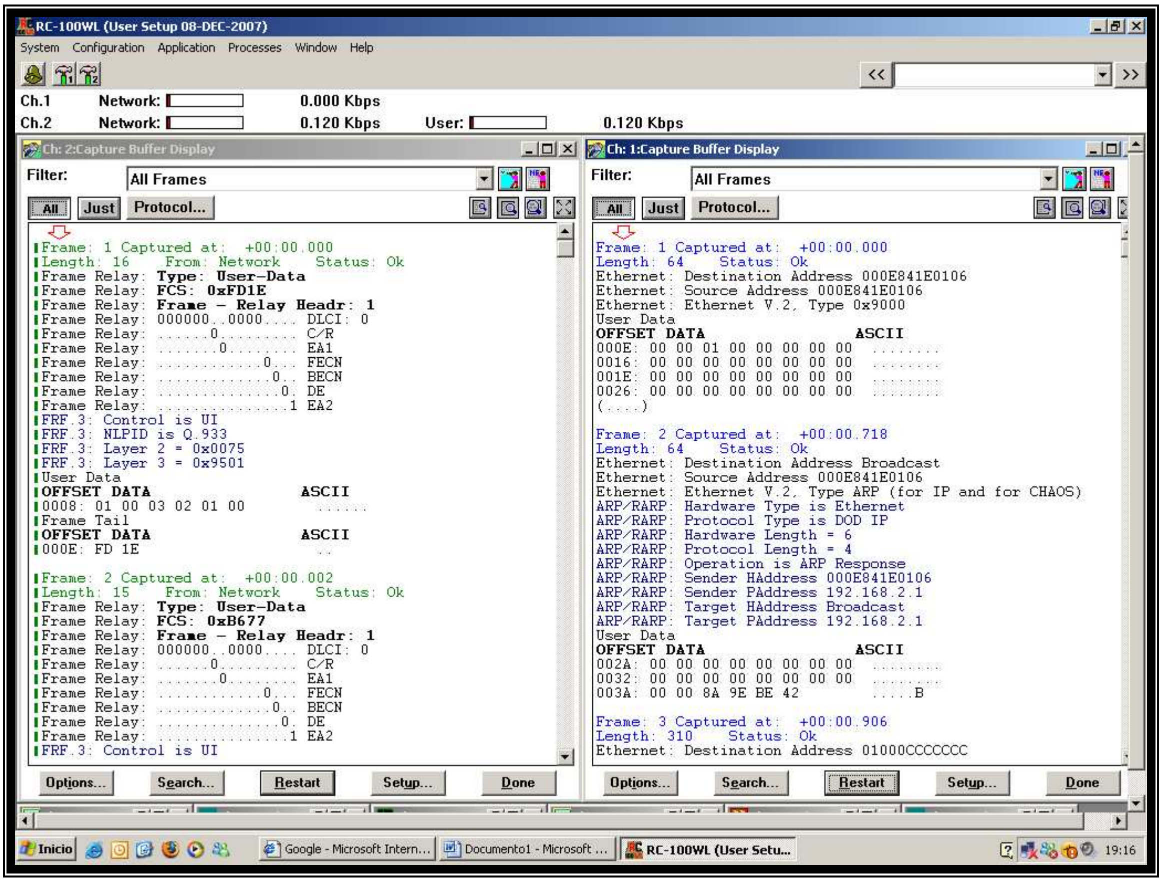



**Figura 4.5.14** Ventana de captura

### 4.5.4.6.- Análisis de la trama de los tipos de mensajes de señalización

Una vez capturada las tramas se procederá a realizar el análisis correspondiente

#### 4.5.4.6.1.- Análisis de la trama Propietario de Cisco

Los mensajes de señalización del protocolo LMI de cisco utiliza el dlci 1023, estos mensajes tienen la causa de la congestión y la lista de DLCIs que deben reducir su tráfico.

Las tramas capturadas por el analizador de protocolos se las obtuvo entre el lab_A y la Nube FR como se muestra en la **figura 4.5.15**.

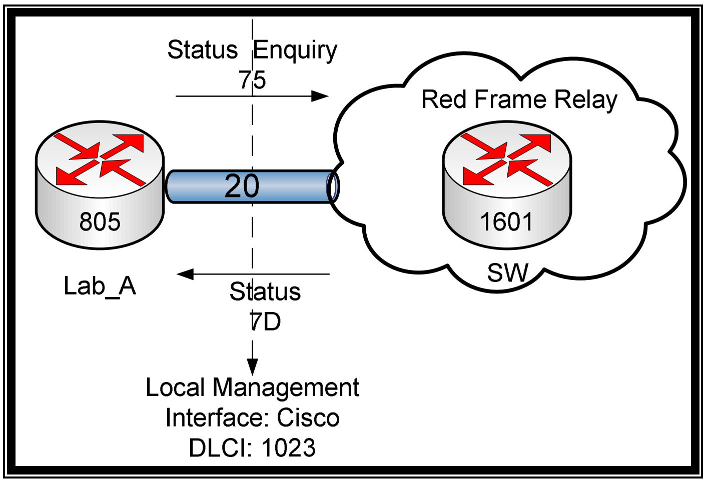



**Figura 4.5.15** Intercambio de mensajes LMI

Después del arranque de los equipos utilizados, los FRAD (Lab_A y Lab_B), no tienen conocimiento de los pvc activos de la nube Frame Relay. Por tal motivo el FRAD envía una trama “status enquiry” (1,0) como se muestra en la

**figura 4.5.16**, en respuesta; la nube FR envía una trama “full status” (1,1) informando del estado de los pvc con sus respectivos dlci’s.

En el siguiente “status enquiry” (2,1) la nube responderá confirmando que el enlace está activo “status” (2,2).

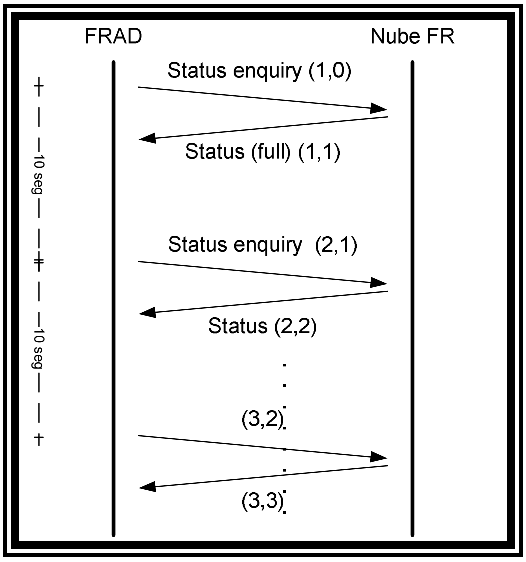



**Figura 4.5.16** Mensajes de señalización

**Paso 1: Verificar el mensaje Status Enquiry (1, 0)**

En las tramas capturadas con el analizador de protocolos, encontrar la trama enviada por el usuario solicitando un “Status Enquiry” a la red FR, para su respectivo análisis.

**Tabla 4.5.2** Trama 3

```
Frame: 3 Captured at:  +00:04.566
Length: 15    From: User    Status: Ok
Frame Relay: Type: PVC Status Request
Frame Relay: FCS: 0xDF4A
Frame Relay: Frame - Relay Headr: 64753  <FCF1>
Frame Relay: 111111..1111.... DLCI: 1023
Frame Relay: ......0......... C/R
Frame Relay: .......0........ EA1
Frame Relay: ............0... FECN
Frame Relay: .............0.. BECN
Frame Relay: ..............0. DE
Frame Relay: ...............1 EA2
Frame Relay: Signature:
Frame Relay:   Unnumbered Info Frame: 0x03  <03>
Frame Relay:   Protocol Discriminator: LMI   <09>
Frame Relay:   Call Reference: 0x00  <00>
Frame Relay: Message Type: Status Enquiry  0x75  <75>
Frame Relay: IE: Report type       ID = 0x1   <01>
Frame Relay:   Len: 1              <01>
Frame Relay:   Type: Full Status    <00>
Frame Relay: IE: Link integrity verification        ID = 0x3   <03>
Frame Relay:   Len: 2              <02>
Frame Relay:   Send Sequence Number: 1  <01>
Frame Relay:   Receive Sequence  Number: 0  <00>
Frame Tail
OFFSET DATA                                        ASCII
000D: DF 4A                                             .J
```

Como se puede ver en la trama (1, 0) en la **tabla 4.5.2**, en el campo de información se observa el DLCI: 1023 lo que indica que es una trama de administración, el cual corresponde al LMI Cisco.

**Paso 2: Crear el mensaje Status Enquiry (1, 0)**

Con los datos obtenidos anteriormente realizar la estructura completa de la trama Frame Relay, ver **tabla 4.5.3**.

**Tabla 4.5.3** Trama 3 (2)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| BANDERA | | | | | | | |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| DLCI MSB | | | | | | C/R | EA1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| DLCI LSB | | | | FECN | BECN | DE | EA2 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| CONTROL | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| DISCRIMINADOR DE PROTOCOLOS | | | | | | | |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| REFERENCIA DE LLAMADA | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| TIPO DE MENSAJE (STATUS ENQUIRY) | | | | | | | |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| IE1: (TIPO DE REPORTE) | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| LONGITUD | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| TIPO: SEQUENCE ONLY | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| IE2: (VERIFICACIÓN DE INTEGRIDAD DEL ENLACE) | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| LONGITUD | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| NUMERO DE SECUENCIA ENVIADO | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| NUMERO DE SECUENCIA RECIBIDO | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| FCS | | | | | | | |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| FCS | | | | | | | |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| FLAG | | | | | | | |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |

**Paso 3: Verificar el mensaje Status (1, 1)**

En las tramas capturadas con el analizador de protocolos, encontrar la trama "Status" enviada por la red Frame Relay en respuesta de la trama "Status Enquiry" solicitada por el usuario final, para su respectivo análisis.

**Tabla 4.5.4** Trama 4

```
Frame: 4 Captured at:  +00:04.569
Length: 23    From: User    Status: Ok
Frame Relay: Type: PVC Status
Frame Relay: FCS: 0xB47F
Frame Relay: Frame - Relay Headr: 64753  <FCF1>
Frame Relay: 111111..1111.... DLCI: 1023
Frame Relay: ......0......... C/R
Frame Relay: .......0........ EA1
Frame Relay: ............0... FECN
Frame Relay: .............0.. BECN
Frame Relay: ..............0. DE
Frame Relay: ...............1 EA2
Frame Relay: Signature:
Frame Relay:   Unnumbered Info Frame: 0x03  <03>
Frame Relay:   Protocol Discriminator: LMI   <09>
Frame Relay:   Call Reference: 0x00  <00>
Frame Relay: Message Type: Status  0x7D  <7D>
Frame Relay: IE: Report type       ID = 0x1   <01>
Frame Relay:   Len: 1              <01>
Frame Relay:   Type: Full Status    <00>
Frame Relay: IE: Link integrity verification        ID = 0x3   <03>
Frame Relay:   Len: 2              <02>
Frame Relay:   Send Sequence Number: 1  <01>
Frame Relay:   Receive Sequence  Number: 1  <01>
Frame Relay: IE: PVC Status       ID = 0x7   <07>
Frame Relay:   Len : 6             <06>
Frame Relay:   PVC DLCI : 20       <0014>
Frame Relay:   PVC Status: 2       <02>
Frame Relay:   0....... Ext [Should Be One]
Frame Relay:   .000.... Spare
Frame Relay:   ....0... New: PVC Is Already Present
Frame Relay:   .....0.. Spare
Frame Relay:   ......1. Active: PVC Is Active
Frame Relay:   .......0 Spare
Frame Tail
OFFSET DATA                                         ASCII
0015: B4 7F                                              ..
```

Como se observa en la trama capturada (1, 1) en la **tabla 4.5.4** la nube FR ha respondido con un elemento de información adicional (IE3), el cual me indica el PVC activo con su respectivo DLCI: 20.

**Paso 4: Crear el mensaje Status (1, 1)**

Se procede a crear la trama con los datos obtenidos anteriormente, ver **tabla 4.5.5**.

**Tabla 4.5.5** Trama 4 (2)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| BANDERA | | | | | | | |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| DLCI MSB | | | | | | C/R | EA1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| DLCI LSB | | | | FECN | BECN | DE | EA2 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| CONTROL | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| DISCRIMINADOR DE PROTOCOLOS | | | | | | | |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| REFERENCIA DE LLAMADA | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| TIPO DE MENSAJE (STATUS) | | | | | | | |
| 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| IE1: (TIPO DE REPORTE) | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| LONGITUD | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| TIPO: FULL STATUS | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| IE2: (VERIFICACIÓN DE INTEGRIDAD DEL ENLACE) | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| LONGITUD | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| NUMERO DE SECUENCIA ENVIADO | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| NUMERO DE SECUENCIA RECIBIDO | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| IE3 : (PVC STATUS) | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| LONGITUD | | | | | | | |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| PVC STATUS HEADER | | | | | | | |
| | | PVC DLCI MSB | | | | | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | PVC DLCI LSB | | | | | | |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| PVC STATUS | | | | | | | |
| | | | | | | ACTIVO | |
| 0 | 0 | | 0 | 0 | 0 | 1 | 0 |
| FCS | | | | | | | |
| 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| FCS | | | | | | | |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| FLAG | | | | | | | |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |

**Paso 5: Verificar el mensaje Status Enquiry (2, 1)**

En las tramas capturadas con el analizador de protocolos, encontrar la trama enviada por el usuario solicitando un “Status Enquiry” a la red FR, para su respectivo análisis, ver **tabla 4.5.6**.

**Tabla 4.5.6** Trama 10

```
Frame: 10 Captured at:  +00:14.561
Length: 15    From: Network    Status: Ok
Frame Relay: Type: Line Check
Frame Relay: FCS: 0x311C
Frame Relay: Frame - Relay Headr: 64753  <FCF1>
Frame Relay: 111111..1111.... DLCI: 1023
Frame Relay: ......0......... C/R
Frame Relay: .......0........ EA1
Frame Relay: ............0... FECN
Frame Relay: .............0.. BECN
```

```
Frame Relay: ..............0. DE
Frame Relay: ...............1 EA2
Frame Relay: Signature:
Frame Relay:   Unnumbered Info Frame: 0x03  <03>
Frame Relay:   Protocol Discriminator: LMI   <09>
Frame Relay:   Call Reference: 0x00  <00>
Frame Relay: Message Type: Status Enquiry  0x75  <75>
Frame Relay: IE: Report type       ID = 0x1   <01>
Frame Relay:   Len: 1              <01>
Frame Relay:   Type: Sequence Only    <01>
Frame Relay: IE: Link integrity verification        ID = 0x3   <03>
Frame Relay:   Len: 2              <02>
Frame Relay:   Send Sequence Number: 2  <02>
Frame Relay:   Receive Sequence  Number: 1  <01>
Frame Tail
OFFSET DATA                                       ASCII
000D: 31 1C                                            1.
```

### Paso 6: Verificar el mensaje Status (2, 2)

Se adjunta la tabla de la captura de la trama status (2, 2), ver **tabla 4.5.7**.

**Tabla 4.5.7** Trama 18

```
Frame: 0 Captured at:  +00:14.566
Length: 15    From: User    Status: Ok
Frame Relay: Type: Line Check
Frame Relay: FCS: 0xB319
Frame Relay: Frame - Relay Headr: 64753  <FCF1>
Frame Relay: 111111..1111.... DLCI: 1023
Frame Relay: ......0......... C/R
Frame Relay: .......0........ EA1
Frame Relay: ............0... FECN
Frame Relay: .............0.. BECN
Frame Relay: ..............0. DE
Frame Relay: ...............1 EA2
Frame Relay: Signature:
Frame Relay:   Unnumbered Info Frame: 0x03  <03>
Frame Relay:   Protocol Discriminator: LMI   <09>
Frame Relay:   Call Reference: 0x00  <00>
Frame Relay: Message Type: Status  0x7D  <7D>
Frame Relay: IE: Report type       ID = 0x1   <01>
Frame Relay:   Len: 1              <01>
Frame Relay:   Type: Sequence Only    <01>
Frame Relay: IE: Link integrity verification        ID = 0x3   <03>
Frame Relay:   Len: 2              <02>
Frame Relay:   Send Sequence Number: 2  <02>
Frame Relay:   Receive Sequence  Number: 2  <02>
Frame Tail
OFFSET DATA                                       ASCII
000D: B3 19                                            ..
```

#### 4.5.4.6.2.- Análisis de la trama T1.617 Annex D (LMI)

Para realizar el análisis del LMI Annex D seleccionamos en el analizador *ANSI T1.617 Annex D* como se muestra en la **figura 4.5.12**. Y en los equipos FRAD configurar en LMI correspondiente en la interfaz.

Las tramas capturadas por el analizador de protocolos se las obtuvo entre el lab_A y la Nube FR como se muestra en la figura **4.5.17**.

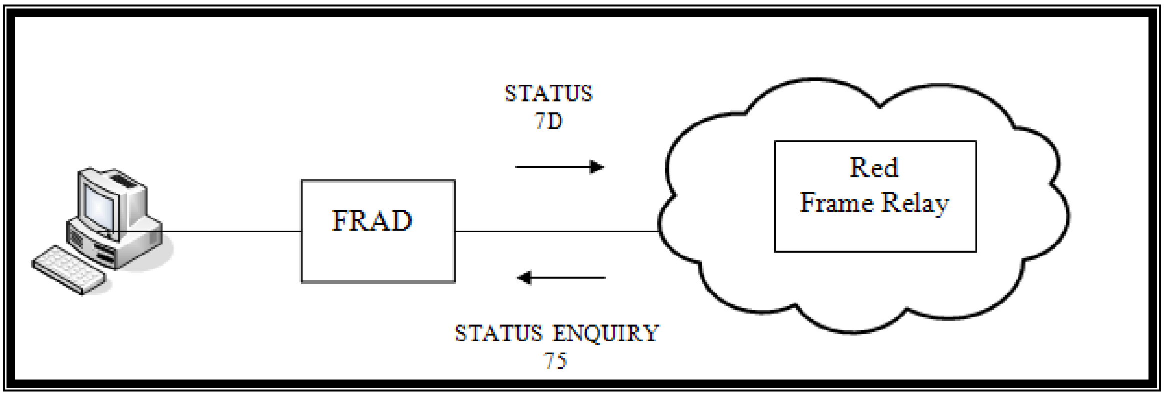



**Figura 4.5.17** Mensajes de señalización (2)

**Paso: 1 Verificar el mensaje Annex D: Status Enquiry (75)**

Para analizar el Status Enquiry se debe capturar con el analizador de protocolos la trama como se muestra a continuación en la **figura 4.5.18**.

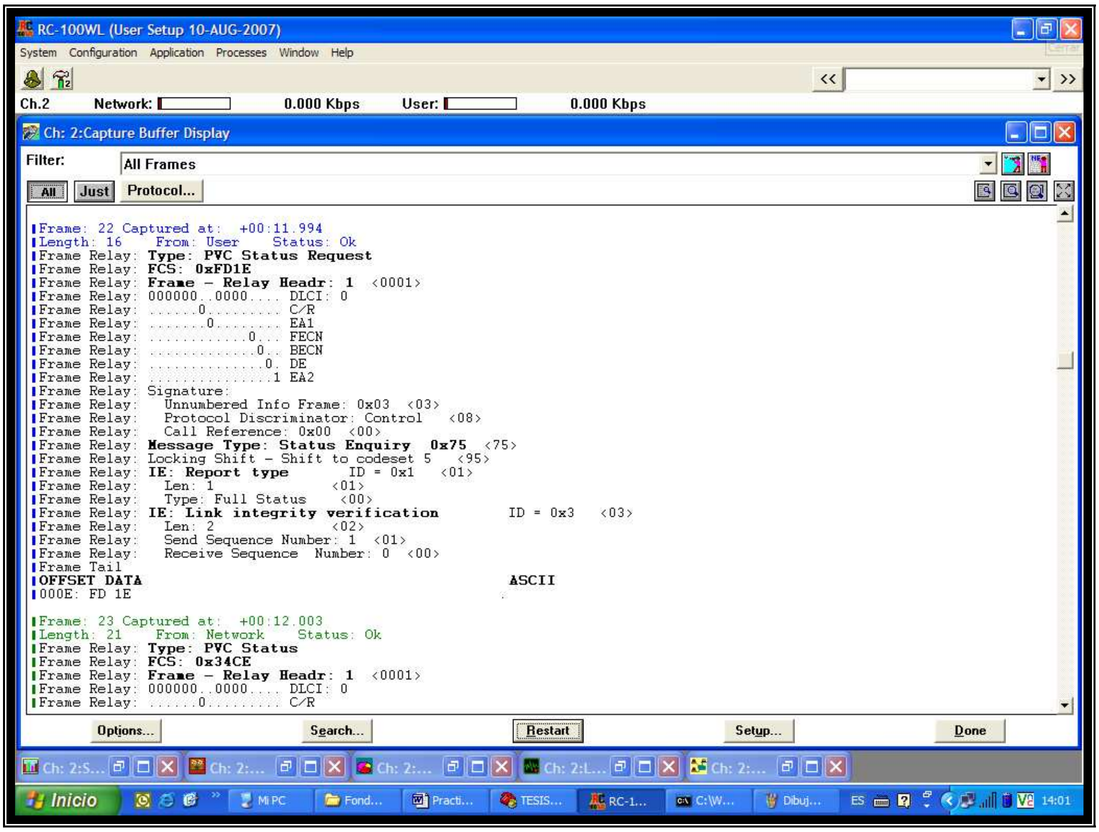



**Figura 4.5.18** Ventana de captura

Para una mejor comprensión se captura la trama en un archivo de texto, como se detalla en la **tabla 4.5.8**.

**Tabla 4.5.8** Captura de datos

```
@ Start time = 14-JAN-2008  17:44:13.000000
@ Stop time = 14-JAN-2008  17:46:47.000000
@ Line type = HDLC
@ Time mode = Relative
@ Protocol stack = Frame Relay
@ Offset = 0

Frame: 1 Captured at:  +00:00.000
Length: 16    From: User    Status: Ok
Frame Relay: Type: Line Check
Frame Relay: FCS: 0xB915
Frame Relay: Frame - Relay Headr: 1  <0001>
```

```
Frame Relay: 000000..0000.... DLCI: 0
Frame Relay: ......0......... C/R
Frame Relay: .......0........ EA1
Frame Relay: ............0... FECN
Frame Relay: .............0.. BECN
Frame Relay: ..............0. DE
Frame Relay: ...............1 EA2
Frame Relay: Signature:
Frame Relay:   Unnumbered Info Frame: 0x03  <03>
Frame Relay:   Protocol Discriminator: Control   <08>
Frame Relay:   Call Reference: 0x00  <00>
Frame Relay: Message Type: Status Enquiry  0x75  <75>
Frame Relay: Locking Shift - Shift to codeset 5   <95>
Frame Relay: IE: Report type       ID = 0x1   <01>
Frame Relay:   Len: 1              <01>
Frame Relay:   Type: Sequence Only    <01>
Frame Relay: IE: Link integrity verification        ID = 0x3   <03>
Frame Relay:   Len: 2              <02>
Frame Relay:   Send Sequence Number: 1  <01>
Frame Relay:   Receive Sequence  Number: 0  <00>
Frame Tail
OFFSET DATA                                        ASCII
000E: B9 15                                             ..
```

Los mensajes Status Enquiry del estándar Annex D tienen un formato similar a los mensajes del estándar Annex A. El elemento de información **Link Integrity Verification** es similar al elemento de información **Keep Alive** pero usa un identificador diferente.

**Paso: 2 Verificar el mensaje Annex D: Status (7D)**

Para analizar el Status se debe capturar con el analizador de protocolos la segunda trama, ver **tabla 4.5.9**.

**Tabla 4.5.9** Trama 2

```
Frame: 2 Captured at:  +00:00.008
Length: 21    From: Network    Status: Ok
Frame Relay: Type: PVC Status
Frame Relay: FCS: 0x26ED
Frame Relay: Frame - Relay Headr: 1  <0001>
Frame Relay: 000000..0000.... DLCI: 0
Frame Relay: ......0......... C/R
```

```
Frame Relay: .......0........ EA1
Frame Relay: ...........0... FECN
Frame Relay: ............0.. BECN
Frame Relay: .............0. DE
Frame Relay: ..............1 EA2
Frame Relay: Signature:
Frame Relay:   Unnumbered Info Frame: 0x03  <03>
Frame Relay:   Protocol Discriminator: Control   <08>
Frame Relay:   Call Reference: 0x00  <00>
Frame Relay: Message Type: Status  0x7D  <7D>
Frame Relay: Locking Shift - Shift to codeset 5   <95>
Frame Relay: IE: Report type       ID = 0x1   <01>
Frame Relay:   Len: 1              <01>
Frame Relay:   Type: Full Status    <00>
Frame Relay: IE: Link integrity verification        ID = 0x3   <03>
Frame Relay:   Len: 2              <02>
Frame Relay:   Send Sequence Number: 1  <01>
Frame Relay:   Receive Sequence  Number: 1  <01>
Frame Relay: IE: PVC Status       ID = 0x7   <07>
Frame Relay:   Len : 3             <03>
Frame Relay:   PVC Status Header: 416  <01A0>
Frame Relay:   0............... Ext
Frame Relay:   .0.............. Spare
Frame Relay:   ..000001.0100... PVC DLCI: 20
Frame Relay:   ........1....... Ext
Frame Relay:   .............000 Spare
Frame Relay:   PVC Status: 130     <82>
Frame Relay:   1....... Ext
Frame Relay:   .000.... Spare
Frame Relay:   ....0... New: PVC Is Already Present
Frame Relay:   .....0.. Spare
Frame Relay:   ......1. Active: PVC Is Active
Frame Relay:   .......0 Spare
Frame Tail
OFFSET DATA                                        ASCII
0013: 26 ED                                             &.
```

Los mensajes de estado de Annex D son similares a los mensajes Annex A, pero tienen tres tipos de informes:

- Informe de estado completo (Full status report): Un mensaje detallado sobre el estado de toda la red (indicando si los DLCIs del switch están activos, inactivos, etc).
- Verificación de la integridad del enlace (Link integrity verification): muestra el estado de un enlace específico.
- Mensaje Single PVC async.

- Status : muestra el estado de un solo DLCI.

#### 4.5.4.6.3.- Análisis de la trama Annex A

**Paso: 1 Verificar el mensaje Status Enquiry (75)**

Se debe verificar entre las tramas capturadas la trama de señalización con el mensaje status enquiry, ver **tabla 4.5.10**.

**Tabla 4.5.10** Trama 44

```
Frame: 44 Captured at:  +02:40.001
Length: 15    From: User    Status: Ok
Frame Relay: Type: PVC Status Request
Frame Relay: FCS: 0xAD27
Frame Relay: Frame - Relay Headr: 1  <0001>
Frame Relay: 000000..0000.... DLCI: 0
Frame Relay: ......0......... C/R
Frame Relay: .......0........ EA1
Frame Relay: ............0... FECN
Frame Relay: .............0.. BECN
Frame Relay: ..............0. DE
Frame Relay: ...............1 EA2
Frame Relay: Signature:
Frame Relay:   Unnumbered Info Frame: 0x03  <03>
Frame Relay:   Protocol Discriminator: Control   <08>
Frame Relay:   Call Reference: 0x00  <00>
Frame Relay: Message Type: Status Enquiry  0x75  <75>
Frame Relay: IE: Report type       ID = 0x51   <51>
Frame Relay:   Len: 1              <01>
Frame Relay:   Type: Full Status    <00>
Frame Relay: IE: Link integrity verification       ID = 0x53   <53>
Frame Relay:   Len: 2              <02>
Frame Relay:   Send Sequence Number: 43  <2B>
Frame Relay:   Receive Sequence  Number: 42  <2A>
Frame Relay:   0....... Ext Bit: 0
Frame Relay:   .010.... Spare Bit: 2
Frame Relay:   ....1... New Bit: 1
Frame Relay:   .....0.. Delete Bit: 0 PVC is Configured
Frame Relay:   ......1. Active Bit: 1
Frame Relay:   .......0 Spare Bit: 0
Frame Tail
OFFSET DATA                                        ASCII
000D: AD 27                                             .'
```

**Paso: 2 Verificar el mensaje Status (7D)**

Se debe verificar entre las tramas capturadas la trama de señalización con el mensaje status, ver **tabla 4.5.11**.

**Tabla 4.5.11** Trama 45

```
Frame: 45 Captured at:  +02:40.009
Length: 20    From: Network    Status: Ok
Frame Relay: Type: PVC Status
Frame Relay: FCS: 0xBC9A
Frame Relay: Frame - Relay Headr: 1  <0001>
Frame Relay: 000000..0000.... DLCI: 0
Frame Relay: ......0......... C/R
Frame Relay: .......0........ EA1
Frame Relay: ............0... FECN
Frame Relay: .............0.. BECN
Frame Relay: ..............0. DE
Frame Relay: ...............1 EA2
Frame Relay: Signature:
Frame Relay:   Unnumbered Info Frame: 0x03  <03>
Frame Relay:   Protocol Discriminator: Control   <08>
Frame Relay:   Call Reference: 0x00  <00>
Frame Relay: Message Type: Status  0x7D  <7D>
Frame Relay: IE: Report type       ID = 0x51   <51>
Frame Relay:   Len: 1              <01>
Frame Relay:   Type: Full Status    <00>
Frame Relay: IE: Link integrity verification       ID = 0x53   <53>
Frame Relay:   Len: 2              <02>
Frame Relay:   Send Sequence Number: 43  <2B>
Frame Relay:   Receive Sequence  Number: 43  <2B>
Frame Relay:   0....... Ext Bit: 0
Frame Relay:   .010.... Spare Bit: 2
Frame Relay:   ....1... New Bit: 1
Frame Relay:   .....0.. Delete Bit: 0 PVC is Configured
Frame Relay:   ......1. Active Bit: 1
Frame Relay:   .......1 Spare Bit: 1
Frame Relay: IE: PVC Status       ID = 0x57   <57>
Frame Relay:   Len : 3             <03>
Frame Relay:   PVC Status Header: 416  <01A0>
Frame Relay:   0............... Ext
Frame Relay:   .0.............. Spare
Frame Relay:   ..000001.0100... PVC DLCI: 20
Frame Relay:   ........1....... Ext
Frame Relay:   .............000 Spare
Frame Relay:   PVC Status: 130     <82>
Frame Relay:   1....... Ext
Frame Relay:   .000.... Spare
Frame Relay:   ....0... New: PVC Is Already Present
Frame Relay:   .....0.. Spare
```

```
Frame Relay:   ......1. Active: PVC Is Active
Frame Relay:   .......0 Spare
Frame Tail
OFFSET DATA                                        ASCII
0012: BC 9A                                             ..
```

### Diferencias entre la encapsulación CISCO y la encapsulación IETF

En la siguiente trama corresponde a la encapsulación IETF la podemos reconocer por el NLPID que identifica que protocolo está encapsulado en la trama FR, en este ejemplo el ID corresponde al protocolo IP 0xCC, ver **tabla 4.5.12**.

**Tabla 4.5.12** Trama capturada

```
Frame:  Captured at:  +00:50.843
Length: 66    From: User    Status: Ok
Frame Relay: Type: User-Data
Frame Relay: FCS: 0x512E
Frame Relay: Frame - Relay Headr: 1089  <0441>
Frame Relay: 000001..0100.... DLCI: 20
Frame Relay: ......0......... C/R
Frame Relay: .......0........ EA1
Frame Relay: ............0... FECN
Frame Relay: .............0.. BECN
Frame Relay: ..............0. DE
Frame Relay: ...............1 EA2
FRF.3: Control is UI                <03>
FRF.3: NLPID is IP                  <CC>
IP: Version = 4                     <45>
IP: IHL = 20 [Bytes]
IP: Type of Service: 0x00           <00>
IP:   Routine
IP:   Normal Delay
IP:   Normal Throughput
IP:   Normal Reliability
IP: Total Length = 60               <003C>
IP: Identification = 27754          <6C6A>
IP: Flags & Fragment Offset: 0x0000  <0000>
IP:   0............... Reserved
IP:   .0.............. May Fragment
IP:   ..0............. Last Fragment
IP:   Fragment Offset = 0 [Bytes]
IP: Time to Live = 127 [Seconds/Hops]  <7F>
IP: Protocol: 1 ICMP                <01>
```

```
IP: Header Checksum = 0x4902        <4902>
IP: Source Address = 192.168.2.2    <C0A80202>
IP: Destination Address = 192.168.3.2  <C0A80302>
ICMP: Type: 0  Echo Reply           <00>
ICMP: Code: 0                       <00>
ICMP: CheckSum: 0xE95B              <E95B>
ICMP: Identifier: 512               <0200>
ICMP: Sequence: 27136               <6A00>
User Data
OFFSET DATA
ASCII
0020: 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
0030: 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69     qrstuvwabcdefghi
Frame Tail
OFFSET DATA
ASCII
0040: 51 2E
```

Esta trama corresponde a la encapsulación CISCO y se diferencia de la encapsulación IETF porque utiliza un ethertype para determinar la encapsulación de los protocolos superiores en este ejemplo utiliza el protocolo IP 0x800, ver **tabla 4.5.13**.

**Tabla 4.5.13** Trama capturada

```
Frame: 0 Captured at:  +09:59.512
Length: 66    From: Network    Status: Ok
Frame Relay: Type: User-Data
Frame Relay: FCS: 0xB034
Frame Relay: Frame - Relay Headr: 1089  <0441>
Frame Relay: 000001..0100.... DLCI: 20
Frame Relay: ......0......... C/R
Frame Relay: .......0........ EA1
Frame Relay: ............0... FECN
Frame Relay: .............0.. BECN
Frame Relay: ..............0. DE
Frame Relay: ...............1 EA2
Frame Relay: Ether Type: 0x0800 IP    <0800>
IP: Version = 4                     <45>
IP: IHL = 20 [Bytes]
IP: Type of Service: 0x00           <00>
IP:   Routine
IP:   Normal Delay
IP:   Normal Throughput
IP:   Normal Reliability
IP: Total Length = 60               <003C>
IP: Identification = 458            <01CA>
IP: Flags & Fragment Offset: 0x0000  <0000>
IP:   0............... Reserved
IP:   .0.............. May Fragment
IP:   ..0............. Last Fragment
```

```
IP:   Fragment Offset = 0 [Bytes]
IP: Time to Live = 127 [Seconds/Hops]  <7F>
IP: Protocol: 1 ICMP              <01>
IP: Header Checksum = 0xB5A2      <B5A2>
IP: Source Address = 192.168.2.2  <C0A80202>
IP: Destination Address = 192.168.1.2  <C0A80102>
ICMP: Type: 8  Echo request       <08>
ICMP: Code: 0                     <00>
ICMP: CheckSum: 0x135C            <135C>
ICMP: Identifier: 768             <0300>
ICMP: Sequence: 14080             <3700>
User Data
OFFSET DATA
ASCII
0020: 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
0030: 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
Frame Tail
OFFSET DATA
ASCII
0040: B0 34
```

### 4.5.4.6.4.- Análisis de la Red

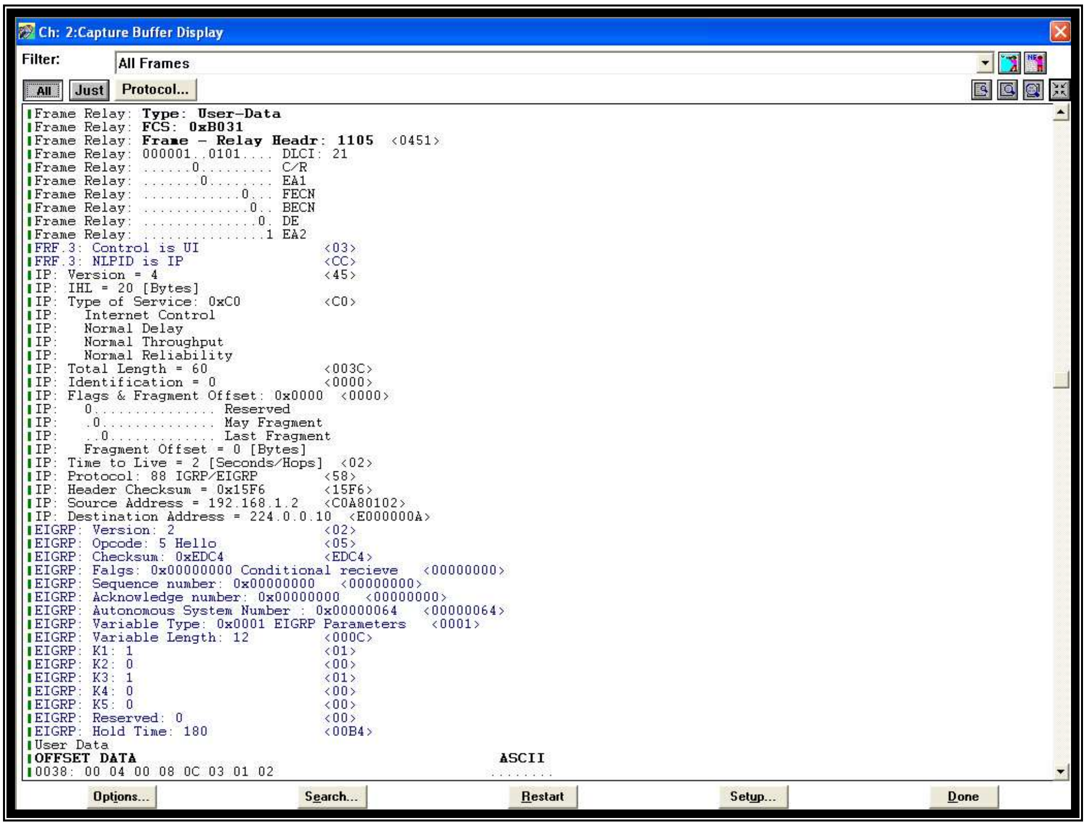



**Figura 4.5.19** Ventana de captura (2)

Este es un ejemplo de decodificación de ip encapsulado sobre Frame Relay. Esta decodificación permite al usuario identificar de forma inmediata los protocolos encapsulados, si los datos recibidos son los esperados y determinar pérdidas de paquetes y con las herramientas de analizador podemos observar la distribución total de las tramas, estadísticas, protocolos de red, actividad y distribución del tráfico, ver **figura 4.5.19**. En la trama capturada de datos podemos observar el protocolo IP y el protocolo de enrutamiento EIGRP.

**Paso 1: Distribución de la trama (Carga DLCI)**

Para observar la distribución de la carga DLCI hacemos click derecho en la pantalla del analizador, seleccionamos en análisis "Frame Distribution" como se observa en la **figura 4.5.20**.

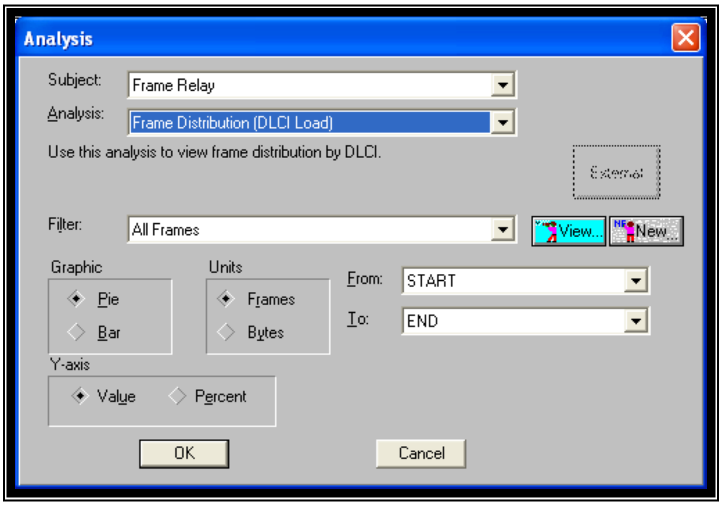



**Figura 4.5.20** Análisis de Frame Relay

Y obtenemos la distribución de la carga del enlace como se muestra en la figura 4.5.21 la cual tenemos que el DLCI 20 tiene 129 tramas y el DLCI 1023 tiene 66 tramas, esto quiere decir que en la estructura de la trama frame Relay dentro del campo de información se ha obtenido mas Datos de Usuario que Mensajes de señalización.

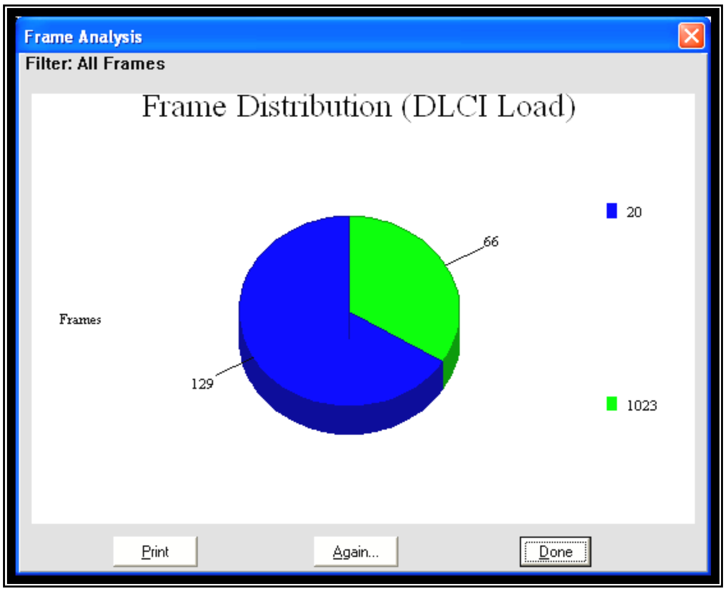



**Figura 4.5.21** Distribución de las tramas

**Paso 2: Distribución total de las trama**

Para obtener la distribución total de las tramas en Bytes hacemos click derecho en la pantalla del analizador, seleccionamos en análisis Frame Distribution(Tabular) como se observa en la **figura 4.5.22**.

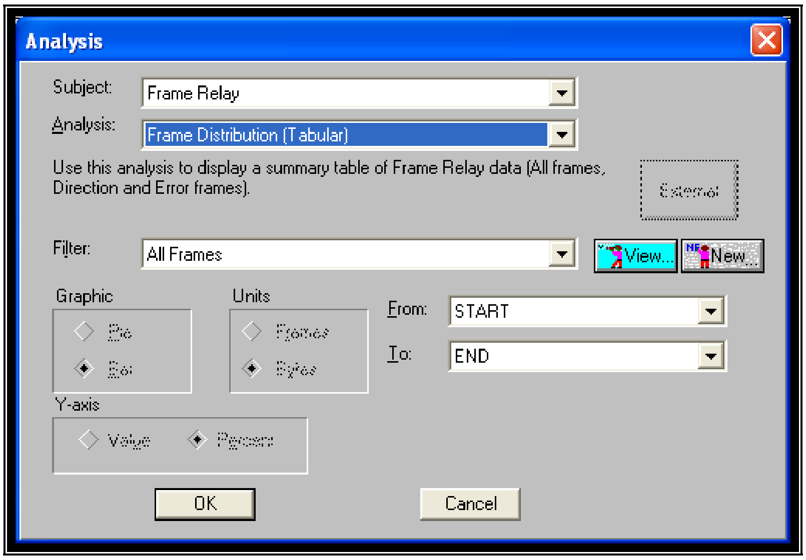
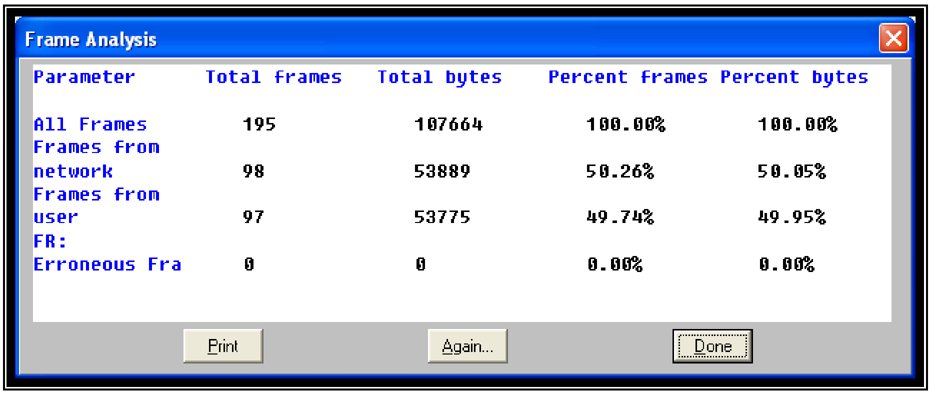



**Figura 4.5.22** Análisis de distribución de las tramas

Y obtenemos el total de tramas, la cual nos indica que se ha recibido un mayor número de tramas debido a que las tramas de la red representa el 50.26%, ver **figura 4.5.23**.



Frame Analysis

| Parameter | Total frames | Total bytes | Percent frames | Percent bytes |
|---|---|---|---|---|
| All Frames | 195 | 107664 | 100.00% | 100.00% |
| Frames from network | 98 | 53889 | 50.26% | 50.05% |
| Frames from user | 97 | 53775 | 49.74% | 49.95% |
| FR: Erroneous Fra | 0 | 0 | 0.00% | 0.00% |

Print Again... Done

**Figura 4.5.23** Análisis de distribución de las tramas (2)

**Paso 3: Estadísticas de las trama**

Para obtener las estadísticas de congestión de las tramas hacemos click derecho en la pantalla del analizador, seleccionamos en análisis Frame Estatistics como se observa en la **figura 4.5.24**.

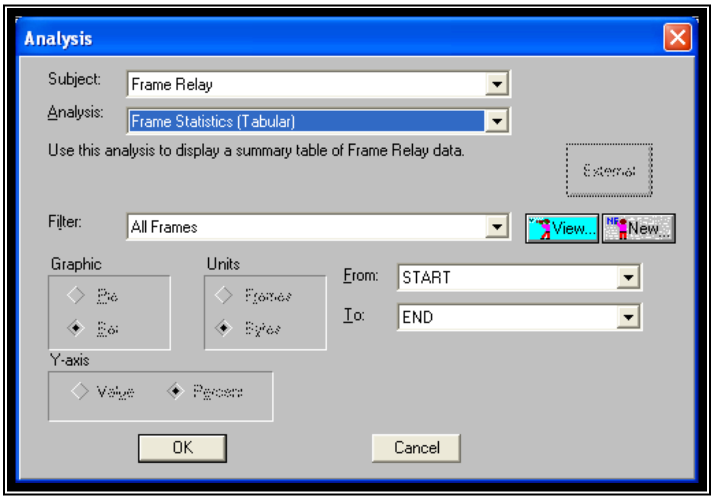



**Figura 4.5.24** Análisis de estadísticas de las tramas

La **figura 4.5.25** indica que no hay congestión en el enlace, ni hay tramas con errores, solo indica tráfico frame relay y mensajes de señalización, lo cual garantiza que el enlace está en óptimas condiciones.

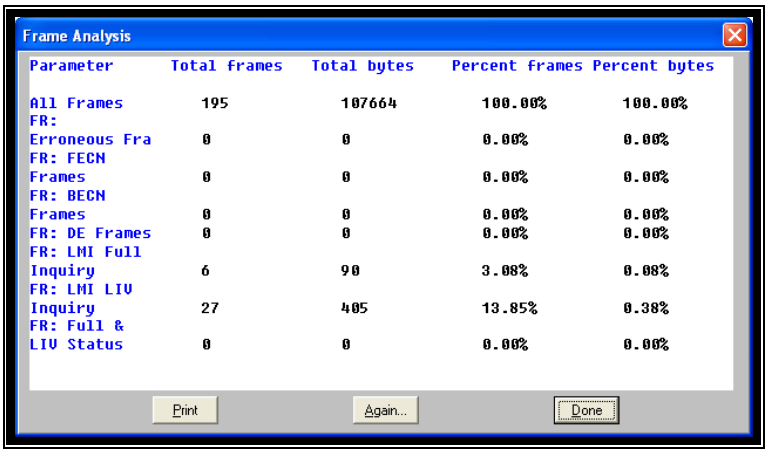



**Figura 4.5.25** Análisis de estadísticas de las tramas (2)

## Paso 4: Protocolo ICMP

Para obtener la distribución del protocolo ICMP, hacemos click derecho en la pantalla del analizador, seleccionamos en análisis Distribution by type como se observa en la **figura 4.5.26**.

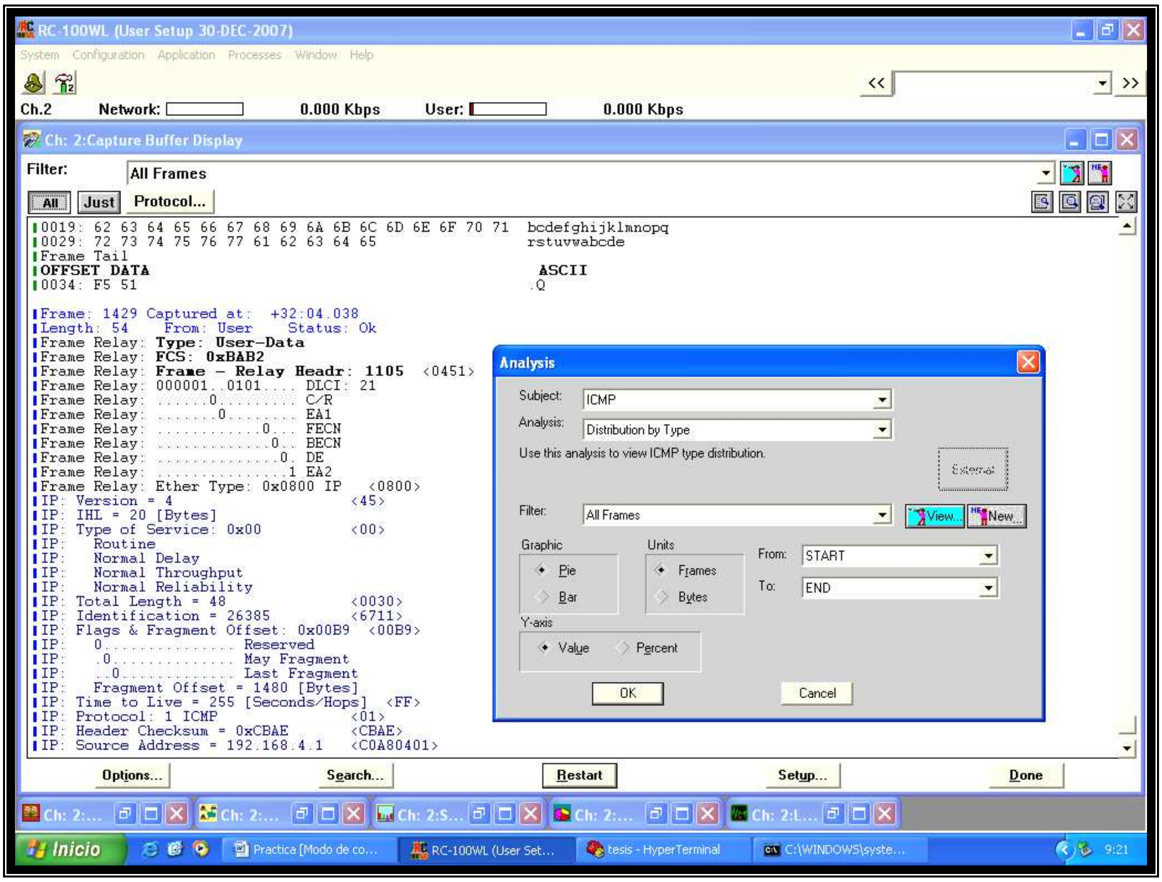


**Figura 4.5.26** Análisis de estadísticas de ICMP

Y obtenemos el total de paquetes de ping enviados, la cual en la **figura 4.5.27** indica pérdidas de ping debido a que en la Petición de eco ICMP(Echo

Request) tenemos 107 paquetes y en la Respuesta de eco ICMP (Echo Reply) tenemos 95 paquetes , la cual nos da un total de 12 paquetes perdidos.

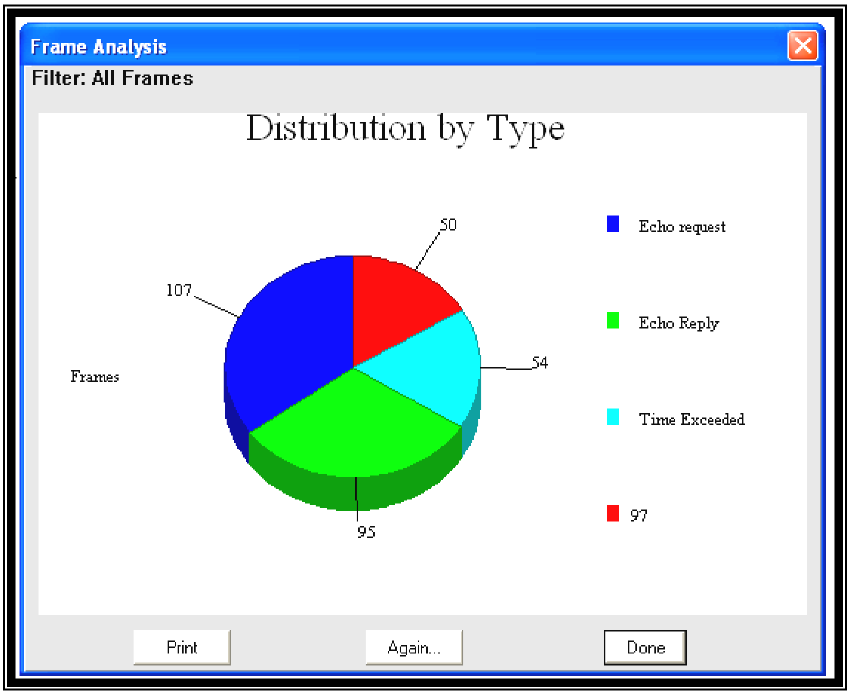



**Figura 4.5.27** Análisis de estadísticas de ICMP (2)

En las pruebas de ping realizadas se puede comprobar la secuencia y el tipo de ICMP verificando estos campos y revisando en orden cronológico las tramas. Se detecta fácilmente tramas faltantes y estas pérdidas se dan en el inicio generalmente debido al tiempo que toma asociar las direcciones MAC a direcciones IP.

**Paso 5: Protocolo IP**

Para obtener información del protocolo IP, hacemos click derecho en la pantalla del analizador, en subject seleccionamos ip y en análisis tenemos algunas opciones como por ejemplo:

**Retardo.** La **figura 4.5.28** indica que tenemos un normal retardo en el enlace.

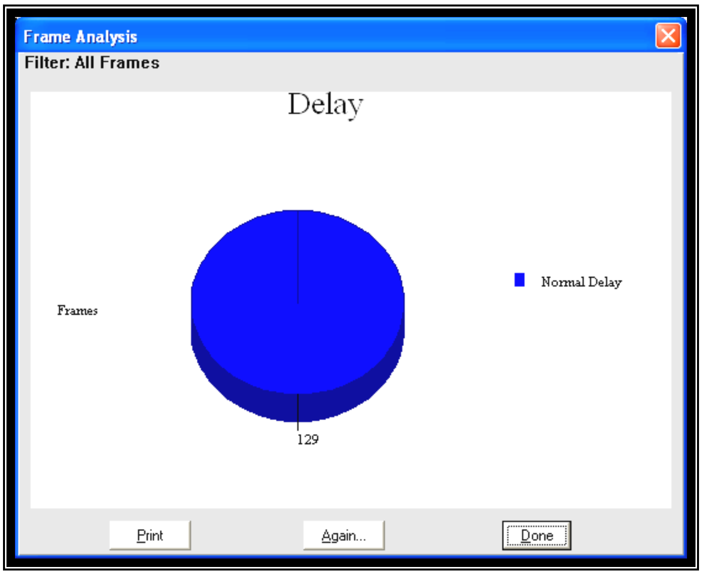



**Figura 4.5.28** Análisis de retardo en IP

**Actividad del tráfico de la red.** En la opción de la actividad del tráfico podemos observar el host que ha generado un mayor tráfico IP, como se observa en la **figura 4.5.29** la dirección ip 192.168.3.2 ha generado tráfico al host 192.168.2.2.

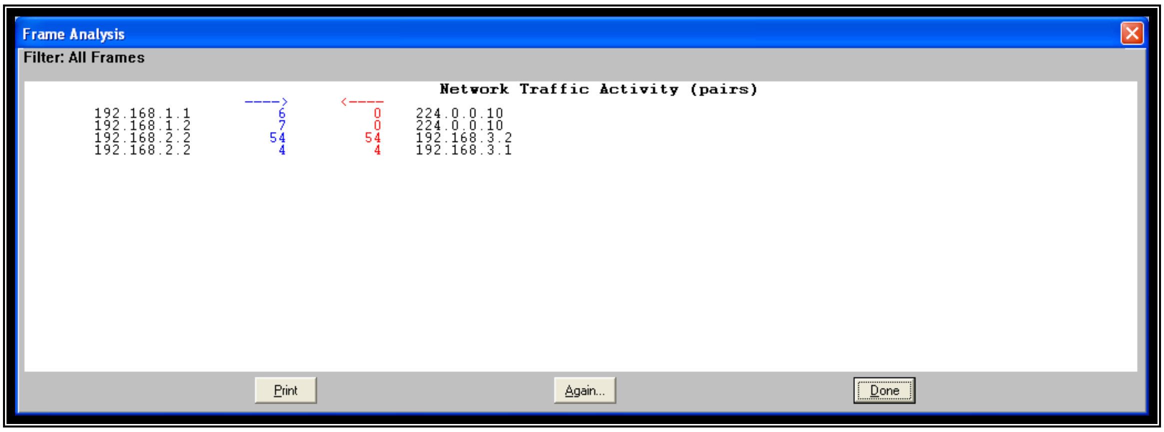



**Figura 4.5.29** Análisis de actividad de tráfico en IP

**Distribución de tráfico por dirección destino.** En la **figura 4.5.30** se obtiene que el host con la dirección ip 192.168.2.2 ha recibido un mayor porcentaje de tráfico.

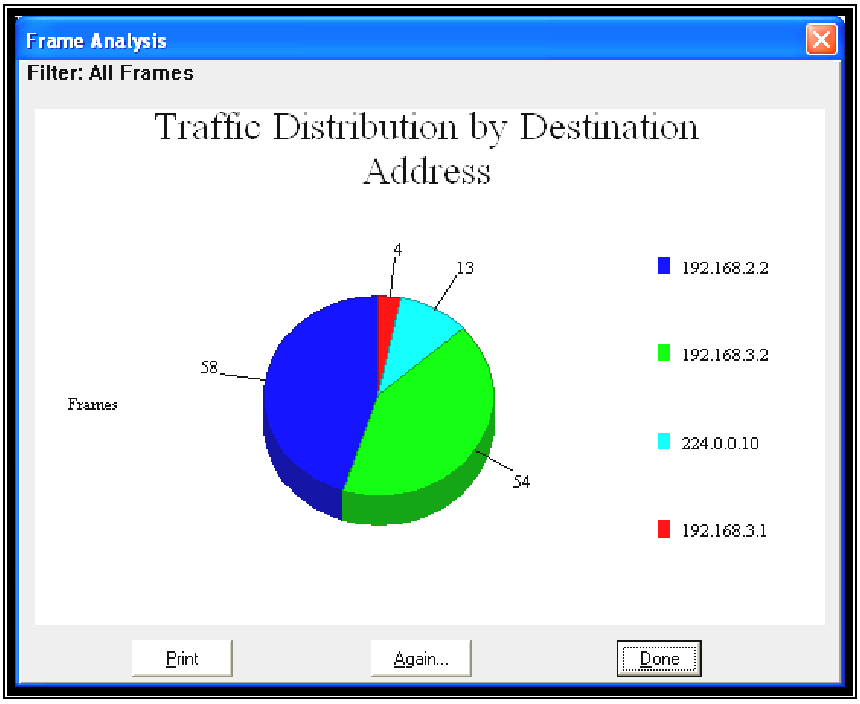



**Figura 4.5.30** Análisis de tráfico por dirección IP destino

**Distribución de tráfico por dirección fuente.** En la **figura 4.5.31** se obtiene que el host con la dirección ip 192.168.3.2 ha generado un mayor porcentaje de tráfico ip.

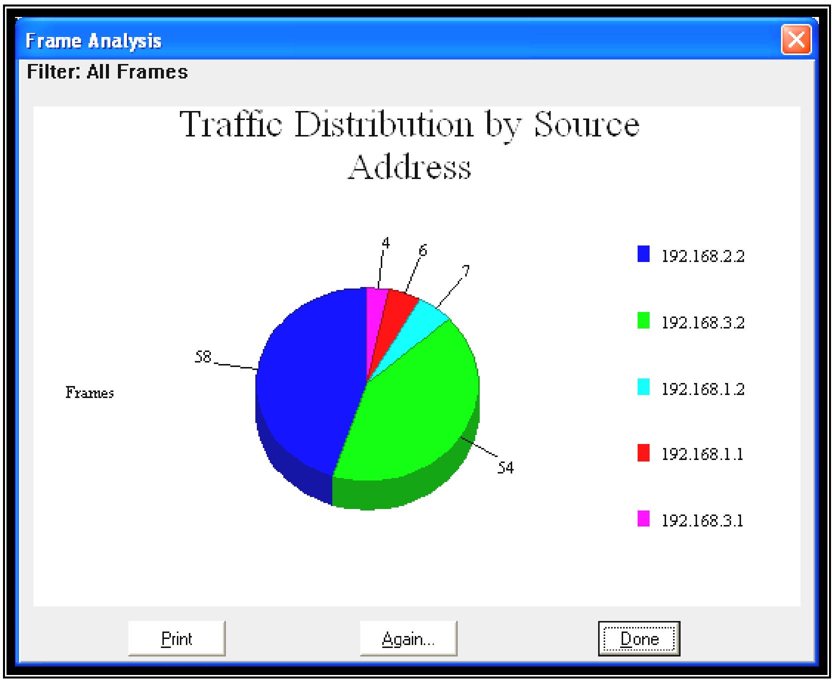



**Figura 4.5.31** Análisis de tráfico por dirección IP fuente

**Paso 6: Distribución de tráfico por protocolos**

En la **figura 4.5.32** se puede observar los protocolos, como por ejemplo: FR, EIGRP, IP, ICMP que han sido capturados en la interfaz serial.

En la **figura 4.5.33** se puede observar los protocolos ordenados en tabla con datos estadísticos como el porcentaje de tramas y bytes en la captura.

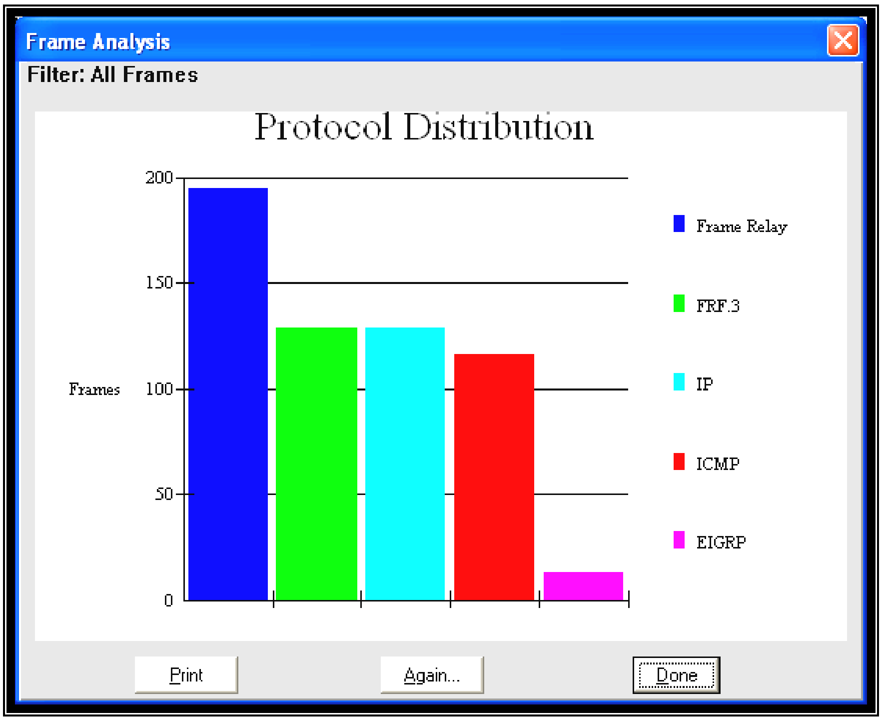
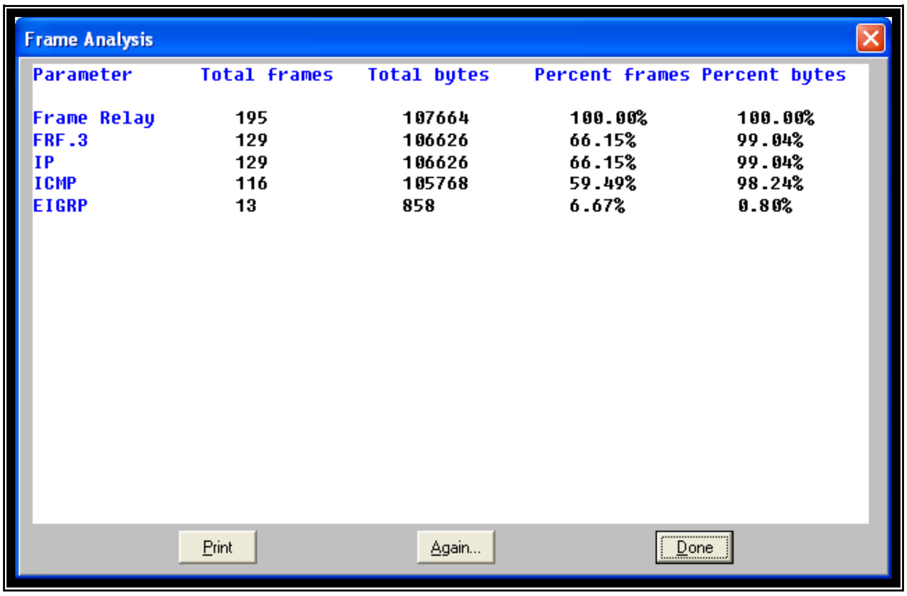



**Figura 4.5.32** Análisis de tráfico por protocolos




| Parameter | Total frames | Total bytes | Percent frames | Percent bytes |
|---|---|---|---|---|
| Frame Relay | 195 | 107664 | 100.00% | 100.00% |
| FRF.3 | 129 | 106626 | 66.15% | 99.04% |
| IP | 129 | 106626 | 66.15% | 99.04% |
| ICMP | 116 | 105768 | 59.49% | 98.24% |
| EIGRP | 13 | 858 | 6.67% | 0.80% |

**Figura 4.5.33** Análisis estadístico por protocolos

**Paso 7: Nivel de trama WAN**

En la siguiente **figura 4.5.34** se puede observar el tamaño de las tramas en el enlace WAN, la cual indica que el mayor porcentaje de las tramas están entre 641 a 1280 bytes.

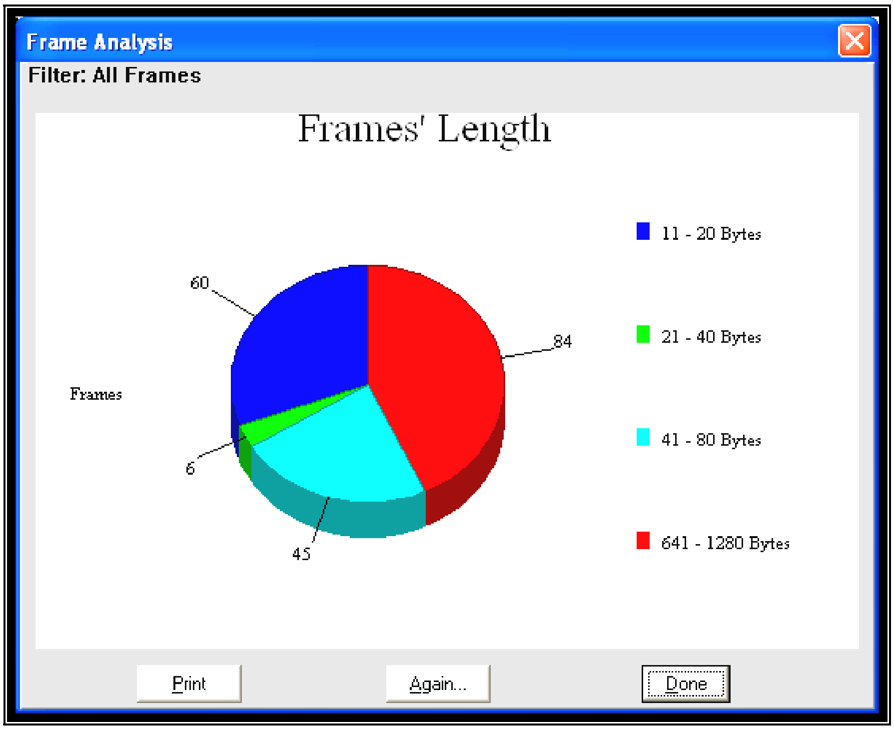



**Figura 4.5.34** Análisis de la longitud de las tramas

### 4.6.- Práctica de Laboratorio de Simulación de ATM

#### 4.6.1.- Descripción general

Esta práctica permite que el estudiante se familiarice con la estructura de la trama ATM, con su PDU de cada una de sus subcapas. Se va analizar la subcapa AAL5 de ATM. Para lo cual se utilizará el software del equipo PrismLite de Radcom.

#### 4.6.2.- Equipos requeridos

- ✓ Un computador con el software del equipo PrismLite

#### 4.6.3.- Descripción del contenido de la práctica.

El software del PrismLite permite capturar datos sin tener una red definida ni equipo físico conectado. Esta herramienta es de ayuda para poder probar las funcionalidades del equipo para capacitación del usuario.

Se utilizara el equipo con un tipo de captura de datos: modo de trama ATM (ATM/SAR). Se analizara los PDU de cada subcapa de ATM.

### 4.6.4.- Desarrollo de la práctica

#### 4.6.4.1.- Proceso de simulación en modo de trama ATM (ATM/SAR)

Para obtener los PDU se procede a inicializar el software PrismLite.

**Paso 1: Ejecutar el programa PrismLite Demo**

En la ventana "configuración demo" en la **figura 4.6.1** en cualquiera de los slot seleccionar "ATM Combo" que corresponde a la tarjeta del equipo y seleccionar en el puerto cualquier interfaz disponible, en este caso se seleccionó el slot 3 y puerto STM-1. Luego de lo cual se debe dar clic en OK.

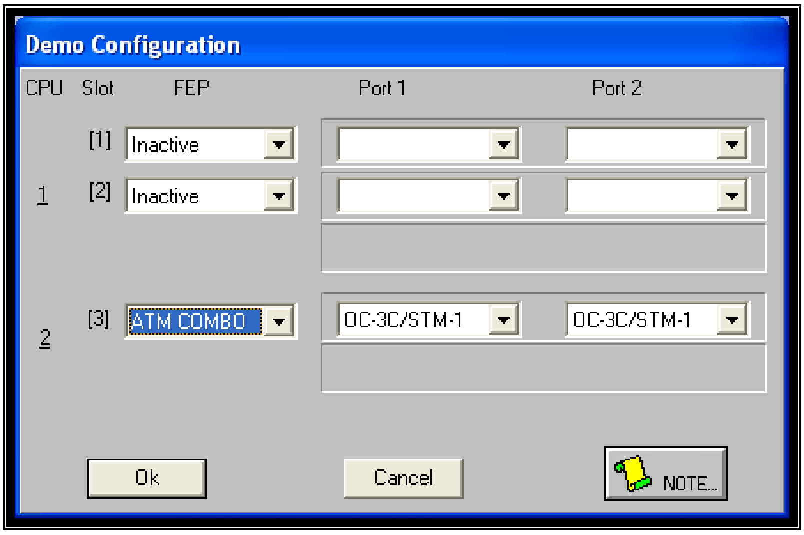



**Figura 4.6.1** Configuración Demo

**Paso 2: Seleccionar el protocolo de pila ATM/SAR**

En el menú "Configuration" seleccionar el canal (ch 3), ver **figura 4.6.2**.

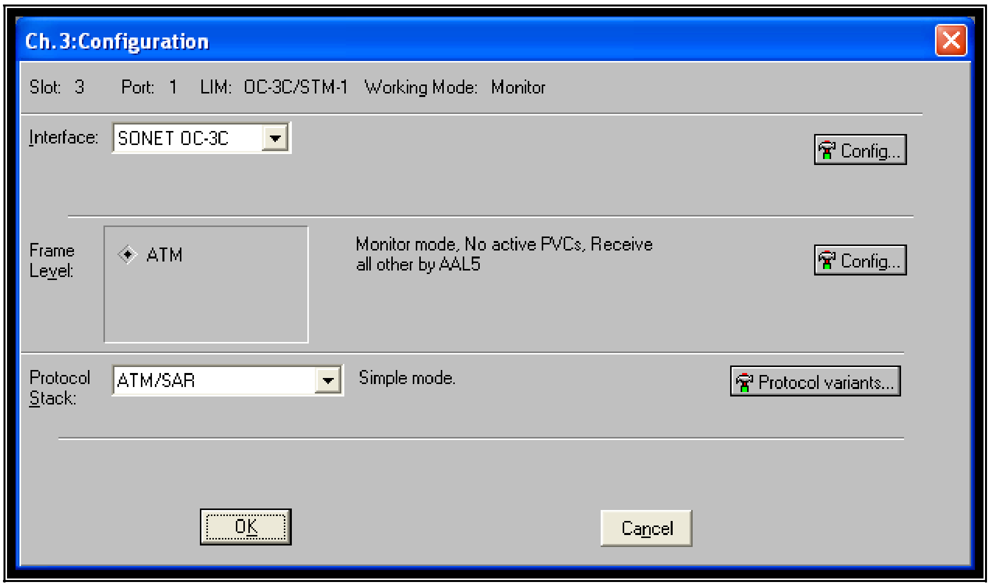



**Figura 4.6.2** Configurar protocolo de pila ATM/SAR

Posteriormente seleccionar ATM/SAR en protocolo de pila.

**Paso 3: Habilitar las ventanas de procesos.**

Para poder habilitar las ventanas para realizar el análisis es necesario ir al menú "Processes" y seleccionar "inicial state". En la ventana "Processes Control" seleccionar "capture" y "analysis", ver **figura 4.6.3**.

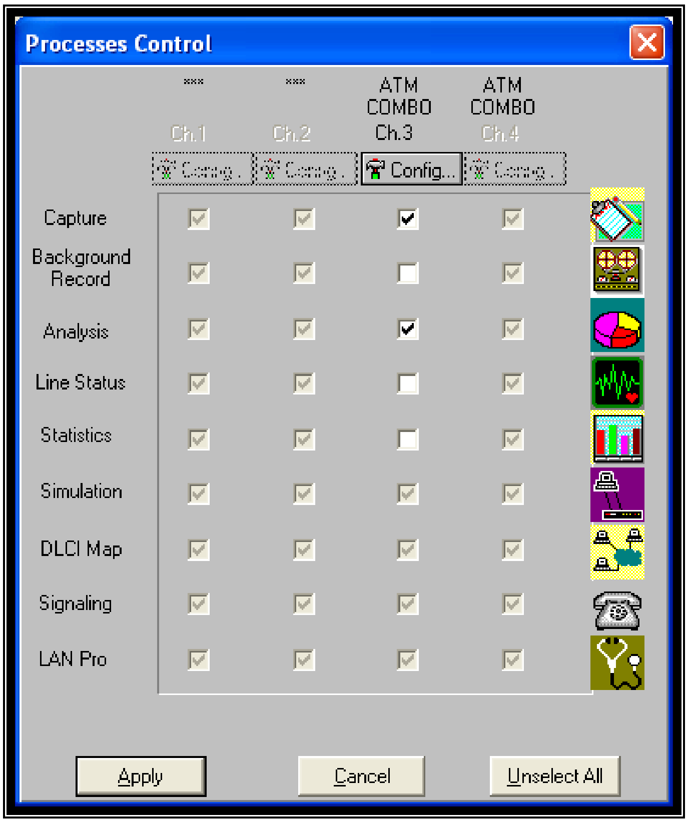



**Figura 4.6.3** Configurar los procesos activos

**Paso 4: Proceso de captura de las tramas**

Se procede a capturar las tramas hasta que el buffer se agote. Para el objetivo de esta práctica es necesario aplicar un filtro para descartar las tramas que no son de interés, en este caso solo se analizarán las tramas con contenido IP, ver **figura 4.6.4**.

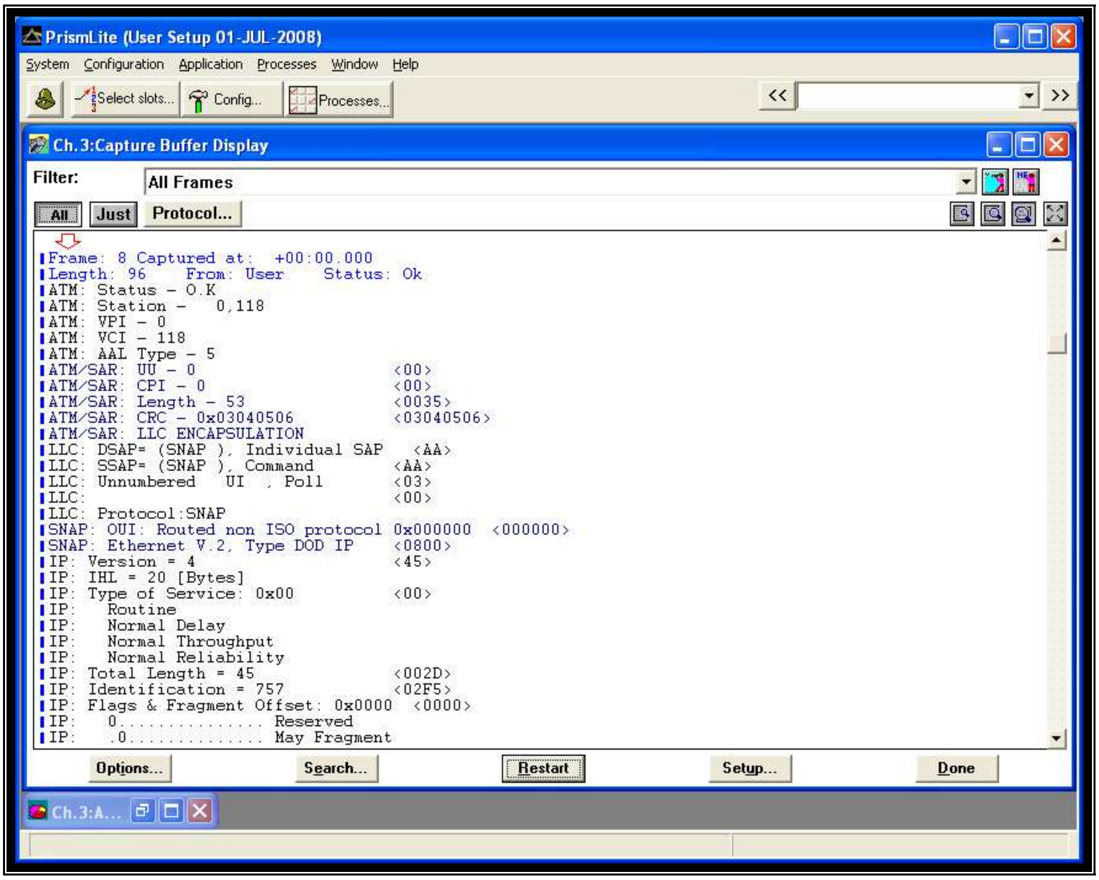



**Figura 4.6.4** Ventana de captura

## Paso 5: Proceso de filtrado de datos

En la ventana de captura se procede a seleccionar en la barra superior la lista despegable y escoge “IP Frames” como se detalla en **figura 4.6.5**. Con esto podemos realizar el análisis de IP sobre ATM.

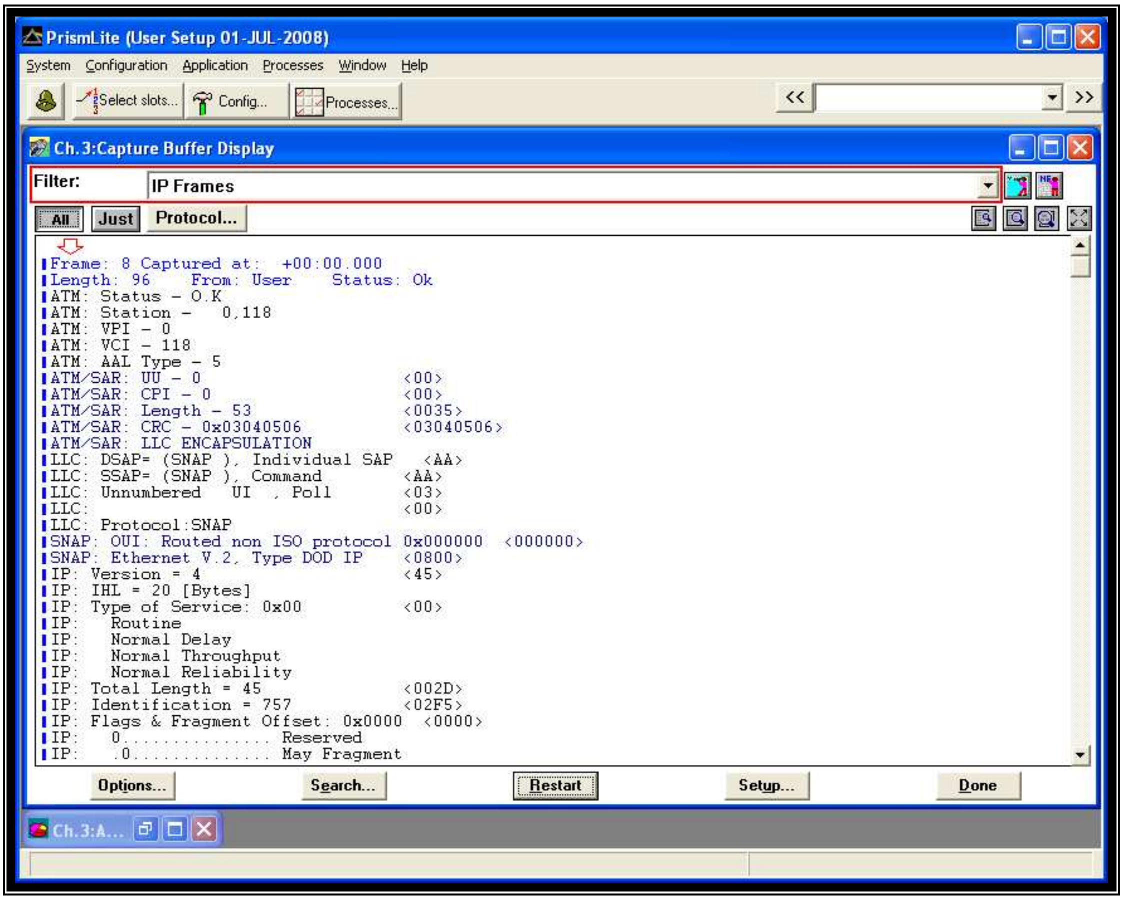



**Figura 4.6.5** Filtrado de tramas

### 4.6.4.2.- Análisis en modo de trama ATM/SAR

Una vez capturada las tramas se procederá a realizar el análisis correspondiente. En la **tabla 4.6.1** se aprecia la primera trama capturada, recordar que ATM trabaja con celdas fijas de 53bytes. El equipo Radcom Prims-Lite está en capacidad de capturar celdas pero se está capturando en modo ATM/SAR; esto es que las celdas han sido reensambladas en SAR-PDU.

**Tabla 4.6.1** Trama capturada

```
Frame: 0 Captured at:  +00:00.000
Length: 96    From: User    Status: Ok                              Datos(53bytes)
ATM: Status - O.K
ATM: Station -   0,118                                              PAD(relleno)
ATM: VPI - 0                                                        35bytes
ATM: VCI - 118
ATM: AAL Type - 5                                                   AAL5(8bytes)
OFFSET DATA                                        ASCII
0000: AA AA 03 00 00 00 08 00 45 00 00 2D 02 F5 00 00  ........E..-....
0010: 3A 06 38 A4 84 42 20 03 84 42 1C AD 00 17 05 FC  :.8..B ..B......
0020: 00 E6 27 BC FF 6F 08 A1 00 00 00 00 41 41 21 21  ..'..o......AA!!
0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0050: 00 00 00 00 00 00 00 00 00 00 00 35 03 04 05 06  ...........5....
```

En el modo de captura de trama ATM, el equipo captura las celdas ATM. Separa y guarda la cabecera ATM de la carga útil (payload) de la celda. En este caso el payload es nombrado SAR-PDU como se muestra en la **figura 4.6.6**.

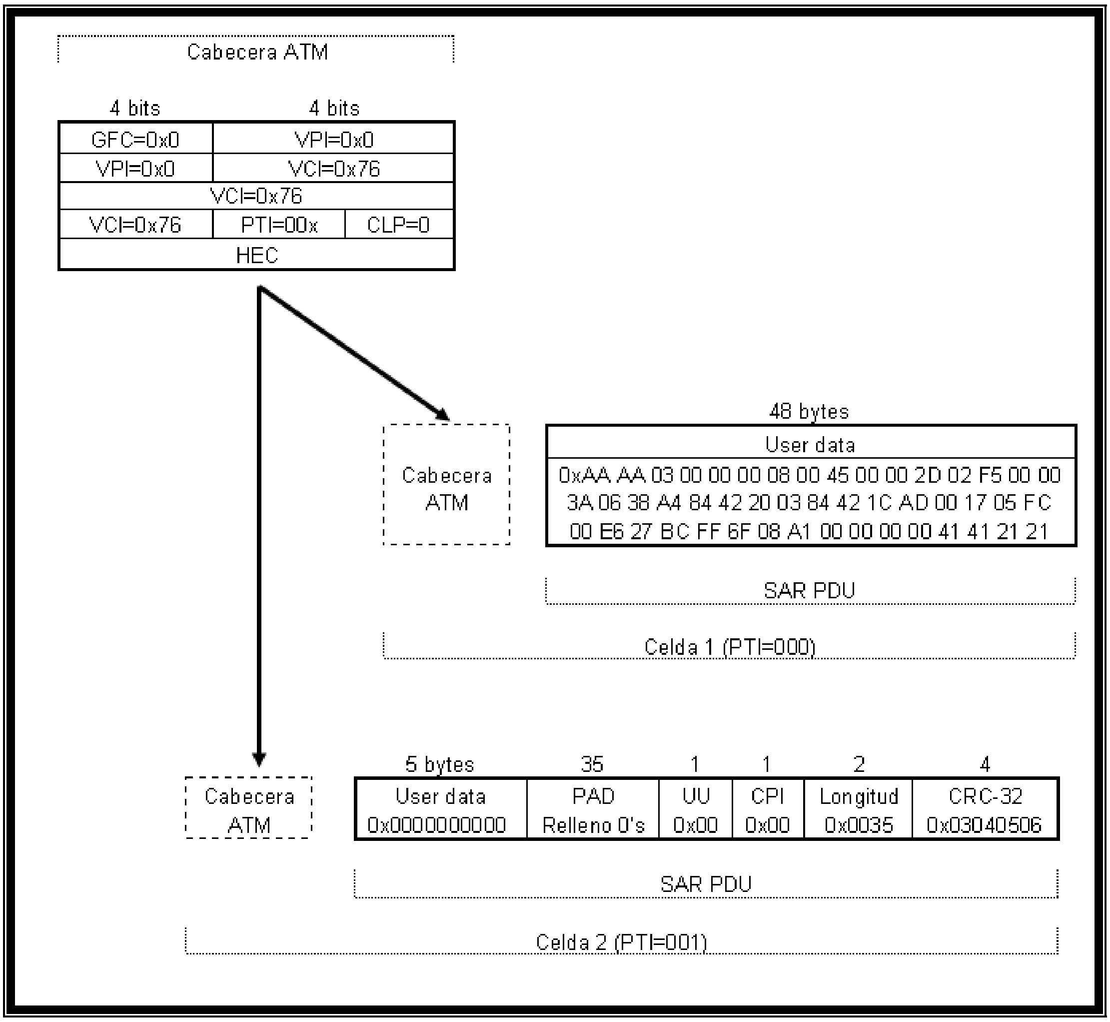



**Figura 4.6.6** Reensamble de celdas en SAR-PDU

Debido a que los datos son de tamaño variable, la subcapa SAR reensambla los SAR-PDU en AAL5-CPCS PDU; esto lo logra debido a que en la cabecera de la celda se encuentra el campo PTI que determina cuando inicia y termina cada AAL5-CPCS; como se muestra en la siguiente **figura 4.6.7**.

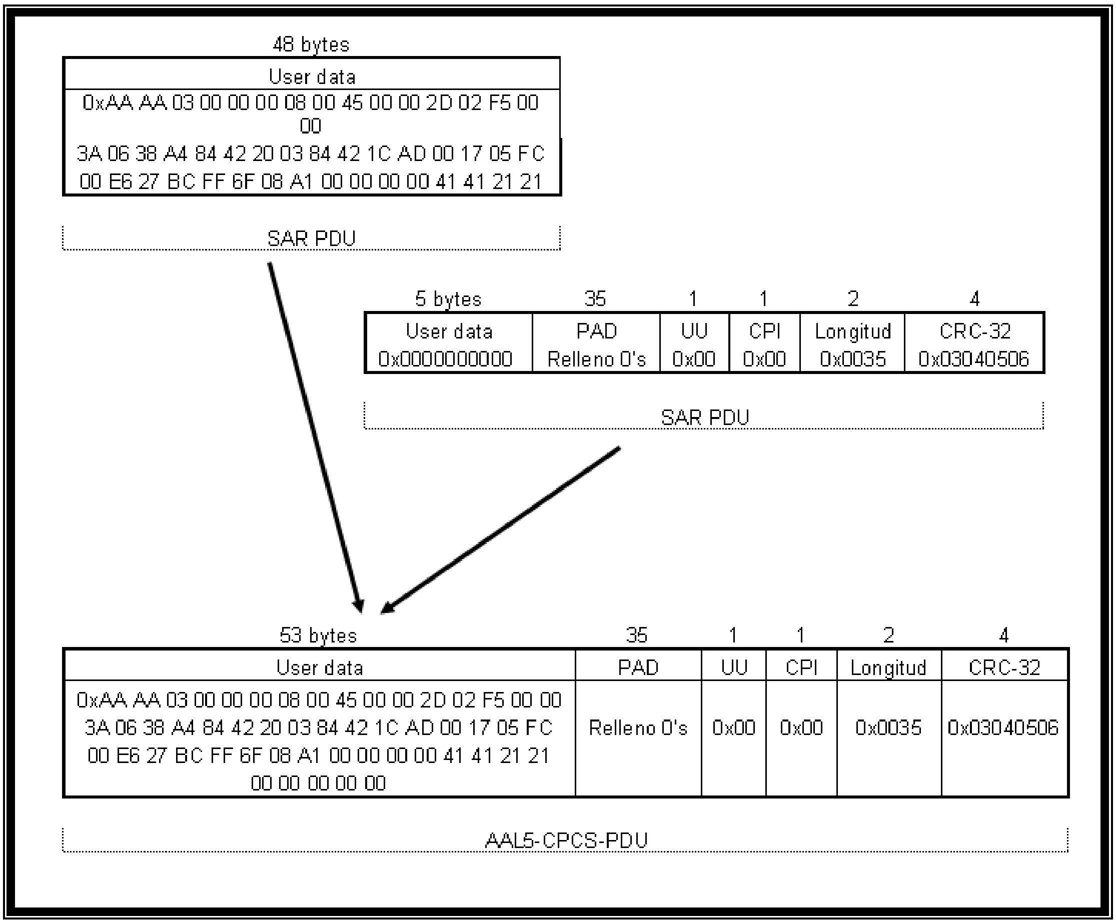



**Figura 4.6.7** Reensamble de SAR-PDU en AAL5-CPCS-PDU

El equipo PrismLite nos muestra el PDU AAL5-CPCS, es decir, el PDU del proceso de la subcapa de convergencia, ver **figura 4.6.8**; debido a que están los datos sin segmentar. En esta además se puede visualizar los campos de la celda ATM como VPI: 0, VCI: 118 y tipo de dato AAL5.

Los ocho bytes finales que se observan en la trama capturada corresponden a campos de la capa de adaptación AAL 5. El primer byte corresponde al campo UU es 0x00, CPI 0x00, LENGTH 0x0035 y CRC-32 0x03040506.

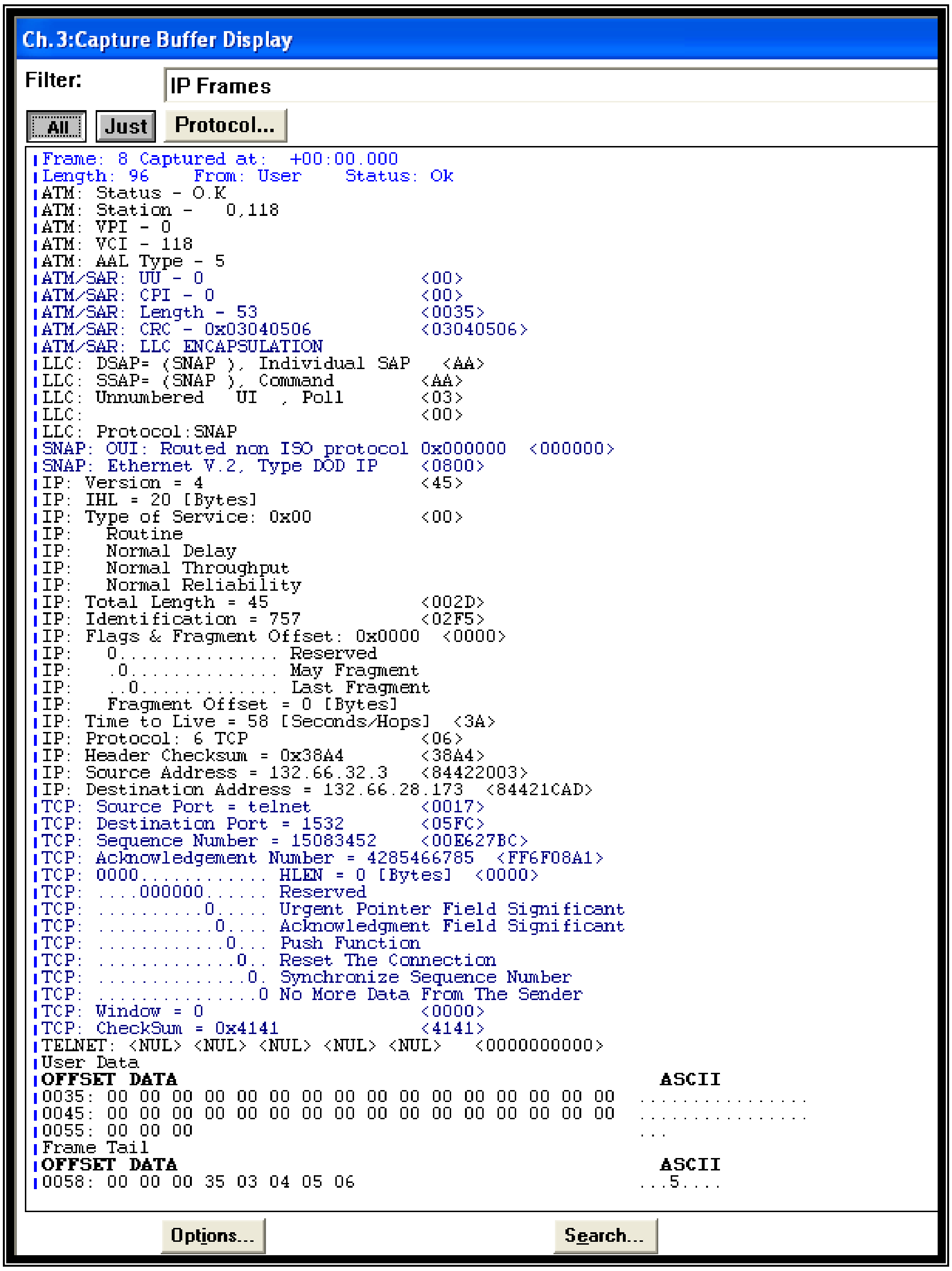



**Figura 4.6.8** Captura de trama

En donde la longitud campo de 2 bytes es 0x0035 cuyo valor en decimal es 53 corresponde a la longitud del tamaño de los datos de la trama CPCS-PDU.

Debido a que en la subcapa SAR el CPCS-PDU debe ser segmentado en tamaños de 48 bytes, es usualmente agregado un relleno de ceros entre el dato de usuario y los campos de adaptación AAL5. Este campo de relleno es llamado PAD y se muestra en la trama en la **tabla 4.6.1**.

**4.6.4.2.1.- Análisis de la red**

El software del equipo Radcom Prism-Lite tiene ventajas debido a que permite analizar los datos capturados con análisis predefinidos (**ver figura 4.6.9**) que se detallan a continuación:

- Distribución de dirección de la trama
- Distribución de la longitud de la trama
- Distribución de status de las tramas
- Distribución del tráfico por tipo AAL
- Distribución del tráfico por VPI
- Distribución de tráfico por VPI/VCI

Se debe tener en cuenta que al aplicar el filtro para solo mantener las tramas de tipo AAL5 se redujo a 8 tramas.

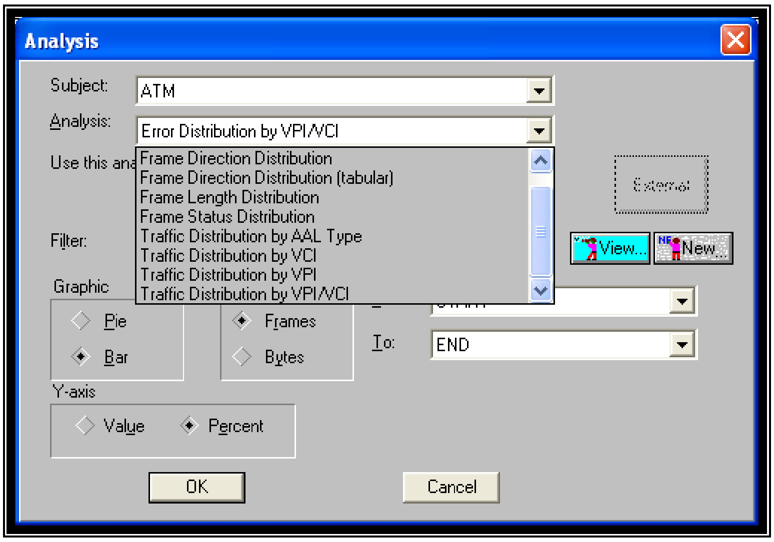



**Figura 4.6.9** Opciones de análisis

**Distribución de dirección de las tramas.** Para poder realiza este análisis se debe seleccionar en la ventana de la figura anterior "Frame Direction Distribution", luego se presenta la ventana como en la **figura 4.6.10**. Es decir tenemos 5 tramas transmitidas y 3 tramas recibidas desde la red.

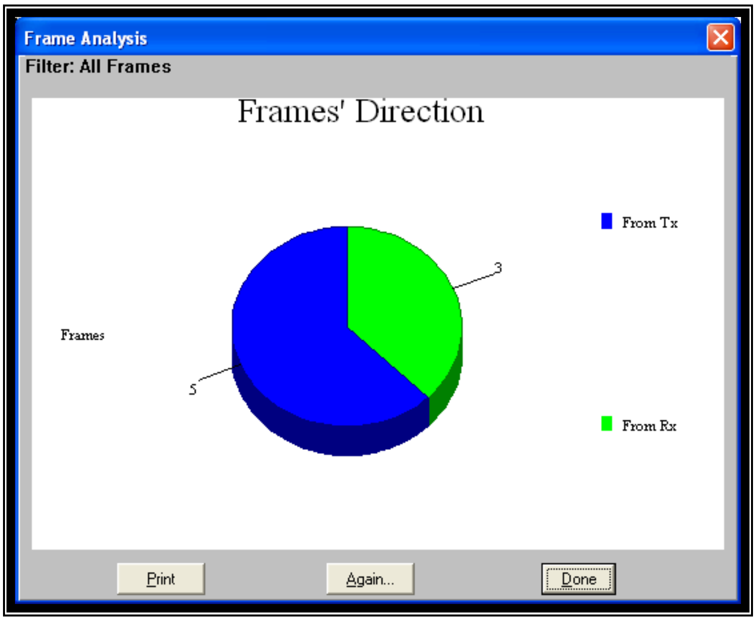



**Figura 4.6.10** Distribución de la dirección de la trama

**Distribución de la longitud de las tramas.** En la **figura 4.6.11** se debe tener en cuenta que en modo ATM/SAR se capturan tramas PDU AAL5-CPCS, por lo tanto; tiene tamaño variable dado a que es el PDU de la subcapa de convergencia.

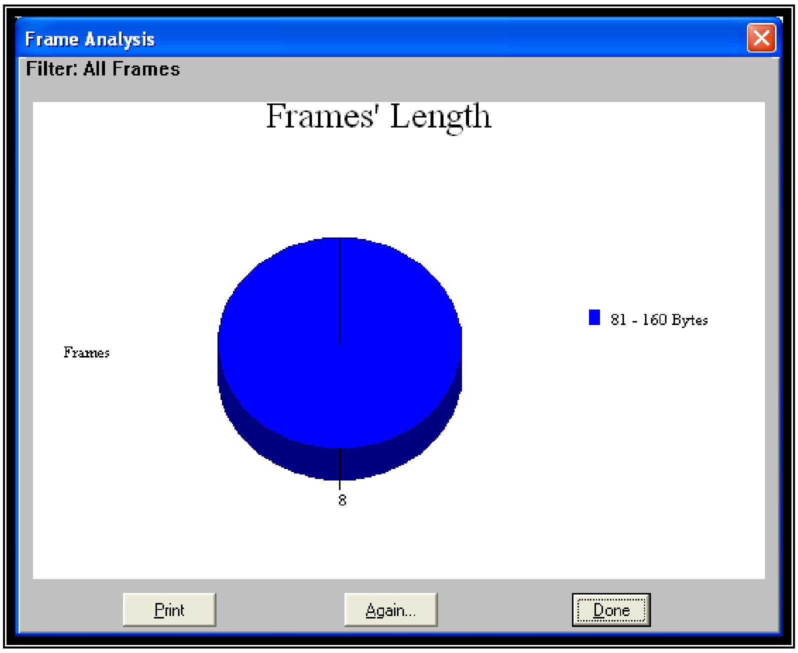



**Figura 4.6.11** Distribución de la longitud de las tramas

**Distribución del status de las tramas.** La **figura 4.6.12** indica que ninguna celda ni trama ensamblada contiene errores y por lo tanto su campo de comprobación HEC es correcto.

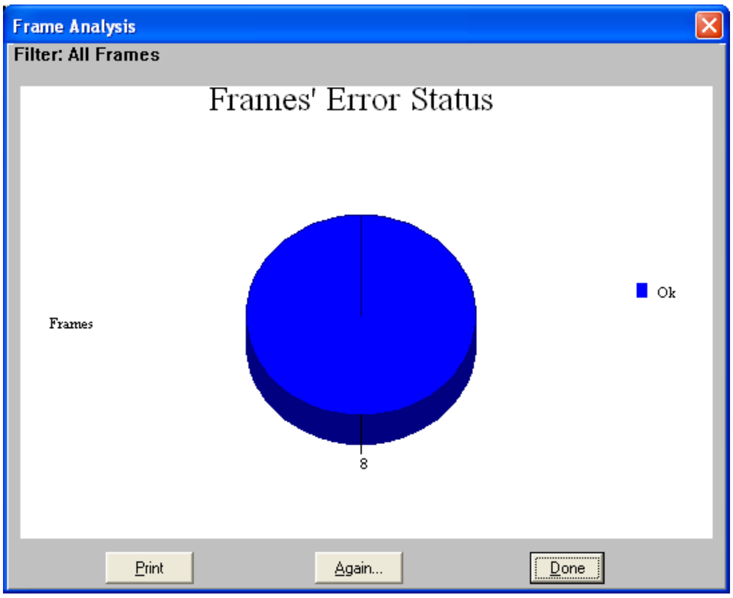



**Figura 4.6.12** Distribución del status de las tramas

**Distribución del tráfico por tipo de AAL.** En la **figura 4.6.13** dado a que se filtro las tramas capturadas se comprueba que solo hay tramas con PDU tipo AAL 5.

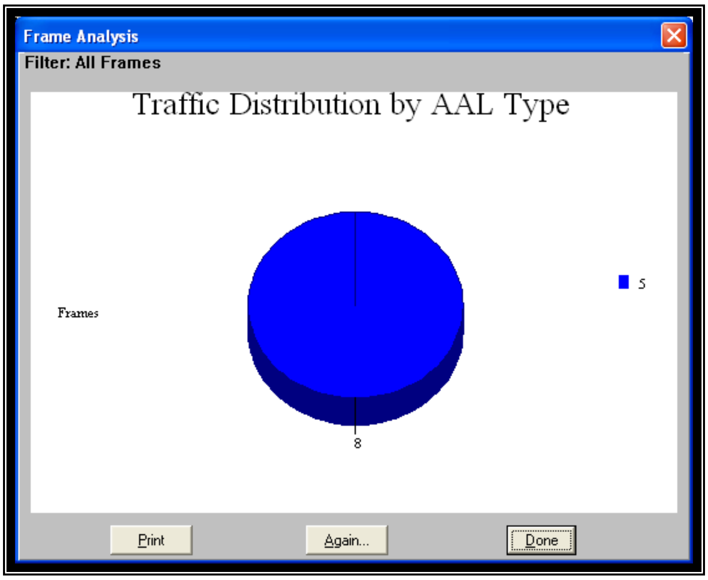



**Figura 4.6.13** Distribución del tráfico por tipo de AAL

**Distribución del tráfico por VPI.** La **figura 4.6.14** muestra que solo tenemos 8 tramas con VPI: 0.

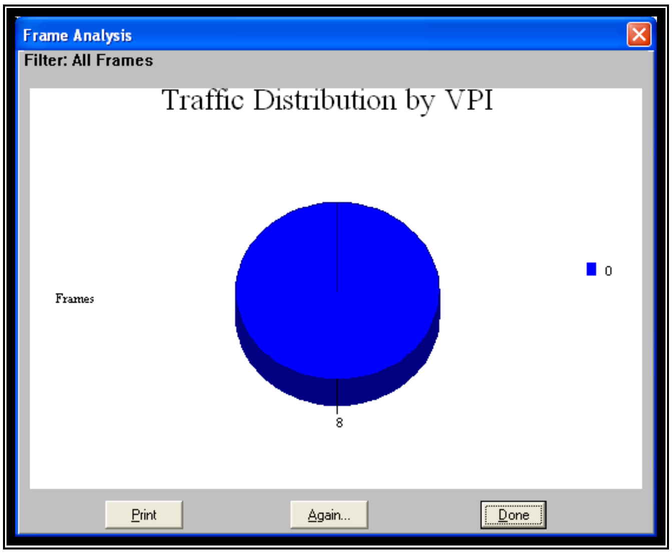



**Figura 4.6.14** Distribución del tráfico por VPI

**Distribución del tráfico por VPI/VCI.** La **figura 4.6.15** nos detalla cuantas tramas hay en el conjunto de VPI/CI, en este caso en particular 8 tramas con VPI: 0, VCI:118

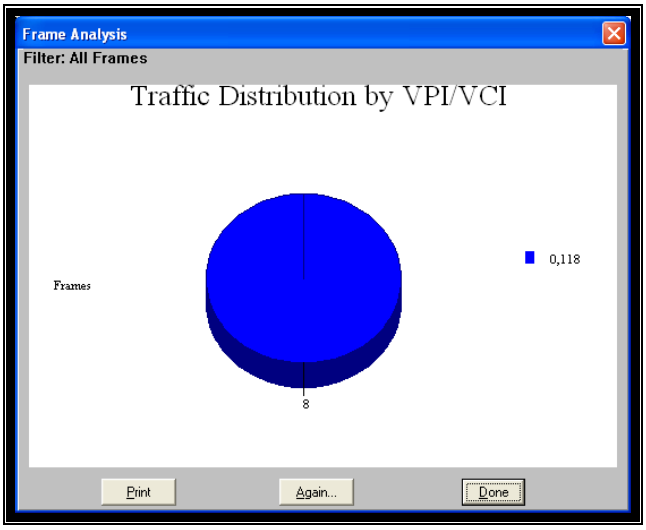



**Figura 4.6.15** Distribución del tráfico por VPI/VCI

# CAPÍTULO 5

## 5. Costos de la implementación de un laboratorio

En el capítulo anterior se detalló los equipos utilizados en cada laboratorio realizado, entre estos se encuentran ruteadores Cisco de series 1601 y 805; los cuales a la actualidad se encuentran descontinuados en venta y soporte por parte del fabricante. Debido a esto se han cotizado ruteadores Cisco de serie 1841 y 2811 para poder incrementar en un futuro la complejidad de laboratorios y sus respectivos análisis.

El analizador de protocolos utilizado en los laboratorios es un Radcom RC-100WL, el cual se encuentra descontinuado en venta y soporte. Se cotizó el analizador Radcom Prism UltraLite con mejoras en su software de captura y análisis. Es muy importante recalcar que este equipo tiene interfaces LAN incorporadas y para análisis de éste no es necesario comprar interfaces.

Se debe recalcar que solo se detallan costos de equipos ruteadores y analizador de protocolos, no se detalla costo de computadores que intervienen en las pruebas ni equipamiento adicional.

## 5.1.- Descripción de los componentes del laboratorio.

En cada laboratorio se ha implementado una red sencilla para su rápido análisis y comprensión. Por esto se ha seleccionado 3 ruteadores Cisco, 2 de las series 1841 y 1 de la serie 2811.

Se detalla la descripción de los componentes:

**Analizador Radcom Prism UltraLite**: Posee 2 canales de operación simultanea, el procesamiento, estadísticas, filtros, captura de datos directamente a disco duro y el análisis se puede obtener en tiempo real y offline. Soporta agregar paquetes de software opcionales para simulaciones de protocolos específicos.

El equipo soporta más de 600 protocolos incluyendo:

WAN/LAN: HDLC, SDLC, LAPD, Frame Relay, ISDN, PPP, ATM, MPLS, LDP, RSVP, VLAN, Ethernet, IP.

VoIP: H.323, H.225, H.450, RTP, RTCP, SIP.

Cellular: GSM, CDMA, GPRS, WAP.

SS7: MTP2, MTP3, MAP, SCCP.

**Ruteador Cisco 1841**: Este ruteador de servicios integrados soporta lo siguiente:

Soporta altas velocidades para tarjetas de interfaz WAN/E1/T1.

Protección de la inversión inicial del equipo mediante incremento en desempeño y modularidad.

Incremento de densidad a través de interfaces WAN de alta velocidad.

Soporta alrededor de 90 módulos o interfaces.

Dos puertos FastEthernet integrados.

Soporta un conjunto completo de protocolos de transporte, calidad de servicio y seguridad en la red.

**Ruteador Cisco 2811**: Este modelo es parte del portafolio de ruteadores de servicios integrados por lo cual posee las características del ruteador 1841 mas las detalladas a continuación:

Diseño modular, protección firewall, cifrado del hardware, soporte de VPN/MPLS, Quality of Service (QoS).

Diseño modular que permite hasta 4 tarjetas HWIC,WIC,VIC o VWIC.

Soporta 1 slot para modulo NM o NME.

## 5.2.- Cálculos y análisis generales de los costos

En cada laboratorio se ha implementado una red sencilla para su rápido análisis y comprensión. Por esto se ha seleccionado 3 ruteadores Cisco, 2 de las series 1841 y 1 de la serie 2811, de los cuales se detallan los costos a continuación en la **tabla 5.1**.

**TABLA 5.1** Costo de ruteadores Cisco y adicionales.

| Código Equipo | Descripción | Cantidad | P. Unitario | Total |
|---|---|---|---|---|
| Serie 1841 | Ruteador de servicios integrados 1841 con 2 puertos FE, IOS:c1841-advipservicesk9-mz | 2 | $1352 | $2.740 |
| Serie 2811 | Ruteador de servicios integrados 2811 con 2 puertos FE, IOS:Cisco 2800 IP Base | 1 | $2420 | $2.420 |
| WIC-2T | Tarjeta de interface serial WAN | 4 | $387 | $1.548 |
| CAB-SS-V35MT | Cable V.35 smart serial DTE | 2 | $82 | $164 |
| CAB-SS-V35FC | Cable V.35 smart serial DCE | 2 | $82 | $164 |
| Total | | | | $7.036 |

Detallar el costo de un analizador de protocolos es mas complejo, se necesita conocer cuales son las interfaces necesarias, el paquete de software adicional para analizar cada protocolo, el desbloqueo para utilizar dos interfaces a la vez, software para simulación y varias mas que se detallan a continuación en la **tabla 5.2**.

**TABLA 5.2** Costo de equipo Analizador de protocolos Radcom.

| Código Equipo | Descripción | P. Unitario |
|---|---|---|
| Prism UltraLite | WAN/LAN analyzer stand-alone basic unit including:<br>HDLC, SDLC, LAPB and LAPD decoding, ASYNC, transparent, Frame Simulation, Burst simulation, BERT.<br>Ethernet and Tokeng Ring decoding.<br>X.25 monitoring and simulation. | $ 8.000 |

| | | |
|---|---|---|
| | Two external Triggers, computer cable, power supply unit, power supply cable.<br>Complete set of manual. | |
| Software Options | | |
| RC-PUL-FRA | Frame Relay analysis - Single Channel | $ 1.395 |
| RC-PUL-FRS | Frame Relay Simulation | $ 1.395 |
| RC-PUL-EA | Encapsulation Protocol Analysis | $ 1.540 |
| RC-PUL-A2CH | Upgrade from one channel to two channel | $ 1.200 |
| Interfaces Modules | | |
| RC-WL-MTYP | RS-449/RS-530/X.21/V.24 Interface - single channel | $ 730 |
| RC-WL-E1 | G.703 E1 interface- single channel | |
| Cables | | |
| RC-WL-V35C | V.35 Monitor Cable - single channel | $ 195 |
| RC-WL-V35S | V.35 Simulation Cable - single channel | $ 95 |
| Total | | $ 15.240 |

El analizador Radcom es una herramienta que se puede adaptar a las nuevas tecnologías solo se necesita agregar el software que se necesita como por ejemplo análisis de protocolo MPLS, protocolos de VoIP y más.

# Conclusiones

1) En el desarrollo de la tesis se ha implementado un procedimiento con el analizador de protocolos RC-100 WL para los laboratorios de simulación del protocolo HDLC, simulación del protocolo MAC/IP, simulación del protocolo Frame Relay, y un procedimiento diferente con el software demo del Radcom Prism-Lite para la simulación del protocolo ATM, con la finalidad de que el estudiante se familiarice con las herramientas utilizadas para poder analizar, simular y comprender la estructura de los protocolos e interpretar como las tramas viajan por una red.

2) En los laboratorios que se utiliza el equipo Radcom RC-100 WL se procedió con la configuración de equipos ruteadores para obtener la red que se desea implementar, se realizan pruebas de conectividad luego de lo cual se procede con la captura de datos en tiempo real y su respectivo análisis de las primeras tramas y graficación de todos los datos capturados con gráficos pre-establecidos.

3) Además se utiliza el programa gratuito Packet Builder disponible en internet que es una herramienta útil y fácil para la creación de paquetes de red y en las prácticas se lo utilizo para enviar paquetes ICMP y poder encapsular dentro de los protocolos analizados.

4) El equipo Radcom RC-100WL es una herramienta que teniendo la licencia de simulación permite generar tráfico, aleatorio o definido por usuario con diversas protocolos como Ethernet, Frame Relay, pero debido a la falta de licencia en el hardware nos decidimos por utilizar el programa Packet Builder anteriormente detallado.

5) En la práctica de laboratorio de simulación Frame Relay con analizar su cabecera se puede diferenciar si el campo de información corresponde a mensajes de señalización o datos del usuario identificando el DLCI utilizado en la trama, además en los mensajes de señalización se identifica que LMI se esta utilizando, en los datos del usuario se analiza el protocolo superior encapsulado.

6) En la práctica de laboratorio de simulación HDLC se implementa una red con dos ruteadores y se comprobó la estructura de la trama cHDLC de Cisco Systems; que es una extensión del protocolo HDLC que utiliza sistema de verificación del estado del enlace mediante mensajes keep-alive.

7) En la práctica IP se detalló la encapsulación de IP sobre Ethernet. Se analizó las distintas tramas, broadcast, unicast y multicast. Se revisó el campo tipo de servicio, para verificar las prioridades de los paquetes IP.

8) En IP se analizo las tramas ICMP, se observo la fragmentación de los paquetes IP. Se determinó la actividad de tráfico de los equipos.

9) El analizador comprobó en las capturas de las tramas que no hubo tramas erróneas. Además se observó la distribución de los protocolos que interactúan en la red.

10) En la práctica de laboratorio de ATM unos de los problemas encontrados fue que el analizador utilizado en los laboratorios no tiene capacidades para analizar una red ATM y además no se disponía de una red básica de ATM para su análisis por tal motivo se utilizó un demo que permite probar las capacidades del analizador antes de proceder con la compra del analizador Prism Lite.

11) En ATM se analiza la subcapa AAL5 debido a que permite trabajar con protocolos no orientados a conexión, en nuestro caso protocolo IP.

12) En el desarrollo de nuestra tesis un obstáculo es que debido a la demanda de un analizador de protocolos en las empresas que lo poseen; tuvimos que regirnos a la poca disponibilidad del mismo y aprovechar al máximo esta herramienta.

13) El analizador de protocolos utilizado en los laboratorios es un equipo que tiene ciertas carencias en ATM y en IPv6, actualmente ha sido reemplazado por el analizador Ultra Prism Lite que posee mejoras para el análisis de una red de datos.

# Recomendaciones

1) Se recomienda utilizar los procedimientos con el programa Dynamips debido a que este permite capturar el tráfico que viaja a través de las interfaces de los ruteadores. Esto es muy recomendado para poder visualizar la estructura de las tramas, aunque no permite capturas sobre interfaces ATM.

2) Se recomienda que luego de tener los conocimientos básicos de análisis se proceda a implementar redes complejas para su respectivo análisis.

3) Se recomienda a la universidad implementar un laboratorio de redes para simular y analizar protocolos de comunicaciones, dado que es muy utilizado por instituciones de control como Senatel/Conatel y Supertel.

# BIBLIOGRAFIA


[1] IP/MPLS Forum. "Frame Relay Forum Implementation Agreements". http://www.ipmplsforum.org/tech/fr_ia.shtml

[2] RFC 791. IP. http://www.rfc-editor.org/rfc/rfc791.txt

[3] RFC 792. ICMP. http://www.rfc-editor.org/rfc/rfc792.txt

[4] RFC 826, 923. ARP – RARP. http://www.rfc-editor.org/rfc/rfc826.txt

[5] Cisco System, Inc. CCNA Curriculum v3.1. http://cisco.netacad.net

[6] Cisco System, Inc. "Asynchronous Transfer Mode (ATM) Switching". http://www.cisco.com/en/US/docs/internetworking/technology/handbook/atm.html

[7] Cisco System, Inc. "Internet Protocols (IP)". http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Internet-Protocols.html

[8] Cisco System, Inc. "Frame Relay". http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Frame-Relay.html

[9] Cisco System, Inc. "Ethernet". http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Ethernet.html

[10] Todd Lammle. "Cisco CCNA Study Guide", Editorial Sybex. Quinta edición. Capitulo 2, 11.

**[11]** Angela Orebaugh. “Wireshark and Ethereal Network Protocol Analyzer Toolkit”. Editorial Syngress. Capitulo 1, 2.

**[12]** Wendell Odom, “CCIE Routing and Switching”. Editorial Cisco. Tercera edición. Capitulo 1, 4, 15.

**[13]** Laura Chappell’s Lab kit. Versión 9. http://www.novell.com/ncmagopenxtest/laurachappell.html

**[14]** Rad Tutorials. “ATM”. http://www2.rad.com/networks/infrastructure/atm/main.htm

**[15]** Rad Tutorials. “Packet Switching”. http://www2.rad.com/networks/2004/PacketSwitching/main.htm

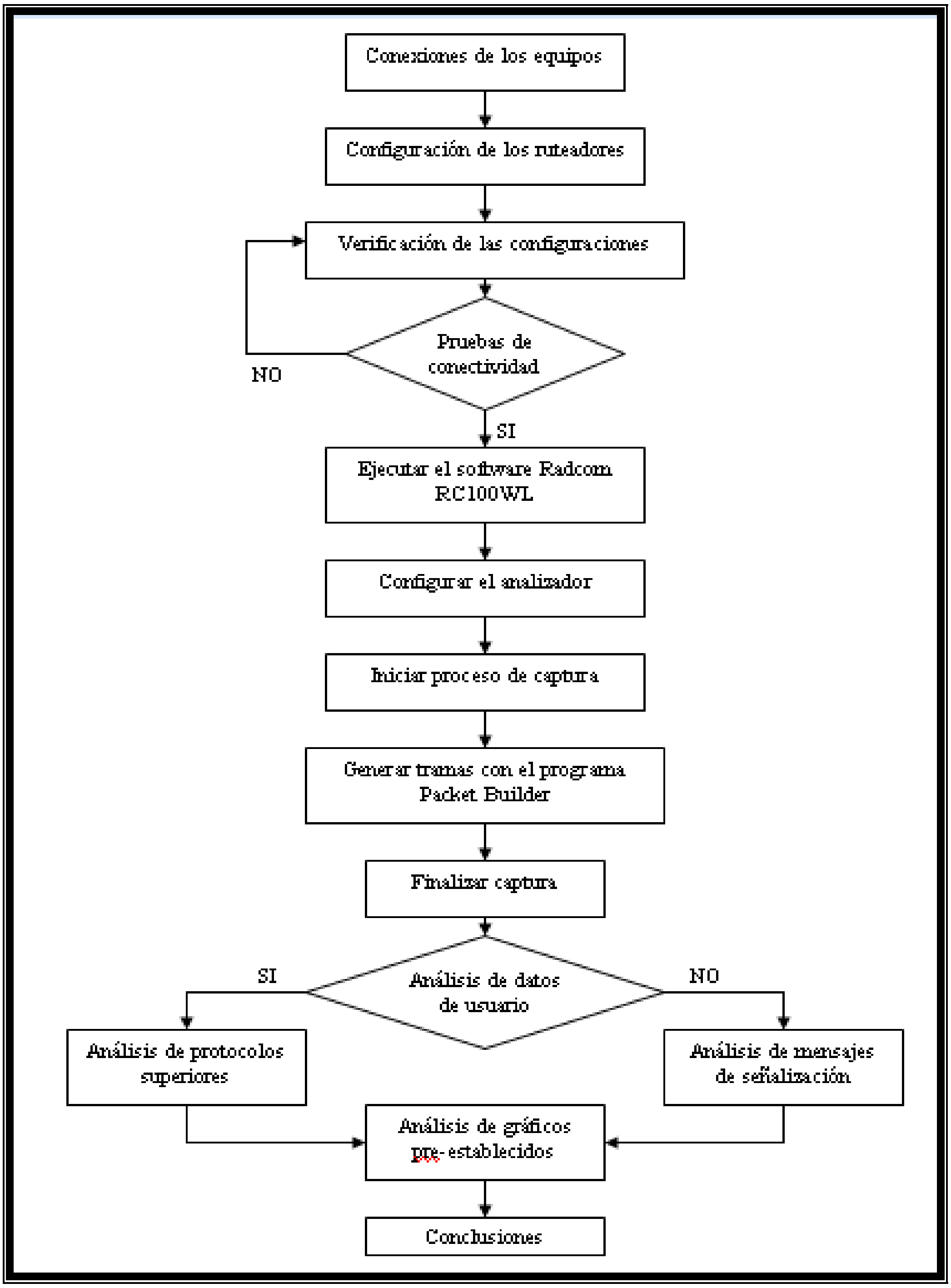
**[16]** Programa Wireshark. http://www.wireshark.org

**[17]** Programa Packet Builder. http://www.engagesecurity.com/products/engagepacketbuilder/

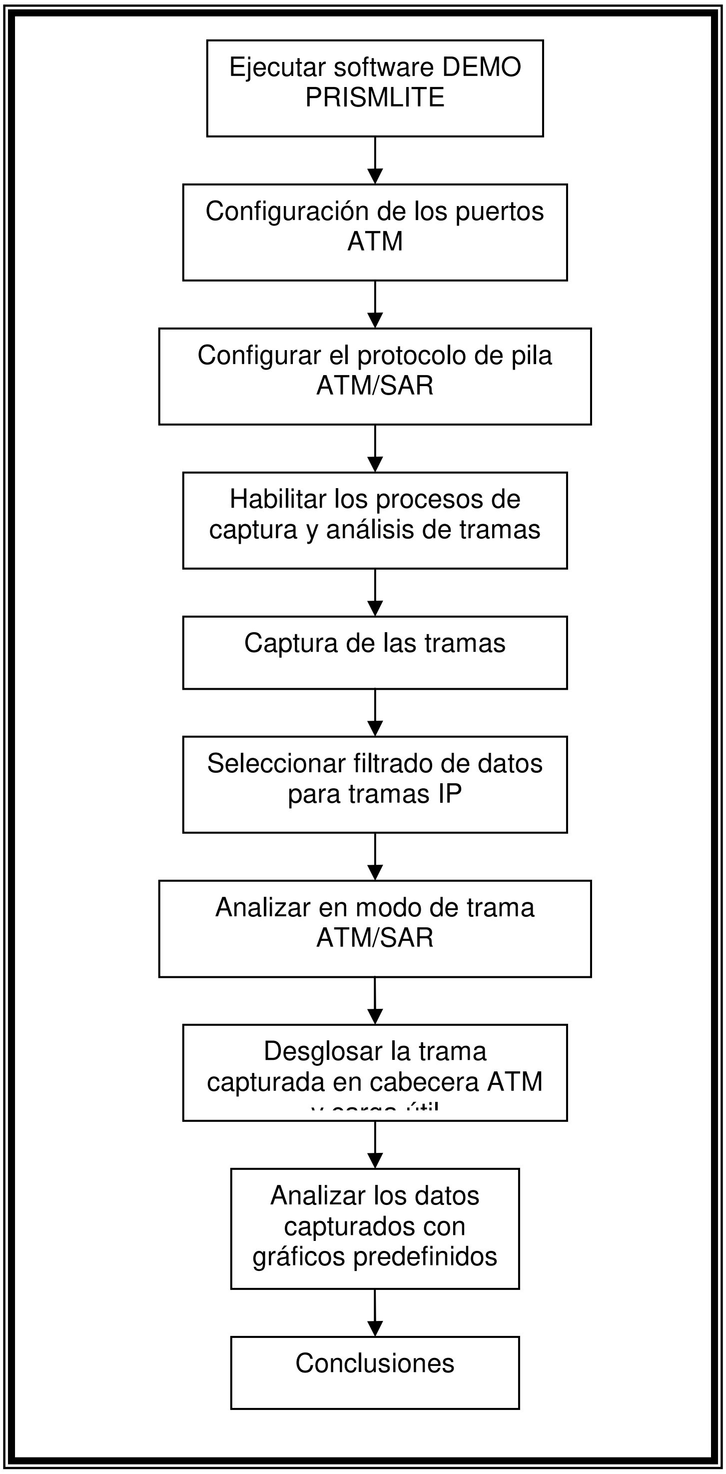
**[18]** Radcom Ultra Prism Lite. http://www.radcom.com/LeadForm1.aspx?BoneId=381&ObjID=-1&staticname1=2&FileName=632616552728437500125.pdf

**[19]** Programa Dynamips. http://www.ipflow.utc.fr/index.php/Cisco_7200_Simulator

## Anexo A. Procedimientos en laboratorios MAC, IP, HDLC y Frame Relay



## Anexo B. Procedimientos en laboratorio ATM



# ABREVIATURAS

**OSI:** Interconexión de Sistemas Abiertos.

**ISO:** Organización Internacional de Normalización.

**DCE:** Data Circuit-Terminating Equipment.

**DTE:** Data Terminal Equipment.

**FR:** Frame Relay

**OSI:** Open System Interconnection. Interconexión de Sistemas Abiertos.

**WAN:** Wide Area Network**.**

**HDLC:** High-Level Data Link Control

**cHDLC:** Cisco High-Level Data Link Control

**SLARP:** Serial Line Address Resolution Protocol

**LABF:** Link Access Procedure for Frame.

**DTE**: Data Terminal Equipment.

**DCE:** Data Communications Equipment

**LAN:** Local Area Network**.**

**FRAD:** Frame Relay Access Device o Frame Relay Assembler/Disassembler.

**DLCI:** Data Link Connection Identifier

**FCS:** Frame Check Sequence

**CR:** Comando / Respuesta

**EA:** Extended Address

**FECN:** Forward Explicit Congestion Notification, Notificación de congestión explicita hacia el destino

**BECN:** Backward Explicit Congestion Notification, Notificación de congestión explicita en el retorno

**DE:** Discard Elegibility

**PAD:** Campo de Relleno.

**NLPI:** Network Layer Protocol Identifier**.** Identificador de Protocolo de Nivel de Red.

**UIT:** Unión Internacional de Telecomunicaciones**.**

**CIR:** Committed Information Rate, tasa de información comprometida

**Be:** Excess Burst Size, ráfaga en exceso

**Bc:** Committed Burst Size, ráfaga comprometida

**LMI:** Local Manager Interface. Interfaz de administración Local.

**ANSI:** American National Standars Institute. Instituto Nacional Americano de Estándares.

**ARP:** Address Resolution Protocol

**ATM:** Asynchronous Transfer Mode (Modo de transferencia asincrónica)

**TC:** Transmission Convergence Sublayer (Subcapa de transmisión y convergencia)

**PM:** Physical Medium Sublayer (Subcapa del medio físico)

**UNI:** User-Network Interface (Interfaz usuario-red)

**NNI:** Network-Network Interface (Interfaz red-red)

**CS:** Convergence Sublayer (Subcapa de convergencia)

**SAR:** Segmentation and Reassembly Sublayer (Subcapa de segmentación y reemsamblado)

**VCC:** Virtual channel connection (conexión de canal virtual)

**VPC:** Virtual path connection (conexión de camino virtual)

**AAL:** ATM Adaption Layer (Capa de adaptación ATM)

**GFC:** Generic Flow Control (Control de flujo genérico)

**VPI:** Virtual Path Identifier (Identificador de camino virtual)

**VCI:** Virtual Channel Identifier (Identificador de canal virtual)

**PT:** Payload Type (Tipo de carga útil)

**CLP:** Cells Loss Priority (Prioridad de pérdida de celdas)

**HEC:** Header Error Control (Control de error de cabecera)

**CRC:** Cyclic Redundant Code (Código de redundancia cíclica)

**SDH:** Synchronous Digital Hierarchy (Red Óptica Síncrona)

**SONET:** Synchronous Optical Network (Jerarquía Digital Síncrona)

**PDU:** Protocol Data Unit (Unidad de Protocolo de Datos)