ESTUDIO DEL EQUIPO INTERNET ADVISOR WAN HP J2300D Y DISEÑO DE PRÁCTICAS DE LABORATORIO

HERNANDO ARGUMERO CORTÉS

VÍCTOR ANDRÉS CASAMACHÍN FERNÁNDEZ

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DEPARTAMENTO DE TELECOMUNICACIONES

POPAYÁN

2002

ESTUDIO DEL EQUIPO INTERNET ADVISOR WAN HP J2300D Y DISEÑO DE PRÁCTICAS DE LABORATORIO

HERNANDO ARGUMERO CORTÉS

VÍCTOR ANDRÉS CASAMACHÍN FERNÁNDEZ

Trabajo de grado presentado como requisito para optar al título de Ingeniero en Electrónica y Telecomunicaciones

Director: IE. Mag. FRANCISCO JAVIER TERÁN CUARÁN

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DEPARTAMENTO DE TELECOMUNICACIONES

POPAYÁN

2002

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

INTRODUCCIÓN

El avance tecnológico en la interconexión de redes y la comunicación entre procesos de diferentes plataformas de redes a nivel LAN y WAN, como también el crecimiento y exigencia de nuevos y mejores servicios en las redes telemáticas, hacen cada día más complejo el análisis del tráfico en estas redes para poder prestar un servicio óptimo, especialmente cuando en la tecnología están involucradas distintas arquitecturas de redes que operan con diversos stacks de protocolos, tanto de transporte como de enrutamiento.

Con el presente trabajo de grado se ha realizado un estudio detallado del equipo Internet Advisor WAN HP J2300D que permite conocer la gama de funcionalidades, características y aplicaciones que posee y explotar toda su potencialidad en el análisis y gestión de redes telemáticas con el fin de definir, diseñar e implementar un conjunto de prácticas de laboratorio que den soporte a las materias de énfasis y electivas del Departamento de Telecomunicaciones dentro del actual plan de estudios del Programa de Ingeniería Electrónica y Telecomunicaciones, como también soportar la parte práctica de algunas asignaturas del Programa de Especialización en Redes y Servicios Telemáticos.

En primera instancia, el capítulo uno hace una breve presentación del Analizador de Protocolos Internet Advisor WAN HP J2300D, destacando sus capacidades y modos de operación, luego se describen las características hardware del equipo, su módulo especial de adquisición y transmisión de datos J3444A Fast Ethernet y los módulos de interfaz J2904B ISDN BRI S/T y J2296B E1/ISDN SIM BNC. Seguidamente se explica la interfaz de usuario correspondiente al software LAN y la conformación y funcionalidad de cada una de sus medidas, se hace una descripción general de todas las capacidades que proporcionan el software WAN y ATM y posteriormente se muestran los parámetros y opciones requeridos para una configuración software apropiada.

El segundo capítulo presenta las prácticas de laboratorio divididas en tres entornos: LAN, WAN y Acceso Telefónico Remoto, las cuales se han realizado utilizando la infraestructura de la Red de Datos de la Universidad del Cauca y los equipos pertenecientes al Laboratorio de Telemática del Departamento de Telecomunicaciones. Éstas están diseñadas con el propósito de aumentar la base de

conocimiento y/o experiencia de los estudiantes que las realicen en el análisis, monitoreo, supervisión, diagnóstico y actividad de las redes telemáticas como también en el estudio y análisis de tráfico de los diversos stacks de protocolos.

1. INTRODUCCIÓN AL EQUIPO INTERNET ADVISOR WAN HP J2300D

En este capítulo se proporciona una descripción del Analizador de Protocolos a nivel hardware y software. Se da una visión global del equipo, los modos de conexión que posee, se describen las partes que lo componen y se ilustra el software para análisis LAN, WAN y ATM.

1.1. DEFINICIÓN

El Internet Advisor J2300D fue diseñado con el propósito de localizar y resolver problemas de forma efectiva en redes LAN y WAN. Se puede conectar en cualquier punto de la red con el propósito de capturar cada trama sin importar el nivel de tráfico y realizar un análisis sobre éstas.

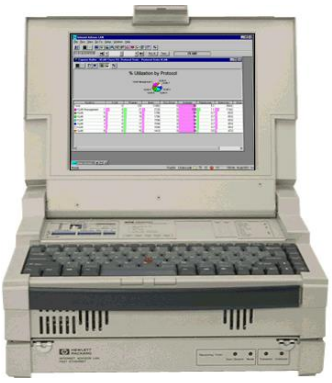


Figura 1.1. Internet Advisor HP J2300D.

El equipo es utilizado para:

- Detectar errores físicos, equipos mal configurados y probar la interoperabilidad de los mismos.
- Hallar el tráfico cursado en la noche y el ancho de banda consumido por las conexiones a Internet.
- Comprobar si los protocolos interactúan sin errores.
- Analizar problemas de tráfico y realizar un análisis estadístico.

- Determinar el ancho de banda consumido, disponible y los equipos que utilizan la mayor parte de éste.
- Localizar tráfico que no pertenezca a la red.
- Realizar medidas de estímulo/respuesta y monitorear simultáneamente su efecto sobre la red.
- Correr Pruebas de Tasa de Error de Bit (BERT).
- Monitorear y decodificar datos LAN y WAN de forma transparente en líneas de alta velocidad. Trabaja con los staks: TCP/IP, Novell, Apple Talk, Banyan VINES, OSI y DECnet.
- Simular cualquier dirección de la línea bajo prueba y procesar datos capturados previamente desde un archivo o un buffer.
- Generar estadísticas por nodo, por conexiones y por protocolos.
- Encontrar todos los nodos activos sobre la red brindando información como la(s) dirección(es) MAC y de red (IP, IPX, DECnet, AppleTalk, OSI CLNP) y el nombre del equipo.
- Mostrar medidas acumulativas y tendencias de red graficadas contra el eje del tiempo. Las medidas son realizadas simultáneamente con valores actuales, promedio y pico.
- Especificar el tipo de tramas que serán almacenadas usando sus 16 filtros de captura hardware.
- Buscar valores específicos, patrones o direcciones sobre las tramas capturadas.
- Almacenar los resultados de las pruebas en un archivo de disco. El almacenamiento puede ser selectivo para aquellas medidas que se deseen.
- Generar tráfico transmitiendo virtualmente cualquier tipo de mensaje, trama o celda sobre la red, una vez, un número determinado de veces, o de forma continua.
- Verificar problemas de configuración en routers y bridges, permitiendo determinar que clase de tráfico LAN está siendo enrutado sobre WAN.

Soporta capacidades de prueba para las principales tecnologías WAN, incluyendo:

- Frame relay, X.25, ISDN, HDLC, SNA/SDLC, PPP y SMDS.
- Protocolos LAN encapsulados sobre WAN.
- Interfaces RS 232/V.24, RS 449/422/423, V.10/11, V.3 5 / V.3 6 y RS 530.
- T1 y E1 full/fractional, accesos BRI y PRI ISDN, X.21, G.703 a 64 Kbps, J2, E3/DS3, STM-1/OC-3c, UTP155 y STM-4c/OC-12c.

1.2. MODOS DE OPERACIÓN

El Internet Advisor puede ser conectado como un *Nodo* sobre la red (**Modo Nodo**) o de tal forma que haga el *Monitoreo* del tráfico entre los nodos (**Modo Monitor**). Es importante distinguir entre configurar el Advisor para que concuerde con el medio físico en el cual será conectado y configurar las medidas individuales que posteriormente se realizaran.

Antes de conectar el Analizador se debe determinar si se está trabajando en un ambiente conmutado (Switch) o en un ambiente compartido (Hub). En un ambiente conmutado se debe conectar y configurar el Internet Advisor en **Modo Monitor** de forma que todo el tráfico entre un switch específico y una estación de trabajo o servidor sea observado por el equipo. De igual forma en un ambiente compartido se debe conectar y configurar el Advisor en **Modo Nodo** para que éste observe todo el tráfico destinado a todos los puertos del Hub.

NODO

Esta conexión algunas veces conocida como punto a punto causa que el Internet Advisor actúe y sea visto como un nodo o punto independiente sobre la red. El Advisor observará todo el tráfico que pasa a través del Hub de la misma forma que cualquier otro nodo Ethernet lo haría.

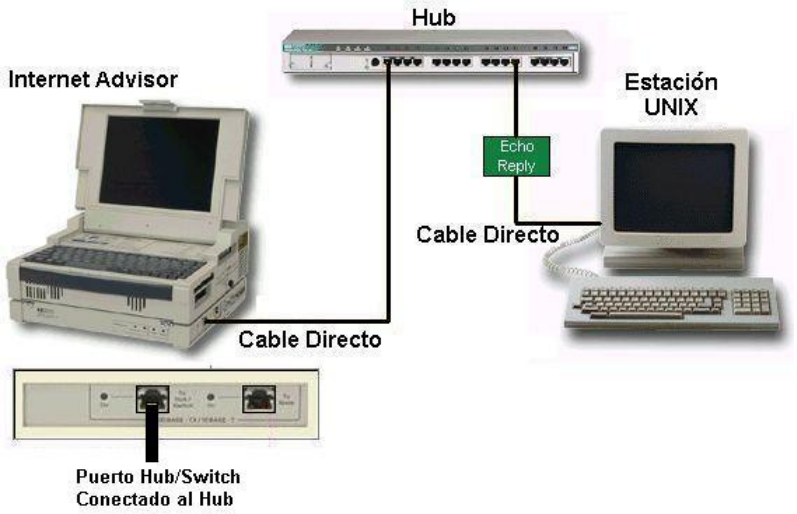


Figura 1.2. Conexión Modo Nodo.

En este modo de conexión, el Internet Advisor es unido directamente a un puerto disponible del hub usando un cable RJ-45 100Base-TX con una longitud máxima de 100 metros. El Advisor puede monitorear tráfico desde todas las estaciones teniendo el mismo dominio de colisión que el puerto del hub donde el Advisor es conectado. En este modo, el equipo también puede generar tráfico sobre la red.

MONITOR

Este modo se usa normalmente en un ambiente conmutado en el cual el Advisor se sitúa entre un puerto del switch/hub y un segmento de red u otro dispositivo. El switch/hub se conecta directamente al servidor a través de un cable directo (O uno cruzado). Para conectar el Internet Advisor entre el servidor y el switch/hub, se desconecta el cable del servidor y se conecta al puerto RJ 45 etiquetado "To Node", luego se conecta un cable directo del switch/hub al puerto RJ 45 " To Hub/Switch ". Este modo se puede usar en redes 10 Mbps o 100 Mbps Ethernet.

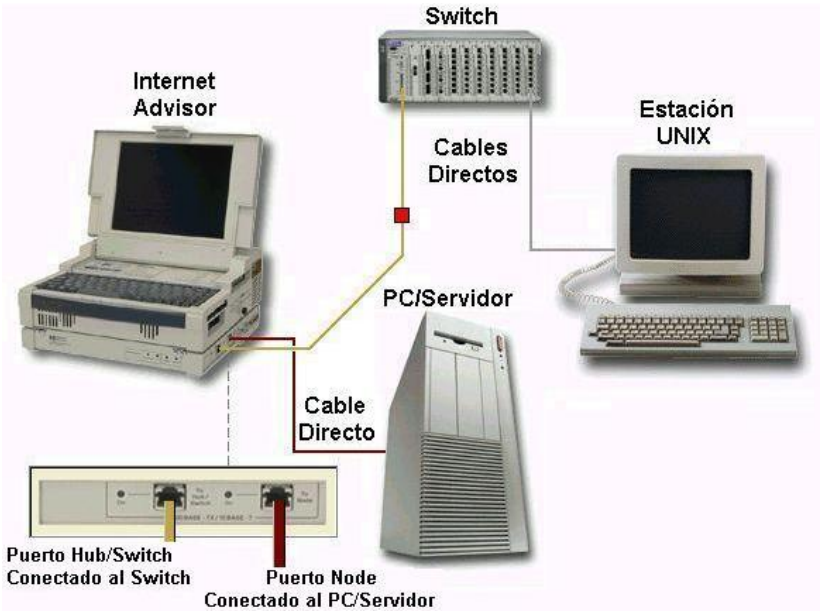


Figura 1.3. Conexión Modo Monitor.

Observaciones:

- El **Modo Monitor** no permite generación de tráfico.

- Para monitoreo full-duplex el **Modo Monitor** permite la captura de datos en ambas direcciones (Switch a servidor y servidor a switch). Es de anotar que la configuración del Analizador emplea los términos hub y nodo, los cuales son equivalentes a switch y servidor en un ambiente conmutado.

- La señal no es regenerada en el Analizador, así, la longitud combinada de ambos cables no debe exceder de 100 metros.

- Si se apaga el Internet Advisor, la conexión entre el servidor y el switch se mantiene.

1.3. CARACTERÍSTICAS HARDWARE

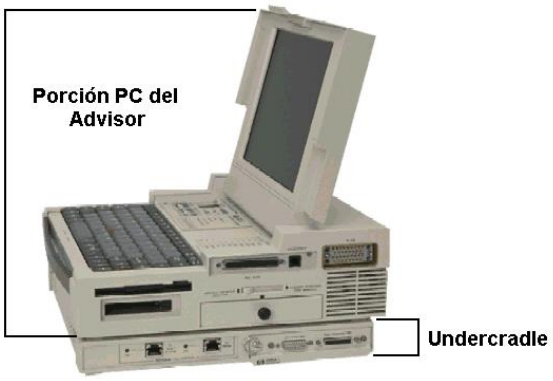


Figura 1.4. Constitución del Internet Advisor.

El HP Internet Advisor WAN es un analizador de protocolos poderoso diseñado para encontrar fallas y analizar la red. Consiste de un computador personal o MainFrame (Porción PC del Advisor) equipado con un hardware modular de adquisición y trasmisión de datos (Undercradle), como también de un software de análisis de red basado en el sistema operativo Microsoft Windows 98.

El conjunto adquirido por la FIET consta de un MainFrame cuya referencia es Internet Advisor HP J2300D, un Undercradle J3444A Fast Ethernet y dos módulos de interfaz el J2904B ISDN BRI S/T y el J2296B E1/ISDN SIM BNC.

1.3.1. Descripción del panel frontal

EL TECLADO Y EL BOTÓN DEL MOUSE

El teclado incluye 88 teclas más el botón del mouse integrado. Los botones derecho e izquierdo del mouse están localizados debajo de la barra de espaciamiento sobre el chasis del Internet Advisor.

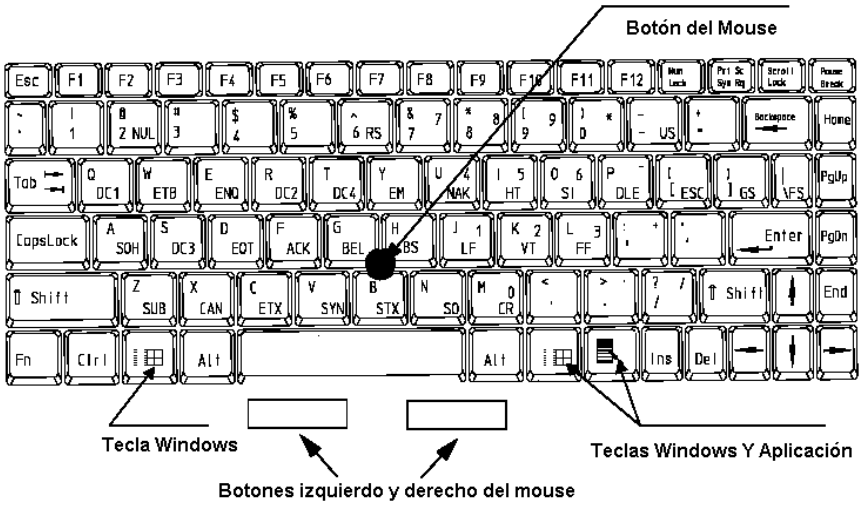


Figura 1.5. Teclado y botón del mouse.

CAJA BREAKOUT Y SISTEMA DE LEDs RS-232/V.24.

El Internet Advisor proporciona una caja *"breakout"* y capacidades de puenteo para circuitos RS-232/V.24. Se debe notar que las flechas negras largas apuntan a los conectores de prueba RS-232/V.24 ubicados en un lado del Internet Advisor. El conector *"Rearward"* es la entrada preferida para la mayoría de las pruebas. El conector *"Forward"* debe ser usado únicamente cuando las señales necesiten ser aisladas por los switches.

Los 25 pines para cada conector son accesibles vía jumpers y sus estados son modificables de acuerdo a la posición de cada switch (El banco de switches numerado de 1 a 25). Si se desea monitorear o simular sobre canales de datos auxiliares u observar otras señales de control diferentes a RTS, CTS, DTR, DSR y CD, se puede realizar la trasposición apropiada abriendo los switches correspondientes y puenteando los pines apropiados. Para hacer esto se conecta el circuito bajo prueba al Internet Advisor

a través del conector de prueba *"RS-232 Forward"* y se realizan las trasposiciones necesarias sobre el banco de switches lateral.

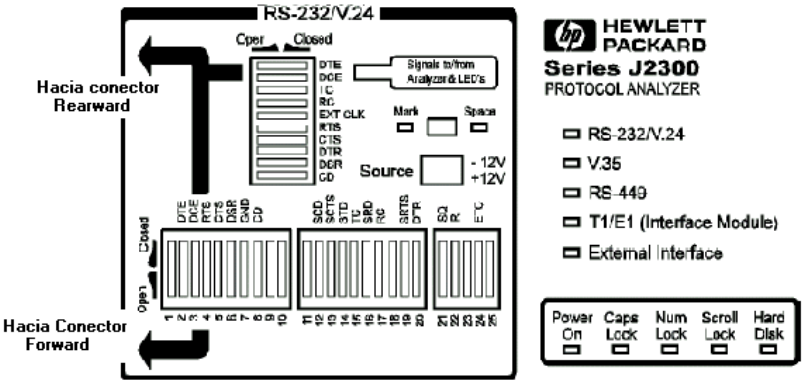


Figura 1.6. Caja Breakout y conexiones asociadas.

El banco de switches vertical proporciona aislamiento hardware en datos de entrada o salida y señales de control para pruebas de propósito especial.

PRECAUCIÓN: No se debe conectar más de un puerto del Internet Advisor al tiempo. Los puertos V.35, RS-449, RS-232, y puertos externos no son independientes uno del otro y conectar más de un puerto al mismo tiempo puede causar resultados inesperados.

En la parte superior derecha del panel frontal, hay diez pares de LEDs que proporcionan una indicación de tiempo real del estado de las señales para todas las interfaces. Estos LEDs también suministran información de datos, reloj y control para las interfaces serie V. La siguiente lista proporciona información sobre el significado de las luces desplegadas por los LEDs:

Columna de LEDs	Color del LED	Significado
Izquierda	Rojo	Estado de Marca u Off para datos o señales de control
Derecha	Verde	Estado de Espacio u On para datos o señales de control
Ambas	Iluminado	Señal cambia activamente de estado
Ambas	Apagado	Ninguna señal presente

1.3.2. Descripción de los páneles laterales

PANEL IZQUIERDO

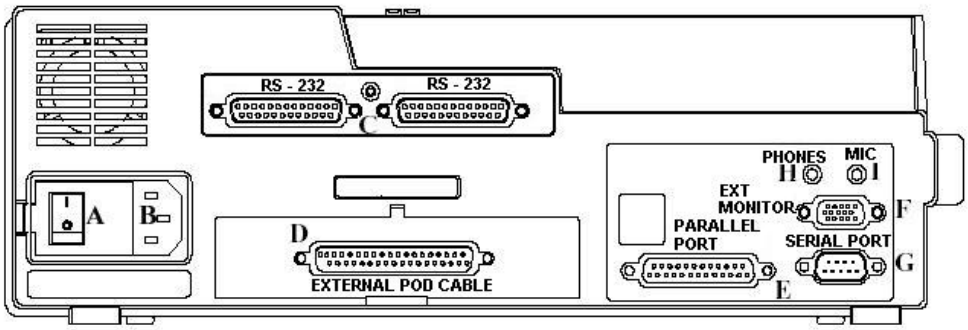


Figura 1.7. Panel Izquierdo del J2300D.

Este consta de los siguientes elementos:

A. Interruptor de alimentación eléctrica.

B. Enchufe de potencia.

C. Dos conectores RS-232/V.24.

D. Conector de interfaz externo pod (No disponible para el modelo J2300D).

E. Puerto paralelo: Se utiliza para conectar una impresora con el propósito de imprimir archivos, temas de ayuda y resultados de medidas.

F. Monitor externo: Este puerto se utiliza para conectar un monitor externo.

G. Puerto serial: Tiene las funciones convencionales de un puerto serial en un PC compatible IBM.

H. Audífono: Para conectar dispositivos de audio externos.

I. Micrófono: Esta es una entrada de audio.

PANEL DERECHO

Este consta de los siguientes elementos:

A. Drive para disco flexible de 3.5 pulgadas.

B. Slot dual PC: El propósito del *"slot PC Card"* es incrementar la flexibilidad en la sección correspondiente al Computador Personal y se usa principalmente para mejorar la capacidad de entrada/salida con el software del Internet Advisor. Esto incluye funciones tales como un MODEM, una interfaz LAN y un Drive de CD-ROM.

El Internet Advisor posee la especificación PC Card 2.10. Cada slot es capaz de recibir una tarjeta Tipo I o Tipo II. Las siguientes clases de tarjetas son compatibles con el equipo: ATA Drive, Audio, Ethernet/MODEM Combo, Fax/MODEM, Network Interface, SCSI Host Adapter y CD-ROM.

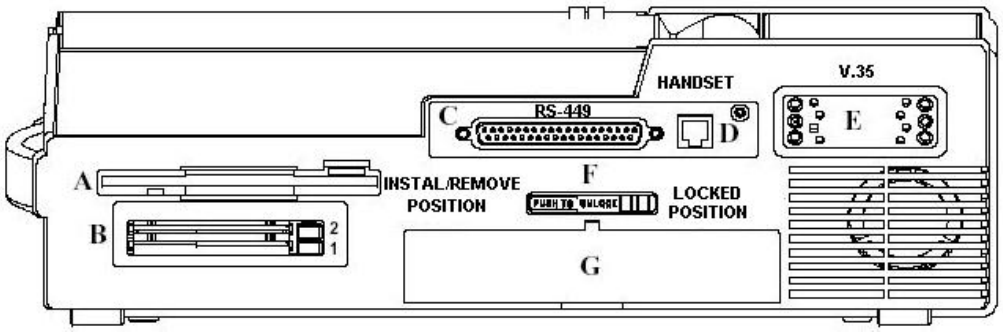


Figura 1.8. Panel Derecho del J2300D.

C. Conector RS-449.

D. Conector Handset: Proporciona la conexión a un punto de red cuando el equipo cuenta con una PC Card.

E. Conector V.35.

F. Latch para los módulos de interfaz: Corresponde a un cerrojo cuya función es la de asegurar y permitir la inserción/extracción de un módulo.

G. Slot para los módulos de interfaz: Almacena un solo módulo de interfaz para aplicaciones LAN, WAN y ATM. Estos módulos dependen del modelo de equipo específico.

1.3.3. Undercradle J3444A Fast Ethernet

Este módulo Hardware se utiliza en redes LAN Ethernet que trabajan a velocidades de 10 y 100 Mbps.

Figura 1.9. Undercradle J3444A Fast Ethernet.

Especificaciones generales:

- Velocidad de operación de 10 y 100 Mbps, con capacidad de auto-negociación (Detección automática de la velocidad de línea a probar).
- Dos conectores RJ-45 con hub lógico que permiten realizar pruebas en ambientes conmutados.
- Conector MII para pruebas Fast Ethernet a través de transceivers externos.
- Conector AUI para pruebas Ethernet a 10Mbps a través de transceivers externos.
- Módulo opcional de interfaz para fibra J3445A.
- Procesador AMD 29040 de 40 MHz con 32 Mbyte de memoria.
- Hardware con una capacidad de muestreo de 100 ns.
- Hardware de filtraje.

Figura 1.10. Detalle de los puertos del Undercradle J3444A.

Constitución interna del J3444A: A nivel funcional el Undercradle está conformado por un conjunto de bloques como se muestra a continuación.

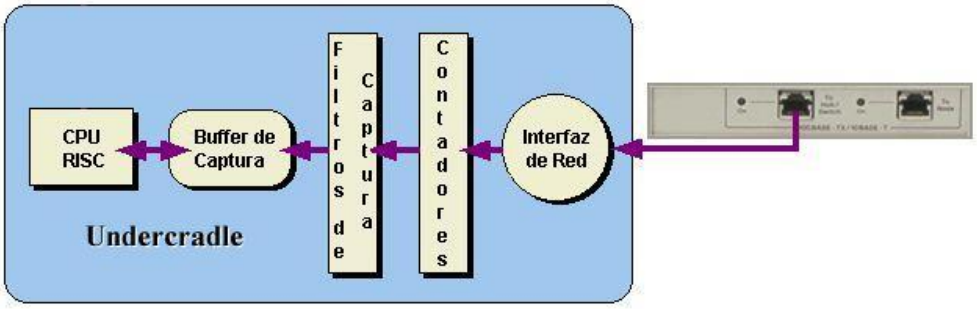


Figura 1.11. Diagrama en bloques del J3444A.

- *Interfaz de red:* Recibe todas las tramas que vienen de la red a través de los puertos RJ-45, AUI o MII.

- *Contadores:* Procesan cada una de las tramas provenientes de la interfaz de red y siguen el total de errores de nivel físico, utilización, tramas y bytes.

- *Filtros de captura:* Después del conteo de las tramas, éstas se comparan con cada uno de los filtros de captura previamente definidos por el usuario. La función principal de estos filtros es controlar que tramas entran al buffer de captura, además se pueden usar para disparar una acción con el fin de iniciar o parar la captura de otras tramas.

- *Buffer de captura:* Es un área de memoria especial que puede ser escrita a alta velocidad y su función es almacenar de forma temporal todas las tramas que han pasado a través de los filtros de captura.

- *CPU RISC:* Es un procesador especial optimizado para precisión y velocidad. Este recibe y ejecuta las órdenes provenientes del MainFrame correspondientes al procesamiento de las tramas almacenadas en el buffer de captura.

1.3.4. Módulo de Interfaz J2904B ISDN BRI S/T

Este módulo adiciona al Internet Advisor capacidades de prueba ISDN para interfaces S/T, monitoreo completamente integrado, establecimiento de llamada, soluciones BERT e identificación de problemas de tasa básica ISDN S/T.

Figura 1.12. Módulo de Interfaz J2904B ISDN BRI S/T.

Las capacidades de prueba son:

- Decodificación completa de canal D en tiempo real con disponibilidad de visualización en las ventanas detallada y resumida, incluyendo elementos de información completos.
- Análisis completo del estado de la información en el nivel 1, elementos de información Q.921 (LAP-D) y Q.931.
- Decodificación completa de las principales variantes Q.931, incluyendo ETSI, NI-1 y otras 14 señalizaciones de los principales fabricantes de switches.
- Decodificación completa de X.25 sobre canal D.
- Monitoreo y decodificación de tráfico LAN encapsulado en ISDN.
- Verificación de la integridad del enlace para transporte de tráfico con pruebas BERT completas.
- Estadísticas tipo mensaje Q.931 y almacenamiento de estadísticas a disco para descubrir problemas aleatorios.
- Estadísticas detalladas para tráfico de canal B como utilización, rendimiento, errores, tipos de trama/paquete y tráfico LAN sobre WAN. Búsqueda, filtraje e inicio de acciones a partir de valores SAPI y TEI.

- Pruebas sobre redes de bus pasivo BRI.
- Verificación rápida del establecimiento de la llamada e integridad del enlace.

Interfaces físicas BRI S/T: Estándar ITU-T I.430, Euro ETS 300 012 y estándar ANSI T1.605. Los dos conectores que posee son RJ-45. Soporta codificación de voz bajo los esquemas de ley A y ley µ.

Tasas de datos: Canal D a 16 Kbps, canal B1 y B2 a 56 o 64 Kbps y canal B1 + B2 a 112 o 128 Kbps.

1.3.5. Módulo de Interfaz J2296B E1/ISDN SIM BNC

El módulo opera a 2 Mbps, tiene cuatro conectores BNC de 75 ohms desbalanceados y proporciona captura completa y análisis de protocolos para todos los niveles en Frame Relay, ISDN, HDLC y X.25. Posee las mismas funcionalidades que el módulo J2904B pero a nivel de ISDN realiza el seguimiento, captura y análisis de los 30 canales de datos B y el canal de señalización D en una interfaz de tasa primaria.

Figura 1.13. Módulo de Interfaz J2296B E1/ISDN SIM BNC.

1.4. CARACTERÍSTICAS SOFTWARE

1.4.1. Interfaz de usuario

La interfaz de usuario del Internet Advisor es similar a otras aplicaciones Windows, permitiendo un manejo rápido y una utilización intuitiva de todas las herramientas y capacidades que ofrece este equipo. A continuación se describen las partes principales que componen dicha interfaz.

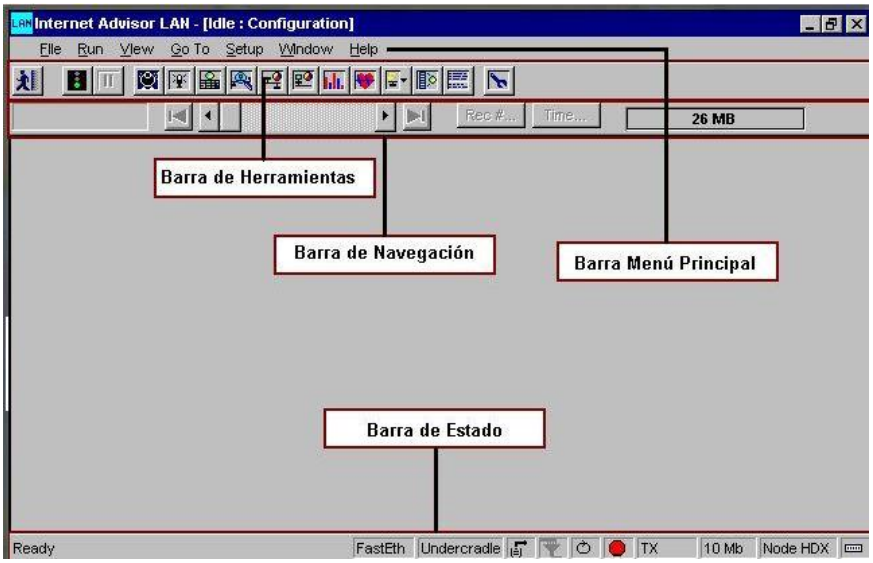


Figura 1.14. Interfaz de Usuario del Internet Advisor LAN.

BARRA HERRAMIENTAS

Esta permite un acceso directo a las principales funciones software del equipo.

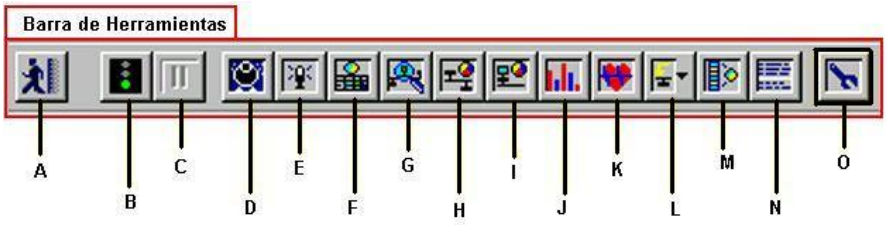


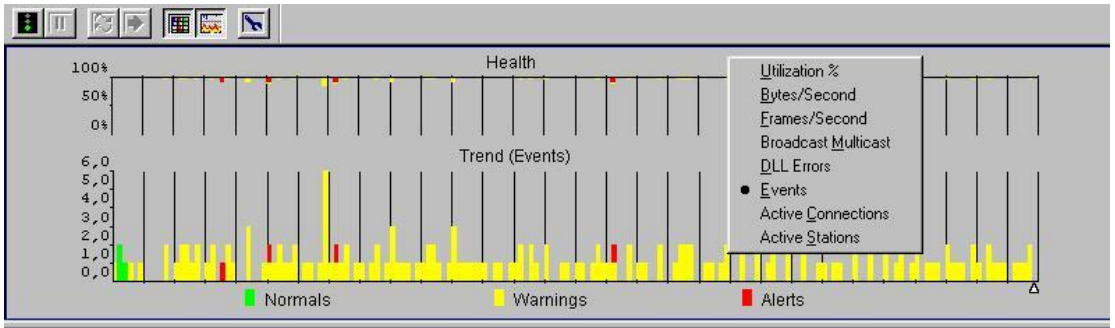
Figura 1.15. Barra de Herramientas LAN.

A. SALIR A WINDOWS: Se utiliza para retornar del software Advisor LAN a Windows 98.

B. INICIAR/ PARAR TODAS LAS MEDIDAS: Un click sobre el semáforo en *verde* inicia todas las medidas, mientras un click con el semáforo en *rojo* las detiene. La mayoría de las medidas poseen su propio semáforo.

C. DETENER/REACTIVAR: Se utiliza para detener todas las medidas y permitir al usuario navegar y buscar a través de los datos capturados. Cuando el usuario reanuda la acción las medidas son re- sincronizadas. Esta opción no está disponible para el Advisor LAN.

D. ANALIZADOR EXPERTO: Evalúa el estado de la red mediante la combinación de los resultados arrojados por otras medidas *como* el *Comentador*, *Descubrimiento de Nodos*, *Estadísticas de Conexión* y de *Protocolo*. La gráfica proporciona estadísticas del porcentaje de utilización del medio, los bytes/segundo, las tramas/segundo, el tráfico Broadcast, Multicast y Unicast, los errores DLL, los eventos y las conexiones y estaciones activas.



Protocols	Utilization %	Stations	Connections	Alerts	Warnings	Normals
Totals	0.97%	13	322	4	165	3
IP	0.96%	12	280	1	162	3
Novell	0.00%	0	42	0	0	0
Other Protocols	0.00%	1		3	0	0
MAC Level	0.00%	12	322	0	3	0
Routers		3		0	126	3

Figura 1.16. Analizador Experto Análisis LAN.

E. COMENTADOR: Observa los paquetes, las conexiones y reporta eventos tales como baja transferencia de archivos, retransmisiones, direcciones duplicadas, entre otros. Los eventos de red son listados de tres formas como nodos involucrados en un evento, conexiones involucradas en un evento y todos los eventos; además, éstos son clasificados de acuerdo a su nivel de severidad como "*Alerts"* (A), "*Warnings"* (W) o "*Normals"* (N).

El árbol "*All Events"* despliega todos los eventos capturados durante la ejecución de la medida con la facilidad de conocer la *trama*, la *fuente* y el *destino* de la misma, el *tiempo* de ocurrencia y el *tipo de evento*. El árbol "*Connection Events"* visualiza las conexiones involucradas con algún evento y el árbol "*Node Events"* posee un conteo de los eventos por cada nodo.

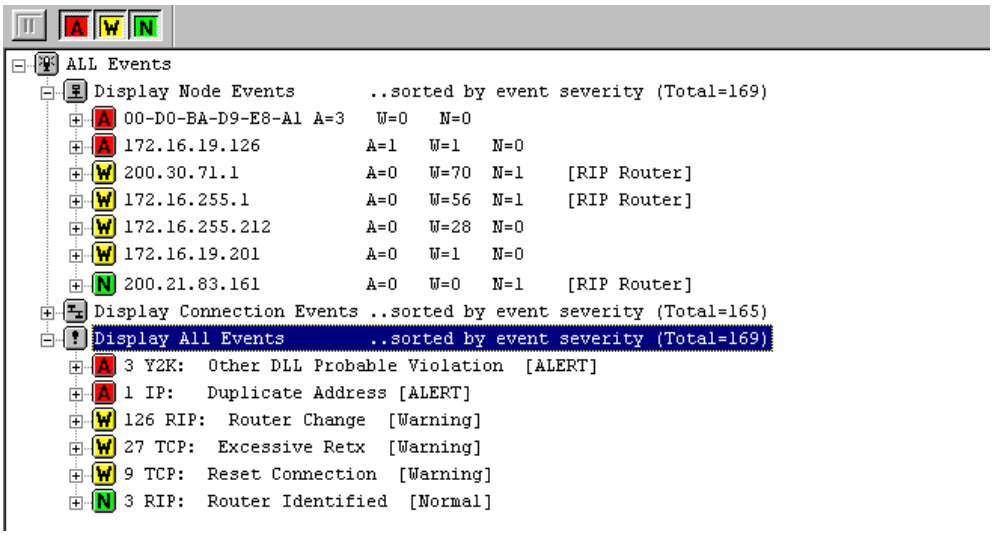
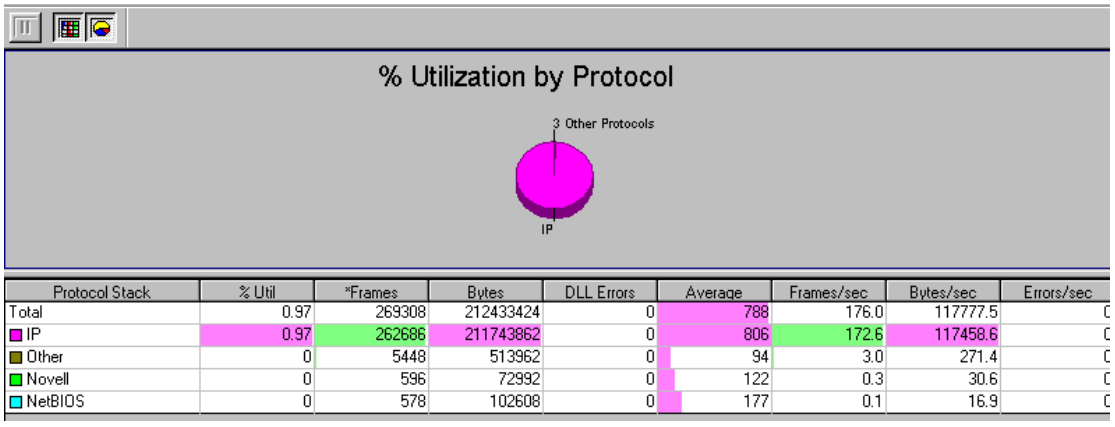


Figura 1.17. Comentador Análisis LAN.

F. ESTADÍSTICAS DE PROTOCOLO: Corre estadísticas para todos los stacks sobre la red y medidas individuales están disponibles usando la opción "*Open Measurement"* del menú "*File"*. Esta medida muestra información en dos formatos: *Un diagrama circular* que ilustra el porcentaje relativo de tráfico ocurriendo en cada protocolo o una distribución de protocolos para diferentes longitudes de trama y *una tabla de datos* que presenta la distribución de tramas, bytes, utilización y errores para cada protocolo.



Protocol Stack	% Util	*Frames	Bytes	DLL Errors	Average	Frames/sec	Bytes/sec	Errors/sec
Total	0.97	269308	212433424	0	788	176.0	117777.5	0
IP	0.97	262686	211743862	0	806	172.6	117458.6	0
Other	0	5448	513962	0	94	3.0	271.4	0
Novell	0	596	72992	0	122	0.3	30.6	0
NetBIOS	0	578	102608	0	177	0.1	16.9	0

Figura 1.18. Estadísticas de Protocolo Análisis LAN.

G. DESCUBRIMIENTO DE NODOS: Esta medida corre automáticamente cuando se activan el *Comentador*, *Estadísticas de Conexión* o el *Analizador Experto*, además, muestra y actualiza los nodos

que hay sobre la red bajo estudio. Si una dirección MAC tiene asociadas direcciones de red, el número y tipo de éstas son listadas con la posibilidad de verlas. La lista de nodos tiene vistas individuales para nodos MAC, IP, Novell IPX, Apple Talk, DECnet, OSI CLNP, VINES, Others y nodos de enrutadores, y en todos los casos pueden ser ordenados por sus direcciones de red, por nombres y por la severidad de los eventos que han ocurrido sobre éstos.

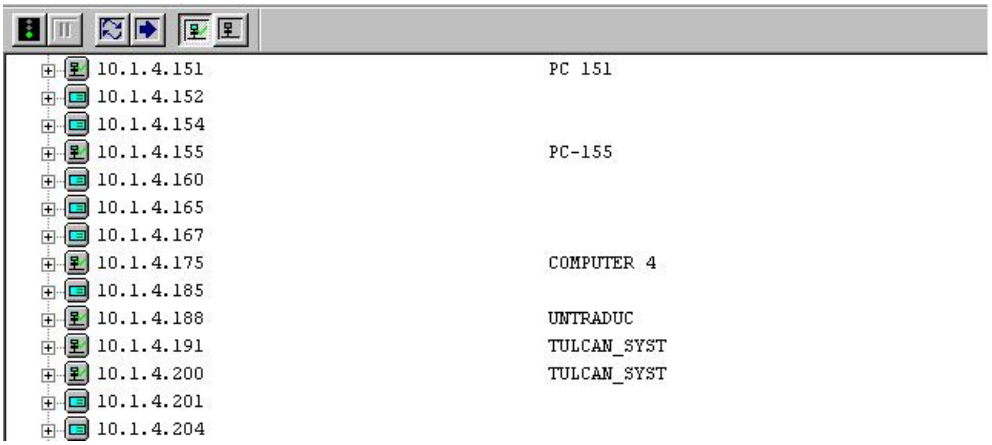
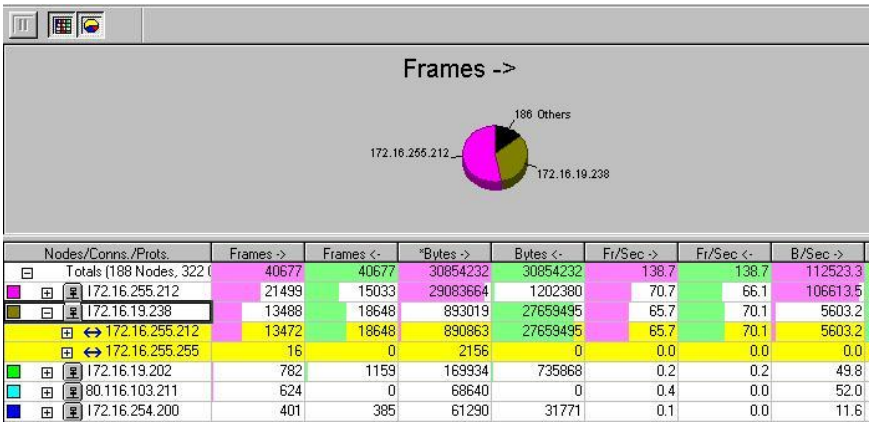


Figura 1.19. Descubrimiento de Nodos Análisis LAN.

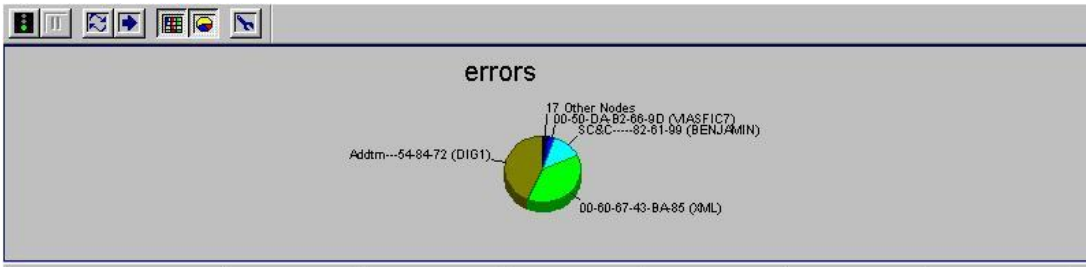
H. ESTADÍSTICAS DE CONEXIÓN: Muestra las conexiones activas sobre la red y las actualiza cada 10 segundos, identifica cuales usuarios están consumiendo el mayor ancho de banda, determina el número de conexiones a Internet, calcula el tráfico transportado por la subred y establece la interfaz de enrutador más ocupada. Presenta dos áreas, la primera es una tabla de datos y la segunda constituye un gráfico estadístico que representa la información de la columna seleccionada.



Nodes/Conns./Prots.	Frames ->	Frames <-	*Bytes ->	Bytes <-	Fr/Sec ->	Fr/Sec <-	B/Sec ->
Totals (188 Nodes, 322 (	40677	40677	30854232	30854232	138.7	138.7	112523.3
172.16.255.212	21499	15033	29083664	1202380	70.7	66.1	106613.5
172.16.19.238	13488	18648	893019	27659495	65.7	70.1	5603.2
↔ 172.16.255.212	13472	18648	890863	27659495	65.7	70.1	5603.2
↔ 172.16.255.255	16	0	2156	0	0.0	0.0	0.0
172.16.19.202	782	1159	169934	735868	0.2	0.2	49.8
80.116.103.211	624	0	68640	0	0.4	0.0	52.0
172.16.254.200	401	385	61290	31771	0.1	0.0	11.6

Figura 1.20. Estadísticas de Conexión Análisis LAN.

I. ESTADÍSTICAS DE NODO MAC: Reporta errores (FCS erróneos, Runts, Jabbers y Dribbles) que ocurren en la capa física del modelo OSI, los cuales indican problemas en el cableado, diseño de la red, puertos o tarjetas de interfaz de red. La tabla lista las direcciones MAC de los 20 nodos más activos observados en el actual periodo de muestreo y la gráfica ilustra la columna seleccionada. Los nodos son organizados de acuerdo a la estadística de la primera columna que por defecto es el porcentaje de transmisión (%tx).

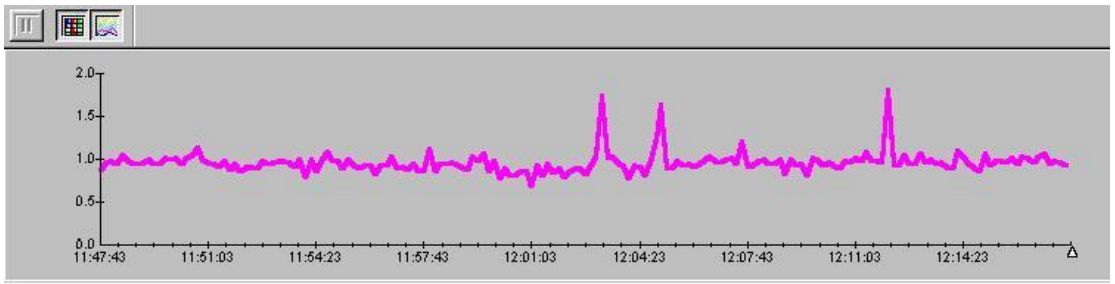


Node Addr/Name	% tx	frames tx/sec	% rx	frames rx/sec	*errors	errors/sec
Total	1.28	36.5	1.28	36.5	128	0
Short Frames	0	0	0	0	0	0
Addtrn---54-84-72 (DIG1)	0.04	2.5	0.37	3.5	FJR 56	0
00-60-67-43-BA-85 (XML)	0.03	3.1	0	0	FJR 49	0
SC&C-----82-61-99 (BENJAMIN	0	0	0	0	FR 16	0
00-50-DA-B2-66-9D (VIASFIC7	0	0	0	0	FJR 4	0
AA-AA-AA-AA-AA-AA	0	0	0	0	DFR 3	0
Cisco----F1-92-04	0.92	8.8	0.06	5.9	0	0

Figura 1.21. Estadísticas de Nodo MAC Análisis LAN.

J. ESTADÍSTICAS VITALES DE LÍNEA: Esta consiste de una prueba de nivel físico que mide y despliega estadísticas de utilización, conteo de tramas, colisiones, FCS's malos, runts (Tramas más cortas de 64 bytes), broadcast, multicast, etc.

K. ESTADÍSTICAS VITALES DE PROTOCOLO: Muestra información organizada por stacks de protocolos, los valores actuales, promedio y pico son actualizados cada segundo para cada estadística en tanto que los valores de umbral representan niveles estadísticos normales y su configuración se lleva a cabo a través de la ventana de configuración propia de la medida. Cada stack de protocolos se puede expandir para observar su correspondiente conjunto de estadísticas, el área gráfica muestra una historia estadística de tres minutos con la posibilidad de representar hasta veinte estadísticas. En el árbol "*Pre-Filter Ethernet Utilization"*, las estadísticas pre-filtradas son calculadas sobre todas las tramas que llegan al equipo mientras que las post-filtradas son estimadas en base a las tramas que pasan a través de los filtros de captura definidos por el usuario.

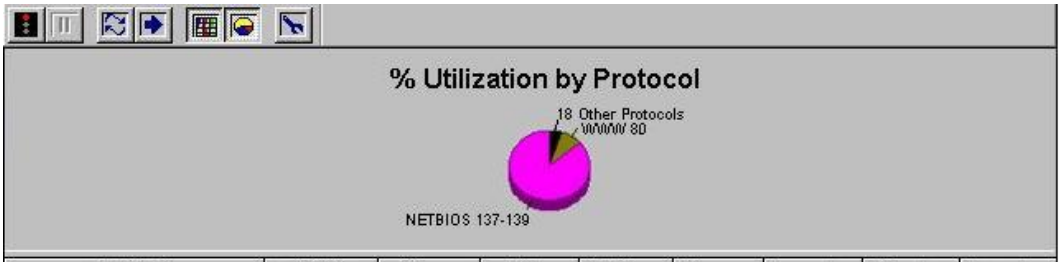


Statistic	Current	Average	Peak	Cumulative	Threshold	Threshold Exceeded
Pre-filter Ethernet Utilization	0.93%	0.99%	2.36%	n/a	40.00%	0
IP Utilization	0.95%	0.99%	2.21%	n/a	5.00%	0
Novell Utilization	0.00%	0.00%	0.01%	n/a	5.00%	0
AppleTalk Utilization	0.00%	0.00%	0.00%	n/a	5.00%	0
VINES Utilization	0.00%	0.00%	0.00%	n/a	5.00%	0
OSI Utilization	0.00%	0.00%	0.00%	n/a	5.00%	0
DEC DRP Utilization	0.00%	0.00%	0.00%	n/a	5.00%	0

Figura 1.22. Estadísticas Vitales de Protocolo Análisis LAN.

L. PRUEBAS ACTIVAS: Su función consiste en *transmitir tráfico real* sobre la red y desplegar las respuestas de los nodos, utiliza un filtro de captura automático para asegurar que estas últimas sean desplegadas. Es importante anotar que si otras medidas están activas, el filtro no será habilitado. Se subdividen en cuatro conjuntos de pruebas como *Pruebas Activas IP*, *Pruebas Activas Novell*, *Generador de Tráfico* y *Edit & Playback.*

M. ESTADÍSTICAS DE PROTOCOLO VLAN: El Advisor LAN decodifica y despliega estadísticas para los protocolos VLAN más utilizados (ISL de Cisco y 802.1 p/Q) e identifica la pertenencia VLAN de cada trama cursada entre switches.



VLAN ID		% Util	*Frames	Bytes	DLL Errors	Average	Frames/sec	Bytes/sec	Errors/sec
Total		0.16	60	5661	0	94	17.7	1670.7	0
Non-VLAN	-	0.10	36	3608	0	100	10.6	1064.8	0
VLAN	5	0.03	11	994	0	90	3.2	293.3	0
VLAN	7	0.02	8	667	0	83	2.4	196.8	0
VLAN	3	0	3	212	0	70	0.9	62.6	0
VLAN Management	1	0	2	180	0	90	0.6	53.1	0

Figura 1.23. Estadísticas de protocolo VLAN Análisis LAN.

El mejor lugar para conectar el Advisor es entre switches porque en este punto el tráfico VLAN es transmitido y puede ser monitoreado. Las estadísticas de tráfico VLAN serán recogidas y desplegadas en el área gráfica y las tramas VLAN serán automáticamente decodificadas y desplegadas en el *Decodificador*.

N. DECODIFICADOR: Decodifica las tramas capturadas y las muestra a través de tres ventanas *"Summary"*, *"Detailed"* y *"Hex"* que ilustran de forma respectiva el resumen de los campos más importantes, el detalle de cada campo y la decodificación hexadecimal de las tramas.

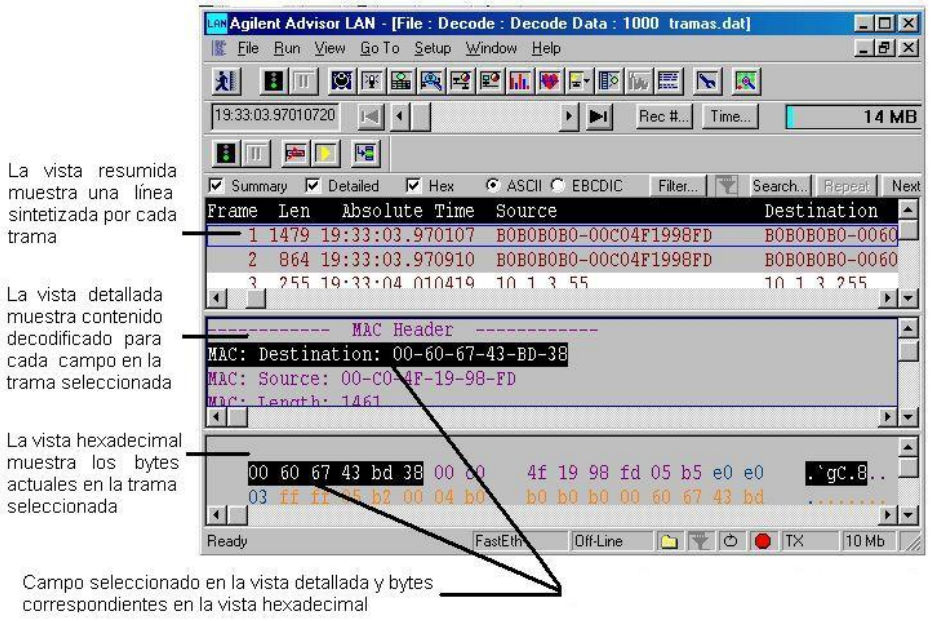


Figura 1.24. Decodificador Análisis LAN.

O. VENTANA DE CONFIGURACIÓN: En ésta se fijan los parámetros de la interfaz del Advisor, se definen los filtros de captura y se habilitan las medidas de almacenamiento.

BARRA DE NAVEGACIÓN

Se utiliza para navegar a través de los datos capturados previamente.

A. Marca de Tiempo: Durante el tiempo de ejecución, ésta muestra la hora actual y durante el procesamiento de los datos refleja el tiempo en que fueron capturados.

B. Controles VCR : Con éstos se puede navegar a través de las muestras de datos durante el p*ost-procesamiento* permitiendo acceder a los registros primero, último, siguiente o previo, desde el buffer de captura, desde un archivo de datos o desde un archivo de almacenamiento log.

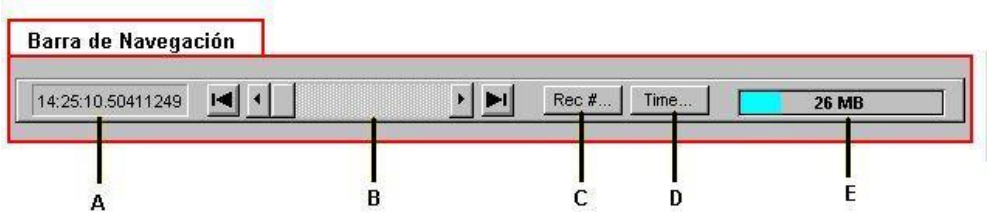


Figura 1.25. Barra de Navegación LAN.

C. Número de Registro: Permite ir a un registro particular.

D. Tiempo: Introduciendo una hora específica, se obtiene el registro capturado en ese momento.

E. Indicador del buffer de captura: Muestra como se llena el buffer de captura durante el proceso de recolección de datos. El número refleja el valor introducido en el campo tamaño del buffer (Buffer Size) en la ventana de configuración.

1.4.2. Análisis WAN

Gracias a los Módulos de Interfaz que posee el Analizador de Protocolos este esta en capacidad de monitorear redes Frame Relay, protocolos SNA (Simple Network Architecture) y SDLC (Synchronous Data Link Control), conexiones ISDN sobre circuitos PRI y BRI, X.25, HDLC, protocolos punto a punto (PPP) tanto sincrónicos como asincrónicos, monitoreo de datos SMDS DXI sobre circuitos V.35, RS-449, RS-232 y E1, y correr pruebas de Tasa de Error de Bit.

1.4.3. Análisis ATM

Para utilizar todas las funcionalidades que ofrece esta parte software del Internet Advisor se necesita el Undercradle J3763A. Sin embargo, una fracción de dichas capacidades pueden ser empleadas con el equipo actual que posee la FIET por medio de Módulos de Interfaz ATM. Entre las funciones adicionales que realiza este software están:

- **Medir la potencia óptica y la amplitud de pulso.**

- **Realizar una vista estadística de la red.**

- **Decodificar todos los niveles correspondientes al stack de protocolos ATM**:
  Capa Física ATM: Protocolo de control IMA.
  Capa de Celda ATM: Detalles del encabezado de celda.
  Capa de Adaptación ATM: AAL-1, AAL-2, AAL-3/4 y AAL-5
  Capa de Servicios: Protocolos encapsulados tales como Frame Relay, X.25 y LAN, decodificación MPEG-2, señalización UNI 3.0, 3.1, 4.0 PNNI, B-1SUP, B-ICI, SPANS. Todos los principales grupos de protocolos son soportados incluyendo TCP/IP, 3Com, AppleTalk, Banyan, Cisco, DECnet, H.323, IBM/SNA, LLC, Microsoft LAN manager, Novell, OSI, SUN, XNS, ISO, SIP, MEGACO, MGCP, SGCP, RTP, GPRS, W-CDMA y más.

- **Autodetección y estadísticas VP/VC:** Mediante esta característica se pueden detectar hasta 1024 canales virtuales y para cada uno de ellos visualizar y almacenar su correspondiente VPI/VCI, utilización máxima e instantánea (%), throughput (Kbps), conteo de celdas y octetos, errores de encabezado (HEC) y estado del CLP.

- **Decodificación VP/VC:** Muestra un conjunto de VPI's/VCI's indicando cual AAL y protocolo LAN encapsulado está corriendo sobre cada uno de ellos.

- **Calidad de servicio (QoS).**

- **Auditoria:** Las pruebas de auditoría son medidas realizadas en tiempo real que comprueban que el flujo de celdas de un canal determinado cumplan el contrato de tráfico.

- **Señalización y establecimiento de llamada:** El Advisor incluye señalización y emulación LAN (LANE) para proporcionar pruebas de conectividad.

- **Filtraje IP en tiempo real:** Consiste en capturar y filtrar paquetes IP-LAN en tiempo real, permitiendo aislar y analizar conversaciones LAN que tienen lugar sobre un circuito ATM.

- **Recolección remota de estadísticas MIB alrededor de la red (Switch Advisor):** Proporciona la capacidad de supervisar la utilización de puertos en switches de forma remota, muestra información del sistema incluyendo referencia del switch, localización, nombre designado e información del contacto. Despliega cada número de puerto y el nombre personalizable (Alias) con la descripción de la interfaz, tipo de medio de transmisión asociado y si la capacidad de RMON es soportada por la interfaz.

1.4.4. Configuración básica del software

El primer paso para conectarse a una red y capturar, procesar y analizar su tráfico es especificar adecuadamente las opciones de la ventana de configuración principal. Esta posee tres etiquetas o pestañas (Interface/Protocols, Capture Filters y Log) las cuales se explicarán a continuación detalladamente.

1. INTERFACE/PROTOCOLS:

- **Type Interface:** Este campo muestra el hardware LAN en uso y es detectado automáticamente por el MainFrame de tal forma que el usuario no puede modificar esta área.
- **Media Connection:** Hay diferentes opciones de medios de conexión para este campo.
  TX Auto Negotiate: El Advisor determina la velocidad del enlace y si el modo de la línea es half o full duplex, para conexiones Fast Ethernet y 10 BASE-T.

  TX Fast Ethernet: Conexión a un enlace 100 BASE-TX, se debe seleccionar el modo de línea a half o full duplex.

  TX 10Mb Ethernet: Conexión a un enlace 10 BASE-T. Si se requiere conectar el equipo a un enlace full duplex 10 BASE-T, configure el campo “Media Connection” a Fast Ethernet y luego el área “Line Speed” a 10 Mb.

  MII Auto Negotiate: Posee la misma funcionalidad que la opción “TX Auto Negotiate”, solo que soporta conexiones para unidades T4 y de fibra óptica MII.
  MII Fast Ethernet: Se utiliza para conectar unidades T4 y de fibra óptica MII sobre un enlace de 100Mb.

  AUI 10Mb Ethernet: Se utiliza para conexiones a otros tipos de medios 10 Mb Ehernet.

- **Line Speed:** Dependiendo del medio de conexión se puede escoger la velocidad de línea (10 o 100Mbps). Cuando se selecciona la opción "Auto Negotiate" esta casilla se deshabilita ya que el Advisor determina automáticamente la velocidad de línea.
- **Line Mode:** Indica al Advisor si la línea es half o full duplex y si el equipo trabaja en modo monitor o en modo nodo.
- **Monitor Type:** Determina por cuanto tiempo el Advisor analiza los datos, de forma continua, por un lapso específico o hasta que el buffer de captura se llene.
- **Monitor Period:** Esta opción se utiliza cuando se selecciona el tipo de monitoreo "Timed".
- **Packet Size:** Establece el tamaño del paquete a capturar. Esta opción se activa habilitando la casilla "Packet Slicing". Si esta casilla no es habilitada los paquetes se almacenan en su totalidad.

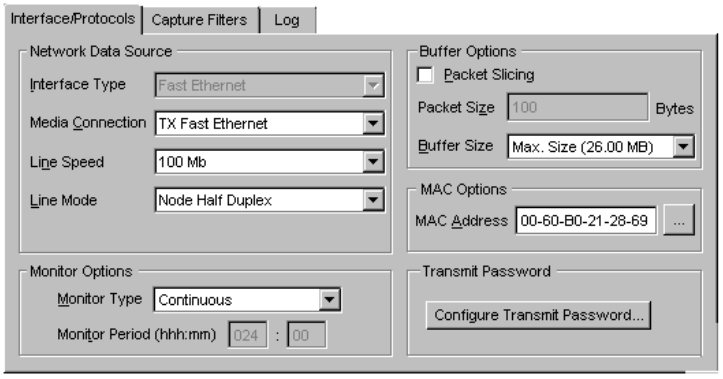


Figura 1.26. Pestaña Interface/Protocols Análisis LAN.

- **Buffer Size:** Fija el tamaño del buffer de captura cuyo valor máximo depende del Undercradle. Para la referencia J3444A corresponde a 26 Mb.
- **MAC Address:** Contiene la dirección de capa física (MAC) que el Advisor utiliza cuando genera tramas. Por defecto ésta corresponde a la dirección hardware del Undercradle.
- **Configure Transmit Password:** Permite cambiar la contraseña de transmisión que por defecto posee el Intenet Advisor ("advisor"), cuando éste trabaja con *pruebas activas*.

2. CAPTURE FILTERS:

Esta ventana permite la creación de filtros de captura con el fin de almacenar tramas de un tipo particular ahorrando espacio en el buffer de captura.

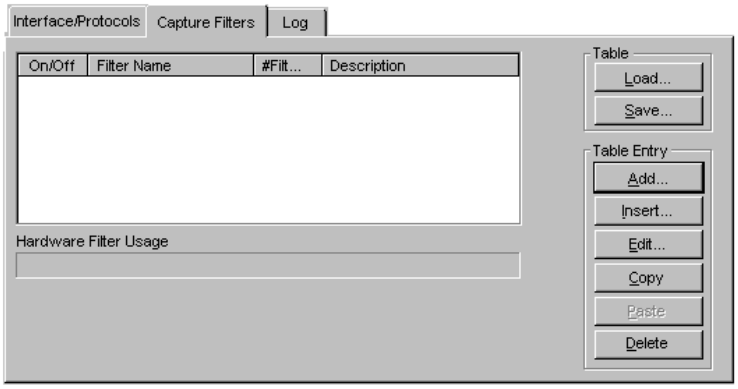


Figura 1.27. Pestaña Capture Filters Análisis LAN.

- **Load:** Abre un conjunto de filtros definidos por el usuario con anterioridad y los visualiza en el área de texto.
- **Save:** Guarda un conjunto de filtros definidos por el usuario en una carpeta.
- **Add:** Esta opción se utiliza para crear los filtros de captura y al seleccionarla aparece la siguiente ventana.

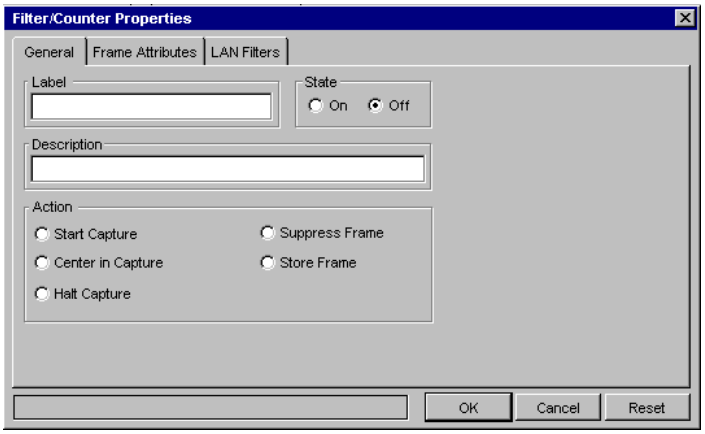


Figura 1.28. Pestaña General Análisis LAN.

General:

- ✓ *Label:* En esta campo se digita el nombre del filtro.
- ✓ *Description:* Contiene una breve descripción acerca del filtro a crear.
- ✓ *State:* Habilita o deshabilita el filtro según la selección.

- ✓ *Start Capture:* Cuando se observa una trama que concuerda con el filtro inicia la captura y detiene esta operación cuando el buffer se ocupa en su totalidad.
- ✓ *Center in capture:* Almacena la primera trama que concuerde con el filtro de captura y detiene esta operación.
- ✓ *Halt Capture:* Detiene todas las medidas activas cuando se detecta que una trama coincida con el filtro de captura.
- ✓ *Suppress Frame:* Las tramas que concuerdan con el filtro son excluidas del buffer.
- ✓ *Store Frame:* Es la opción habilitada por defecto y almacena todas las tramas que concuerden con el filtro.

Frame Attributes:

Las casillas de verificación se utilizan para capturar tramas con combinación de errores y se pueden definir bytes de datos hexadecimales para filtrar sobre el área de datos de la trama.

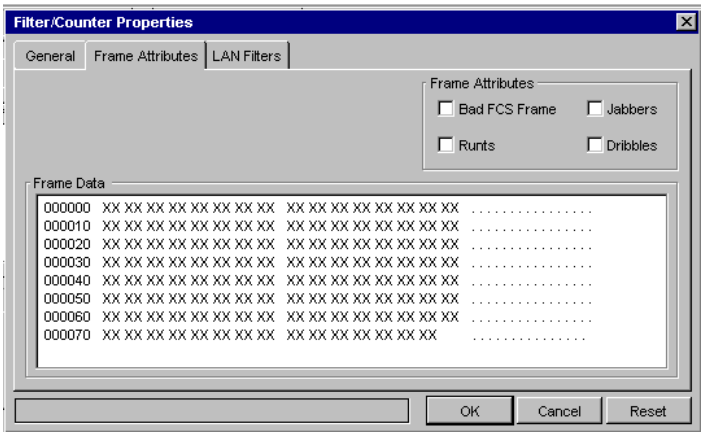


Figura 1.29. Pestaña Frame Attributes Análisis LAN.

LAN Filters:

Se emplean para filtrar conexiones de LAN's Virtuales, protocolos específicos y tramas que interactúan con una estación en particular.

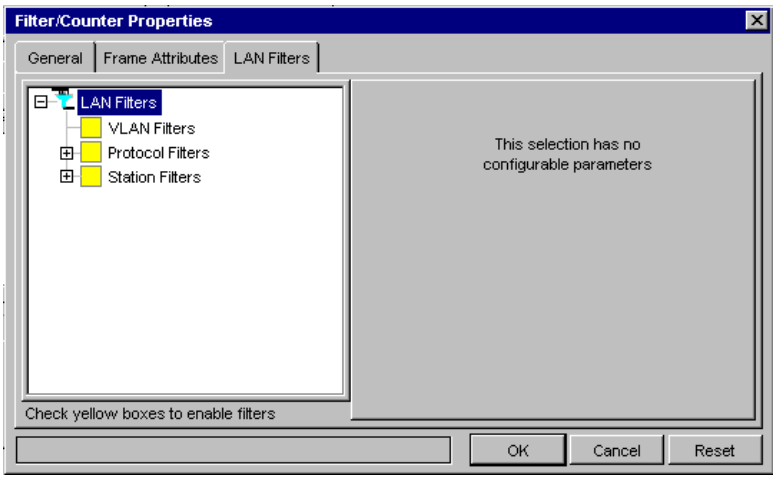


Figura 1.30. Pestaña LAN Filtres Análisis LAN.

- **Insert:** Permite la introducción de un nuevo filtro.
- **Edit:** Se modifican las propiedades del filtro de captura seleccionado.
- **Copy:** Copia un filtro de captura seleccionado previamente en la ventana de texto.
- **Paste:** Pega el filtro de captura en la ventana de texto.
- **Delete:** Borra los filtros seleccionados de la pantalla.

3. LOG:

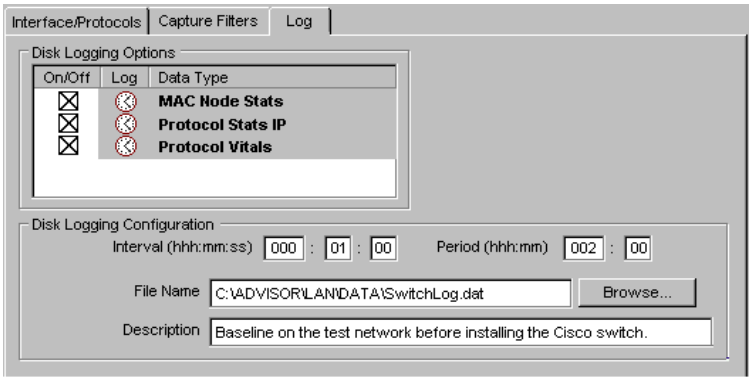


Figura 1.31. Pestaña Log Análisis LAN.

Esta opción se utiliza cuando se desea almacenar información para determinadas medidas durante un periodo tomando muestras a intervalos de tiempo definidos por el usuario. Todas las medidas activas son listadas en la ventana "*Disk Logging Options"* y sólo aquellas habilitadas son almacenadas. "*File*

Name" y "*Description"* representan el nombre del archivo donde se guardarán todos los datos capturados para cada medida habilitada y la descripción de la operación.

2. PRÁCTICAS DE LABORATORIO CON EL INTERNET ADVISOR WAN HP J2300D

En este capítulo se presentan las prácticas de laboratorio realizadas con el Internet Advisor WAN HP J2300D divididas en tres entornos: LAN, WAN y Acceso Remoto Telefónico.

2.1. ENTORNO LAN

2.1.1. Práctica No 1. Funcionamiento Básico del Internet Advisor

- **OBJETIVOS:**

  - Familiarizarse con el equipo Internet Advisor WAN HP J2300D y sus capacidades.
  - Configurar, implementar y operar los modos de conexión del equipo HP J2300D.
  - Especificar los parámetros necesarios en la ventana de configuración principal y familiarizarse con la interfaz de usuario.
  - Monitorear el *Login* y *Password* en diferentes aplicaciones como Telnet, ftp y correo electrónico.

- **MARCO TEÓRICO**

El tamaño y complejidad de las Redes y Servicios Telemáticos han crecido sin cesar debido en gran parte a la aparición de las redes públicas de datos y a la creciente oferta de servicios de comunicaciones de valor agregado. Así surge la necesidad de gestionarlas, es decir, de controlar los recursos que las componen en términos de rendimiento, capacidad, utilización, reconfiguración, diagnósticos y planificación. En respuesta a este ambiente de trabajo y a las necesidades de operación se utilizan herramientas que facilitan la gestión como el Analizador J2300D para la infraestructura teleinformática.

El Internet Advisor WAN HP J2300D es un equipo compacto construido con tecnología de punta y cuyo propósito es detectar y resolver problemas de forma efectiva en redes LAN y WAN, se puede conectar en cualquier punto de la red, capturar todos los datos necesarios y realizar un análisis sobre éstos. Está conformado por un computador personal o MainFrame (Porción PC del Advisor) y un hardware modular de adquisición y trasmisión de datos (Undercradle), como también de un software

de análisis de red basado en el sistema operativo Microsoft Windows 98. El conjunto adquirido por la FIET consta de un MainFrame cuya referencia es Internet Advisor WAN HP J2300D, un Undercradle J3444A Fast Ethernet y un módulo de interfaz PRI J2296B E1/ISDN SIM.

- **EQUIPO UTILIZADO**
  - Internet Advisor WAN HP J2300D.
  - Dos cables de conexión RJ-45 100Base-TX.
  - Computador Personal con punto de red.
  - Punto de red adicional.
  - Computador con sistema operativo linux.

- **PROCEDIMIENTO**

A. Conexión Modo Nodo.

Esta conexión algunas veces conocida como punto a punto causa que el Internet Advisor actúe y sea visto como un nodo o punto independiente sobre la red. El Advisor observará todo el tráfico que pasa a través del hub de la misma forma que cualquier otro nodo Ethernet lo haría. El Advisor puede monitorear tráfico desde todas las estaciones teniendo el mismo dominio de colisión que el puerto del hub donde el Advisor es conectado. En este modo, el equipo también ***puede generar tráfico*** sobre la red.

1. Encienda el equipo y conecte el puerto etiquetado “To Hub/Switch” al punto de red adicional empleando un cable de conexión RJ-45 100Base-Tx de longitud apropiada.

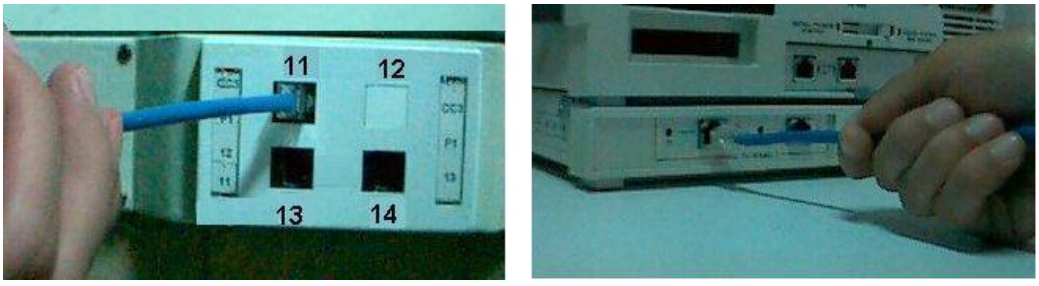


Figura 2.1. Proceso de Conexión Modo Nodo.

B. Especificación de parámetros para una conexión Modo Nodo.

2. Entre al software LAN Fast Ethernet Undercradle y seleccione la pestaña *Interface/Protocols*.

3. Seleccione en *Media Connection* la opción *TX 10Mb Ethernet*.

4. En *Line Mode* elija *Node Half Duplex*.

5. Seleccione en *Monitor Type* la opción *Continuous*.

6. En el campo *Buffer Size* escoja *22.00 MB*.

   Mediante esta configuración se ha establecido el monitoreo half duplex de todo el tráfico proveniente del Hub hacia los computadores bajo el dominio de colisión de éste a una velocidad de línea de 10 Mbps en una red 10 BaseT. El monitoreo seleccionado es continuo y se capturan todos los Bytes de cada paquete para ser almacenados en un buffer cuya capacidad máxima es de 22 MB.

7. Abra las *medidas* desde el *Analizador Experto* hasta el *Decodificador* exceptuando *Pruebas Activas y Estadísticas de Protocolo VLAN*.

8. Capture tráfico para las *medidas* anteriores durante cinco minutos. Verifique que la conexión se realizó con éxito, percatándose que el led denominado *"Receiving from: Hub/ Switch"* en la parte frontal del Undercradle *titile* y el led del puerto RJ-45 *To Hub/Switch encienda*.

9. Terminada la captura de tráfico detenga las medidas y familiarícese con el entorno de trabajo observando los resultados arrojados por cada una de las *medidas abiertas anteriormente*. Responda las siguientes preguntas:

P 1.1. ¿Bajo este modo el Advisor *captura todo el tráfico entrante y saliente* del Laboratorio de Telemática?

P 1.2. ¿Cuál debe ser la configuración del Internet Advisor si se desea capturar todo el tráfico de los Hubs conectados a un switch en el Laboratorio de Telemática bajo la suposición de que existe un puerto (Donde el Advisor está conectado) en el switch al cual se reflejaría el tráfico de todos sus puertos?

P 1.3. Si desea monitorear un enlace del cual no conoce sus características. ¿Qué configuración emplearía?

P 1.4. ¿Si existieran errores de capa física, errores en niveles superiores y errores por *alta utilización* del ancho de banda de la red, cuales medidas del software LAN del Internet Advisor utilizaría en cada caso?

P 1.5. ¿Cuál es la medida que permite *la transmisión de paquetes* sobre la red y en que modo de operación?

C. Conexión Modo Monitor.

El modo monitor ***no permite generación de tráfico*** ya que su función es monitorear de forma transparente el tráfico cursado entre dos puntos de la red seleccionados. Este modo es usado normalmente en un ambiente conmutado en el cual el Advisor es situado entre un puerto de un switch o hub y un segmento de red u otro dispositivo.

10. Tome un computador que posea una NIC, un punto de red y una conexión a Internet activa. Conecte el puerto del Undercradle *"To Node"* a la NIC del PC mediante otro cable de conexión RJ-45 100Base-Tx (Cable blanco).

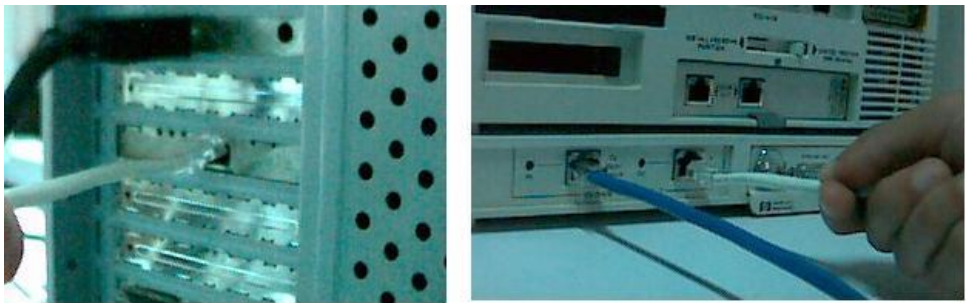


Figura 2.2. Proceso de Conexión Modo Monitor.

D. Especificación de parámetros para una conexión Modo Monitor.

11. Seleccione en *Media Connection* la opción *TX Fast Ethernet.*

12. Escoja en *Line Speed 10 Mb*.

13. En *Line Mode* elija *Monitor Full Duplex Both Directions*.

14. Seleccione en *Monitor Type* la opción *Timed* y escriba en las casillas correspondientes del campo *Monitor Period (hhh:mm)* 000-05.

15. Habilite la casilla de verificación *Packet Slicing* y digite en el campo *Packet Size* el número *200*.

16. En el campo *Buffer Size* escoja *26.00 MB*.

    Mediante esta configuración se ha establecido el monitoreo full duplex del tráfico cursado entre el PC y el hub en ambas direcciones a una velocidad de línea de 10 Mbps en una red Ethernet. El monitoreo seleccionado es temporizado con una duración de cinco minutos y se capturan los 200 primeros Bytes de cada paquete para ser almacenados en un buffer de captura cuya capacidad máxima es de 26 MB.

17. Abra el *Decodificador* e inicie la captura de tráfico. Responda afirmativamente a la caja de diálogo que aparece una vez haya terminado el proceso de captura.

P 1.6. ¿Sin tráfico saliente del PC, por qué y que tipo de tráfico monitorea el Internet Advisor entrando al PC?

P 1.7. ¿Cuál sería la configuración del HP J2300D para el enlace Fast Ethernet entre Atenea y un Switch si se desea observar pasivamente todo el tráfico cursado entre ellos hasta que el buffer de captura se llene?

P 1.8. En el PC ejecute el Internet Explorer a cualquier URL. ¿ El *Modo Monitor* afecta la conexión activa a Internet del computador?

P 1.9. ¿Si se apaga el Internet Advisor, la conexión entre el PC y el punto de red se mantiene?

E. Monitoreo del *Login* y *Password* de una cuenta.

18. En el PC ejecute Outlook Express y configure una cuenta de tal manera que pueda consultar su correo electrónico en el servidor de la Red de Datos de la Universidad del Cauca (*atenea.ucauca.edu.co*). Adicionalmente, configure los parámetros necesarios para *mantener una copia de los mensajes* en atenea.

19. Mantenga la conexión **Modo Monitor** anteriormente realizada. Vaya a la pestaña *Interface/Protocols* del Advisor, deshabilite la casilla de verificación *Packet Slicing* e inicie la captura de tráfico.

20. Presione el botón *Enviar y recibir todo* en la barra de herramientas de Outlook Express y detenga el *Decodificador* una vez se hayan descargado los mensajes de la cuenta de correo.

21. Habilite las casillas *Summary* y *Hex* y presione el botón *Search*. Seleccione la pestaña *Frame Attributes*, habilite el campo *Floating position search* y escriba en el área de texto de la fila etiquetada como *000000* su ***login***. Presione *OK*.

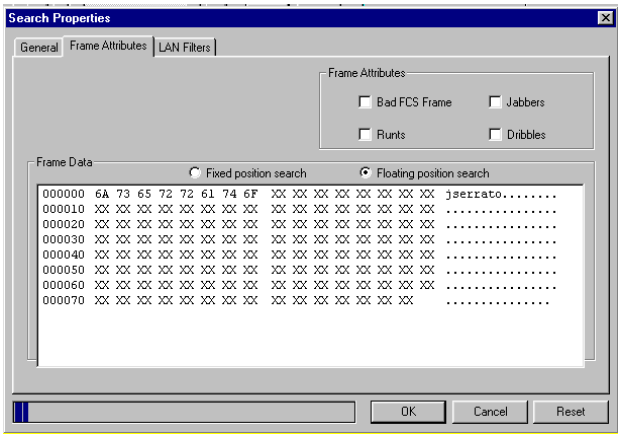


Figura 2.3. Búsqueda de un login empleando la opción Search del Decodificador.

22. Repita el punto anterior pero consigne su *password* en lugar del *login*.

23. Cierre Outlook Express y abra el programa SSH. Corra de nuevo el *Decodificador*, consulte su correo en el servidor Atenea y luego ciérrelo. Detenga el *Decodificador* y mediante la funcionalidad *Search* trate de encontrar su *login* y *password* de la misma manera que con Outlook Express.

24. Realice el anterior punto pero desde la página web de la Universidad del Cauca.

P 1.10. ¿Por qué no pudo encontrar su *login* y *password* en los dos casos anteriores?

P 1.11. Realice una *conexión* y *configuración* en **Modo Nodo** conectando el Advisor al punto de red adicional**,** reconecte el PC a su punto de red original y repita los anteriores pasos. ¿Se obtienen los mismos resultados que con la conexión *Modo Monitor*?

F. Monitoreo del login y password utilizando las aplicaciones FTP y Telnet.

25. Mantenga la conexión y configuración en **Modo Nodo** anteriormente realizada, active el *Decodificador* y establezca una conexión con el ftp de la Universidad (odín.ucauca.edu.co). Ver Figura 2.4. Escriba el *login* **anonymous** y posteriormente el *password*, el cual puede ser cualquier cuenta de correo electrónico, por ejemplo, jsanchez@hotmail.com.

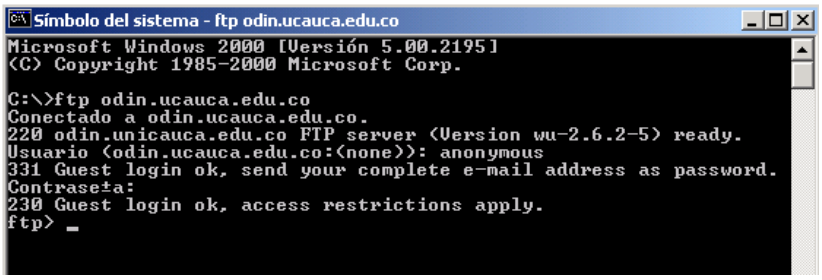


Figura 2.4. Conexión al FTP de la Universidad del Cauca.

P 1.12. Detenga el *Decodificador* y busque el *login* y *password* anteriormente introducidos. Realice el anterior procedimiento para una conexión y configuración en **Modo Monitor**. ¿Qué resultados obtuvo?

26. Realice una conexión y configuración en **Modo Nodo**, active el *Decodificador* y desde el PC ejecute un *Telnet* al computador con sistema operativo *Linux* cuya IP es: 200.30.71.50. Introduzca la palabra *invitado* como *login* y como p*assword*. Salga del *Telnet* y detenga el *Decodificador*.

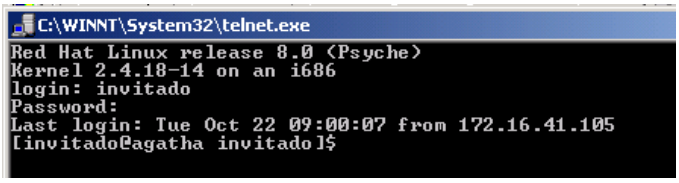


Figura 2.5. Telnet a una máquina Linux.

NOTA: Si el computador con sistema operativo Linux no está activo pruebe con otro el cual debe tener previamente configurada una cuenta *invitado* con su respectivo *login* y *password.*

P 1.13. Trate de encontrar su *login* y p*assword* dentro del tráfico capturado. Realice el anterior procedimiento para una conexión y configuración en **Modo Monitor**. ¿Por qué razón tanto el login como el password bajo esta aplicación se capturan caracter a caracter y no de forma completa?

- **CONCLUSIONES**

2.1.2. Práctica No 2. Descubrimiento de Nodos Activos en la Red

- **OBJETIVOS:**

  - Utilizar la herramienta denominada *Node Discovery* con el fin de hallar el conjunto de todos los *nodos activos* sobre la Red de Datos de la Universidad del Cauca e identificar los eventos generados por ellos.
  - Emplear la gama de utilidades que presenta la herramienta *Node Discovery*.
  - Utilizar el primer conjunto de medidas que ofrece la herramienta *Active Tests*.

- **MARCO TEÓRICO**

Dirección MAC: Las direcciones MAC identifican dispositivos de red en redes de área local que implementan direcciones MAC IEEE del nivel enlace de datos y son únicas para cada interfaz LAN, también denominadas "Direcciones Hardware" o "Direcciones Físicas". Están conformadas por 48 bits expresados en 12 dígitos hexadecimales, los primeros 6 son administrados por la IEEE e identifican al fabricante o vendedor y comprenden el Identificador Ùnico Organizacional (OUI) y los últimos 6 dígitos comprenden el número serial de la interfaz u otro valor administrado por el vendedor específico

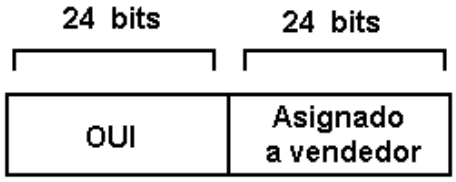


Figura 2.6. Estructura de una dirección MAC.

Este tipo de *"Direcciones Físicas"* se encuentran en las tarjetas Ethernet o Token Ring, son inmutables, no poseen ninguna semántica de localización geográfica asociada y algunas veces son llamadas *burned-in addresses (BIAs)* ya que son grabadas en una memoria ROM y copiadas en la RAM cuando la tarjeta de interfaz se inicializa.

Dirección IP: Es una *"Dirección Lógica",* jerárquica, configurable mediante software y tiene asociada un significado geográfico. Cada host en una red TCP/IP tiene una dirección única de 32 bits dividida en dos partes principales: la dirección de red y la dirección de host. La primera identifica una red y debe ser asignada por el Centro de Información de Red Internet (InterNIC) si la red va a ser parte

de Internet y la segunda identifica un host sobre la red y es asignado por el administrador de la red local.

El direccionamiento IP soporta cinco clases de direcciones diferentes: A, B, C, D, E y solamente las tres primeras son utilizadas comercialmente.

a) Direcciones Clase A: Utilizan el primer byte para identificar la NetId (Dirección de red) y los tres restantes para indicar el HostId (Dirección de host), teniendo en cuenta que el primer bit de la NetId es siempre cero (0). Su formato es el siguiente:

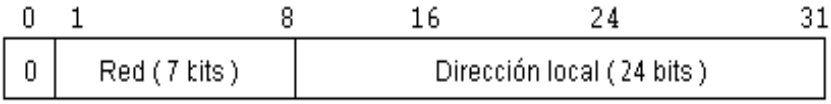


Figura 2.7. Dirección IP clase A.

Así se tienen $2^7 - 2 = 126$ redes posibles de direccionar y $2^{24} - 2 = 16777214$ hosts de identificar en cada una de ellas. Por este motivo, esta clase corresponde a redes grandes con muchas máquinas. Ahora si se toma el primer byte se observa que el primer valor posible es **0**0000000 (0) y el último lo constituye **0**1111111 (127). Por tanto el rango de direcciones Clase A en decimal será desde 0.1.0.0 hasta 127.0.0.0. Sin embargo esta última dirección IP se reserva para *loopback* y está diseñada para usarse sólo en pruebas TCP/IP y para la comunicación de los procesos internos en la máquina local.

b) Direcciones Clase B: Emplean los dos primeros bytes para identificar la NetId y los dos restantes para indicar el HostId, teniendo en cuenta que los dos primeros bits de la NetId son siempre uno y cero (1,0). Su formato es el siguiente:

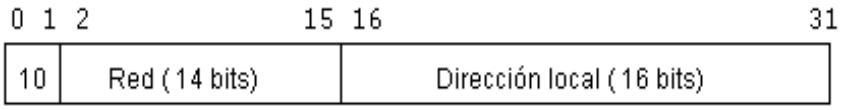


Figura 2.8. Dirección IP clase B.

De esta forma se tienen $2^{14} - 2 = 16382$ redes posibles de direccionar y $2^{16} - 2 = 65534$ anfitriones de identificar en cada una de ellas. Siguiendo el proceso anterior en las direcciones IP clase A se tiene que el rango de las direcciones Clase B va de 128.0.0.0 (Primer byte=**10**000000 (128)) hasta 191.255.0.0 (Primer byte= **10**111111 (191)).

c) Direcciones Clase C: Destinan los tres primeros bytes para identificar la NetId y el byte sobrante para indicar el HostId, teniendo en cuenta que los tres primeros bits de la NetId son siempre uno, uno y cero (1,1,0). Su formato es el siguiente:

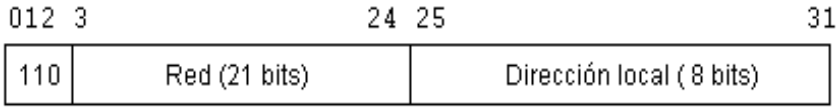


Figura 2.9. Dirección IP clase C.

Significa que se puede direccionar hasta 2^{21}– 2=2097150 redes posibles, cada una con 2^{8}– 2=254 anfitriones. Las direcciones de esta clase están comprendidas entre 192.0.1.0 (Primer byte= **110**00000) y 223.255.255.0 (Primer Byte=**110**11111).

d) Direcciones Clase D: Dedican 28 bits para propósitos de *multidifusión* cuando se quiere una difusión general a más de un dispositivo. Se caracterizan porque los cuatro primeros bits más significativos de los cuatro octetos son uno, uno, uno y cero (1,1,1,0). Su formato es el siguiente:

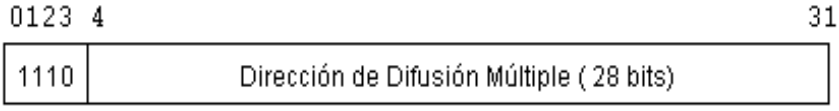


Figura 2.10. Dirección IP clase D.

El rango es desde 224.0.0.0 (Primer byte=**1110**0000) hasta 239.255.255.255 (Primer byte= **1110**1111).

e) Direcciones Clase E: Aunque su uso es futuro, el rango va desde 240.0.0.0 (Primer Byte=**11110**000) hasta 247.255.255.255 (Primer byte= **11110**111).

NOTA: En este esquema de direccionamiento no es permitido que existan direcciones con todos los bits 1's o todos los bits 0's, razón por la cual se deben restar dos direcciones para NetId y HostId en todas las clases.

Direccionamiento de subred: Las redes IP pueden ser divididas en redes más pequeñas denominadas subredes o subnets y este proceso se conoce como subnetting cuya ventaja principal es permitir a una sola dirección de red (Dirección IP oficial) abarcar muchas redes físicas. Las subredes están bajo el

dominio o administración local, es decir, las demás redes al exterior de este dominio observan una organización como una red única y no tienen conocimiento detallado de su estructura interna.

Dada una dirección de red, ésta puede ser dividida en muchas subredes, por ejemplo, si a un país se le asigna la dirección 180.93.0.0, las direcciones 180.93.1.0, 180.93.2.0, 180.93.3.0,..., 180.93.255.0 constituyen subredes dentro de la red 180.93.0.0.

Máscaras de subred: Debido a la actual escasez de direcciones IP la mayoría de las organizaciones vienen realizando su plan de direcciones empleando el esquema de subnetting, el cual consiste en que una vez la organización posee su dirección o direcciones IP, se emplea una máscara que divide el HostId en SubNet + Host. De esta forma lo que se logra es incrementar el número de subredes al interior de la organización, pero se sacrifica un número determinado de direcciones IP.

Para realizar subnetting se fija una máscara que consiste de cuatro bytes, semejantes a una dirección IP. Esta máscara es asignada por el proveedor de servicios de conexión a Internet acorde con las necesidades y planes de crecimiento de la organización y se debe tener en cuenta que la máscara debe ser de 1's contiguos y que no se permiten SubNet (SubNetId) ni Host en todos 1's o 0's.

Ejm: A una institución en Colombia afiliada a Internet se el asigna por parte de InterNIC la dirección de red 200.21.83.0 con máscara 255.255.255.0. Utilizando los tres bits de mayor peso del último octeto de la máscara dada, determinar las posibles subredes, los hosts en cada subred y el número total de ellos posibles a direccionar.

Dirección IP de red: 200.21.83.0
Máscara de Subred: 255.255.255.0

Esta dirección IP de red corresponde a una clase C, lo que implica tres bytes para NetId y sólo un byte para SubNetId y Host. Si se toma la máscara y se transforma a su equivalente binario:

255.255.255.0 = 11111111. 11111111. 11111111. 00000000
< **Red** > < **Host** >

Tomando los tres bits de mayor peso del último octeto en la máscara: **000**0 0000, se tienen las siguientes combinaciones:

000	No se debe usar	001	Primera Subred
010	Segunda Subred	011	Tercera Subred
100	Cuarta Subred	101	Quinta Subred
110	Sexta Subred	**111**	Submáscara

Luego: **001**0 0000 equivale a 32 Primera Subred
0100 0000 equivale a 64 Segunda Subred
0110 0000 equivale a 96 Tercera Subred
.
.
.
1100 0000 equivale a 192 Sexta Subred
1110 0000 equivale a 224 Submáscara

Primera Subred: - Dirección de red: 200.21.83.32
-Máscara: 255.255.255.224
-Hosts: 200.21.83.33, 200.21.83.34, 200.21.83.35,..., 200.21.83.62.

Segunda Subred: - Dirección de red: 200.21.83.64
-Máscara: 255.255.255.224
-Hosts: 200.21.83.65, 200.21.83.66, 200.21.83.67,..., 200.21.83.94.
.
.
.

Sexta Subred: - Dirección de red: 200.21.83.192
-Máscara: 255.255.255.224
-Hosts: 200.21.83.193, 200.21.83.194, 200.21.83.195,...,200.21.83.222.

Total Hosts por cada Subred: $2^5 - 2 = 30$

Total Hosts a direccionar: $30 * 6 = 180$

Formato de datagrama IP: Los campos del paquete IP son los siguientes,

- *Versión:* Indica la versión del protocolo Internet usado actualmente.
- *Longitud del Encabezamiento IP* (IHL): Indica la longitud del encabezado para el datagrama en palabras de 32 bits.
- *Tipo de Servicio:* Especifica al protocolo de capa superior como debe manejar el datagrama actual y le asigna diversos niveles de importancia.

- *Longitud Total:* Especifica la longitud en bytes del paquete IP entero, incluyendo datos y cabecera.

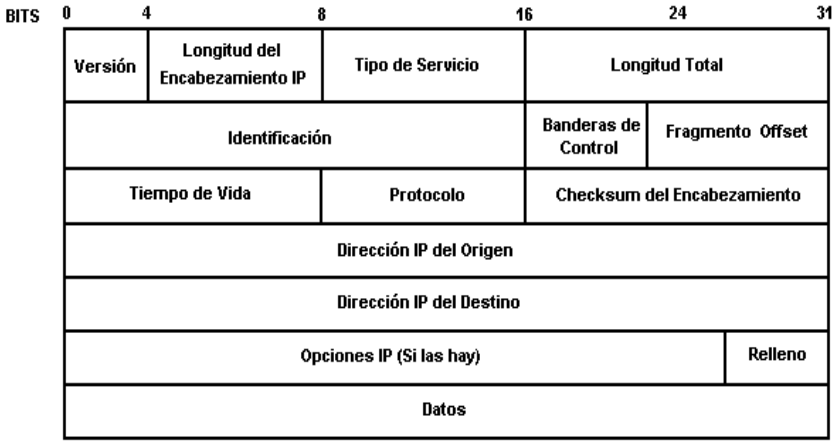


Figura 2.11. Datagrama IP.

- *Identificación:* Contiene un entero que identifica el datagrama actual. Este campo es utilizado para ayudar a ensamblar los fragmentos del datagrama IP.
- *Banderas de Control:* Consiste de un campo de 3 bits de los cuales los dos de bajo orden controlan la fragmentación. El bit de más bajo orden especifica si el paquete puede ser fragmentado, el del medio indica si el paquete es el último fragmento y el tercer bit no es usado.
- *Fragmento Offset:* Indica la posición de los datos del fragmento con respecto al comienzo de los datos en el datagrama original, lo cual le permite al proceso IP destino reconstruir adecuadamente el datagrama original.
- *Tiempo de Vida:* Contiene un contador que se decrementa gradualmente hasta cero en cuyo punto el datagrama es descartado. Este mecanismo evita que paquetes IP circulen indefinidamente sobre la red.
- *Protocolo:* Indica que protocolo de nivel superior recibe los paquetes entrantes después de que el procesamiento IP culmina.
- *Checksum del Encabezamiento:* Ayuda a asegurar la integridad del encabezado IP.
- *Dirección IP del Origen:* Especifica el nodo transmisor.
- *Dirección IP del Destino:* Especifica el nodo receptor.
- *Opciones IP:* Permite a IP soportar diversas opciones, tales como seguridad.

- *Relleno:* Conjunto de bits en "0" para asegurar que la longitud del encabezamiento sea múltiplo exacto de 32 bits.
- *Datos:* Contiene la información de las capas superiores.

PING (Packet Internet Groper): Es una herramienta de diagnóstico para verificar la conectividad entre dos computadores en una red. Envía paquetes ICMP con Solicitud de Eco a una dirección IP remota, observa las respuestas ICMP e indica el tiempo exacto que tardan los paquetes en ir y volver desde la máquina origen hasta la máquina destino.

Ejemplo: C:\> ping atenea
Haciendo ping a atenea [200.21.83.129] con 32 bytes de datos:
Respuesta desde 200.21.83.129: bytes=32 tiempo<10ms TTL=255
Respuesta desde 200.21.83.129: bytes=32 tiempo<10ms TTL=255
Respuesta desde 200.21.83.129: bytes=32 tiempo<10ms TTL=255
Respuesta desde 200.21.83.129: bytes=32 tiempo<10ms TTL=255

Estadísticas de ping para 200.21.83.129:
Paquetes: enviados=4, recibidos=4, perdidos= 0 (0% perdidos).

La salida puede dividirse en tres secciones. La primera sección, la línea empezando con la palabra "PING", muestra un vistazo del comando. La segunda sección, las líneas que empiezan con "64 bytes" muestran las respuestas obtenidas. La tercera sección, todo después de la línea "--- atenea ping statistics ---", muestra un sumario de los resultados. En este caso, los resultados son buenos, ninguno de los paquetes fueron perdidos y todos pasaron suficientemente rápido.

TRACEROUT: Este comando permite observar la ruta que siguen paquetes UDP desde la máquina fuente a la destino. El "traceroute" se basa en ICMP. Envía un datagrama IP con un tiempo de vida (TTL) de 1 al host de destino. El primer "router" que vea el datagrama decrementará el TTL a 0 y devolverá el mensaje ICMP "Tiempo excedido" ("Time Exceeded"), además de eliminar el datagrama. De este modo se identifica el primer "router" del camino. Este proceso se puede repetir sucesivamente con valores mayores del TTL con el fin de identificar la serie de "routers" que se encuentran en el camino hasta el host de destino. En realidad, el "traceroute" envía al host de destino datagramas UDP que referencian un número de puerto que está fuera del rango usado normalmente. Esto permite al "traceroute" determinar cuando se ha alcanzado el host de destino, es decir, cuando recibe el mensaje ICMP "Puerto inalcanzable" ("Port Unreachable").

ARP (Address Resolution Protocol): Es un protocolo estándar específico de las redes y es responsable de convertir las direcciones de protocolo de alto nivel (Direcciones IP) a direcciones de red físicas (Direcciones MAC). En una sola red física, los hosts individuales se conocen a través de su dirección física. Los protocolos de alto nivel direccionan a los hosts de destino con una dirección simbólica (En este caso la dirección IP). Cuando tal protocolo quiere enviar un datagrama a la dirección IP de destino w.x.y.z, el driver del dispositivo no la entiende.

En consecuencia, se suministra un módulo (ARP) que traducirá la dirección IP a la dirección física del host destino. Utiliza una tabla (Llamada a veces *caché ARP*) para realizar esta traducción. Cuando la dirección no se encuentra en la caché ARP, se envía un *"Broadcast"* en la red, con un formato especial llamado *petición ARP*. Si una de las máquinas en la red reconoce su propia dirección IP en la petición, devolverá una *respuesta ARP* al host que la solicitó. La respuesta contendrá la dirección física del hardware así como información de encaminamiento, tanto esta dirección como la ruta se almacenan en la caché del host solicitante. Todos los posteriores datagramas enviados a esta dirección IP se podrán asociar a la dirección física correspondiente, que será la que utilice el driver del dispositivo para mandar el datagrama a la red. ARP se diseñó para ser usado en redes que soporten broadcast por hardware. Esto significa, por ejemplo, que ARP no funcionará en una red X.25.

RARP (Reverse Address Resolution Protocol): Realiza la operación inversa de ARP, es decir, obtiene la dirección IP a partir de la dirección MAC. Algunos hosts, como por ejemplo estaciones de trabajo sin disco, desconocen su propia dirección IP cuando arrancan. Para determinarla, emplean un mecanismo similar al ARP, pero ahora el parámetro conocido es la dirección hardware del host y el requerido su dirección IP. La diferencia básica con ARP es el hecho de que debe existir un "servidor RARP" en la red que mantenga una base de datos de direcciones hardware a direcciones de protocolo.

Topología actual Red de Datos de la Universidad del Cauca: La topología actual es de dos estrellas, interconectadas. Una en el IPET y otra en el CARMEN. Todos los enlaces entre edificios están en fibra óptica. Las estrellas físicamente son Switches de Fast Ethernet.

La Universidad del Cauca tiene dos enlaces (Uno a 1536 Kbps y otro a 1024 kbps), el primero es de ORBITEL con la dirección 200.30.71.0/24 (Máscara: 255.255.255.0) y el segundo de TELECOM con la dirección 200.21.83.0/24 (Máscara: 255.255.255.0). En este último caso la red de datos se encuentra dividida en dos sub-redes: la 200.21.83.128/26 (Máscara: 255.255.255.192) que es la principal y 200.21.83.64/26 (Máscara: 255.255.255.192) que es la secundaria.

NO OFICIALES: Para el interior de la Universidad, la dirección que se utiliza es la 172.16.0.0/16 (Máscara: 255.255.0.0).

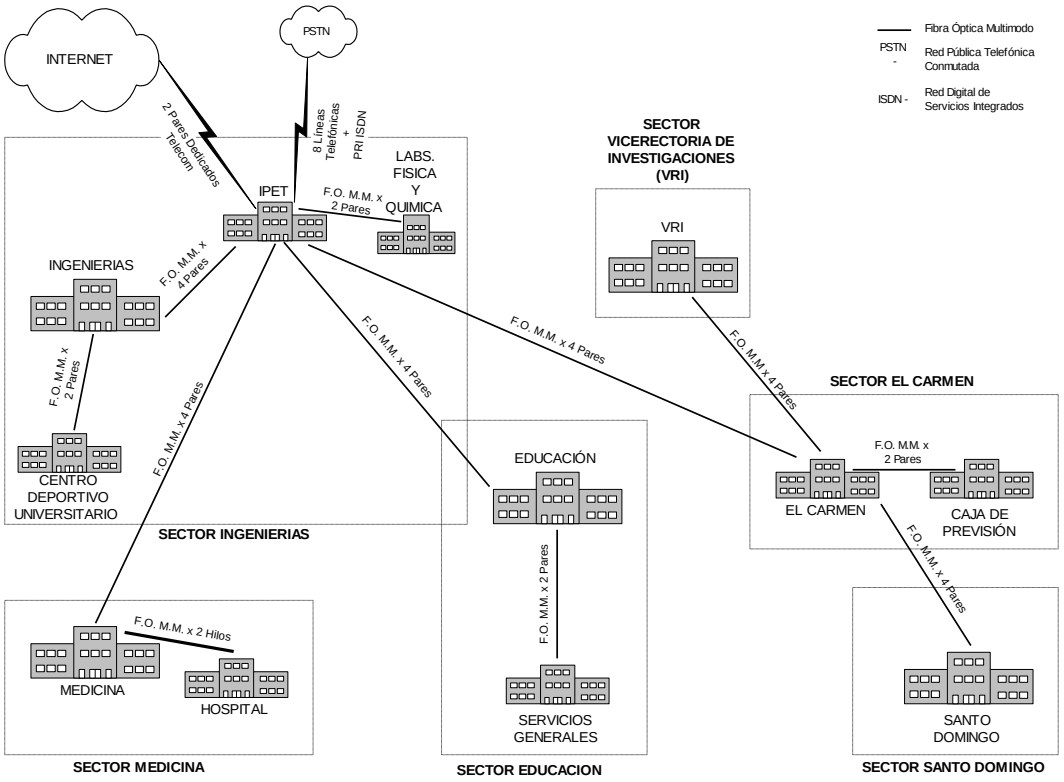


Figura 2.12. Topología Actual Red de Datos Universidad del Cauca.

Debido al número limitado de direcciones IP públicas, y para obtener un mejor desempeño, ésta se ha dividido en subredes de la siguiente forma

Tabla 2.1. Subredes Red de Datos Universidad del Cauca.

SECTOR	SUBRED
Santo Domingo	172.16.10.0
	172.16.11.0
Artes	172.16.20.0
El Carmen	172.16.30.0
Ingenierías	172.16.40.0
	172.16.41.0
Salud	172.16.50.0
VRI	172.16.60.0
Laboratorios	172.16.70.0
Casa Rosada	172.16.80.0
Caja de Previsión	172.16.90.0

Museo Mosquera	172.16.100.0
Educación	172.16.110.0
Servicios Generales	172.16.120.0
IPET	172.16.130.0
Biblioteca – División Comunicaciones	172.16.140.0
CDU	172.16.150.0
Ciencias Agropecuarias	172.16.160.0
Hospital	172.16.170.0

- **EQUIPO UTILIZADO**

  - Internet Advisor WAN HP J2300D.
  - Cable de conexión RJ-45 100Base-TX.
  - Punto de red (Puerto de un Hub) para el Internet Advisor.
  - Computador con punto de red.
  - Computador con sistema operativo linux.

- **PROCEDIMIENTO**

A. Utilización de la herramienta Node Discovery.

1. Encienda el equipo, realice una conexión en **Modo Nodo** y entre al software LAN Fast Ethernet Undercradle.

2. Especifique los parámetros de la ventana de configuración principal para realizar un monitoreo temporizado durante 5 minutos, a una velocidad de línea de *100 Mbps* y en un modo de línea *half duplex*. Mantenga el tamaño del buffer de captura a 26 Mb.

3. Abra el *Comentador y Estadísticas de Conexión* (Dado que la medida *Descubrimiento de Nodos* corre *automáticamente* al abrir una de ellas) e inicie la captura de tráfico.

4. Abra la medida *Descubrimiento de Nodos*. A continuación expanda el árbol y visualice todos los nodos sobre la red ordenados por sus direcciones MAC, el *nombre del nodo* (Si lo tiene), el *número y tipo de direcciones* bajo esa dirección MAC y el *protocolo* manejado. Expanda el primer nodo y observe la(s) dirección(es) de red.

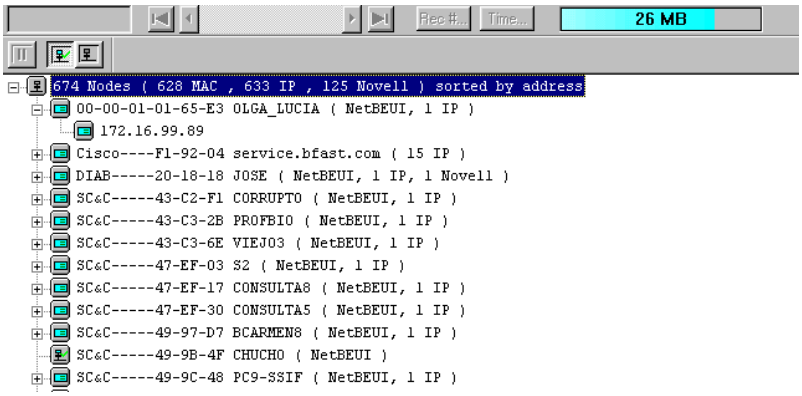


Figura 2.13. Resultados de la medida Descubrimiento de Nodos.

P 2.1. Escoja la opción *View IP Nodes* mediante el botón derecho del mouse. Consigne la información para 5 direcciones IP que considere adecuadas. El estado del nodo hace referencia a la descripción proporcionada por el ícono al lado de cada dirección.

Tabla 2.2. Identificación de nodos IP.

Dirección IP	Dirección MAC	Nombre del nodo	Estado del nodo

P 2.2. Seleccione la opción *View Novell IPX Nodes* y llene la siguiente tabla con los nodos que satisfacen la información solicitada.

Tabla 2.3. Identificación de nodos Novell.

Nombre	Network ID	Fabricante	Dir MAC	Estado del Nodo

P 2.3. Seleccione la opción *View Router Nodes* y llene la siguiente tabla**.**

Tabla 2.4. Identificación de Enrutadores.

Dir IP	MAC	Nombre

P 2.4. Seleccione una a una las siguientes opciones: *View Apple Talk Nodes*, *View DECnet Nodes*, *View OSI CLNP Nodes* y *VINES Nodes*. ¿Se encuentran nodos de estos tipos sobre la red?

NOTA: Cuando en una de estas opciones *no se encuentran nodos* que concuerden es necesario señalar el resultado y realizar *click con el botón derecho* del mouse para observar las demás opciones.

P 2.5. ¿Por qué se caracterizan los nodos visualizados con la opción *View Other Nodes*?

5. Seleccione las opciones *Sort Nodes by Event Severity* (Ordena los nodos por severidad de eventos) y *View IP Nodes*. Seleccione el primero de ellos, haga click con el botón derecho del mouse, escoja *Drill Into Commentator* y observe las opciones desplegadas: *From Address* (Muestra todos los eventos generados por el nodo seleccionado hacia cualquier otro), *To Address* (Muestra los eventos generados desde otros nodos hacia el seleccionado), *To or From Address* (Es la combinación de las dos opciones anteriores), *From Subnet* (Despliega los eventos generados desde la Subred a la cual pertenece el equipo, hacia cualquier otro nodo), *To subnet* (Despliega los eventos generados desde cualquier nodo hacia la Subred a la cual pertenece la máquina seleccionada) y *To or from Subnet* (Es una combinación de las dos opciones anteriores).

Figura 2.14. Despliegue de eventos para un nodo seleccionado.

P 2.6. Escoja la opción *From Address*, expanda progresivamente el árbol *Display Node Events* y consigne los valores solicitados en la *Tabla 2.5*.

NOTA: Las opciones *Display Connection Events* y *Display All Events* proporcionan la misma información que *Display Node Events*, pero organizada de forma diferente.

Tabla 2.5. Determinación de eventos para un nodo seleccionado.

Eventos	Número de eventos	Tipo de evento	Dir IP Problema	MAC's involucradas
Alertas (A)				
Warnings (W)				
Normales (N)				
IP Nodo seleccionado				

P 2.7. Seleccione el segundo nodo en la ventana *Node Discovery*, escoja la opción *To or From Subnet*, expanda progresivamente el árbol *Display Connection Events* (Esto se da siempre y cuando se presenten Eventos de Conexiones) y consigne los datos para la primera conexión. ¿Cuáles son las subredes involucradas en los eventos?

Tabla 2.6. Determinación de eventos entre nodos pertenecientes a diferentes subredes.

IP fuente / Puerto	IP destino / Puerto	No y tipo de alarmas	No y tipo de Warnings	No y tipo de Normals

6. En algunas ocasiones es conveniente *editar el nombre de un nodo* para su fácil reconocimiento y ubicación, *adicionar un nodo* que no está en la lista o borrar alguno que no se requiera. Con el *botón derecho del mouse* entre a *Add Node* y seleccione la opción *Add IP Node*. Introduzca en el campo *IP Address* el número 10.15.42.2, luego en el campo *Name* la frase *Nodo de Prueba* y en el campo *MAC Address* el número 09-D4-F5-6C-8B-99.

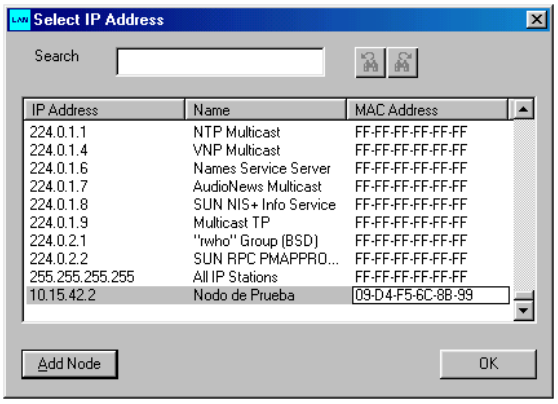


Figura 2.15. Adición y edición de un nodo IP.

7. Observe el anterior nodo en la ventana de la medida *Descubrimiento de Nodos*, reconozca su nombre y dirección MAC. Por último selecciónelo y elimínelo de la lista.

B. Utilización de las pruebas activas IP.

8. Seleccione el menú *Setup*, escoja la opción *Workspace Options* y modifique los siguientes campos de la pestaña *LAN Addresses*:

   - *Advisor IP Address:* 200.30.71.50.
   - *Default Routing Addr:* 200.30.71.254.
   - *DNS Server Addr*: 200.30.71.129.

9. Seleccione la medida *Pruebas Activas* y escoja *IP Ping*.

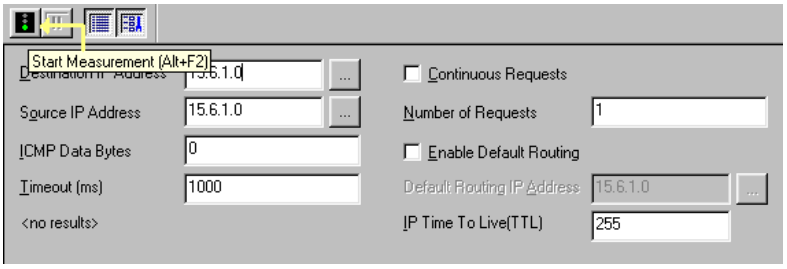


Figura 2.16. Prueba Activa IP Ping.

Llene los campos con la siguiente información:

- *Destination IP Address* (Máquina con la cual se quiere comprobar conectividad): 200.21.83.190 (Olimpo).
- *Source IP Address* (Dirección IP del Advisor): Esta dirección es configurada en el campo *Advisor IP Address* de la ventana *Workspace Options* en el menú *Setup* o en ésta casilla de forma directa.
- *ICMP Data Bytes* (Número de bytes que serán insertados dentro del campo de datos de los paquetes de requerimiento de eco ICMP, su valor oscila entre 0 y 1472): 20.
- *Timeout* (Cantidad de tiempo en milisegundos que el *IP Ping* espera por un paquete de respuesta ICMP después de haberse enviado uno de requerimiento. Este valor debe ser mayor a 1000 ms y menor de 60 000 ms): 2000.
- *Continuos Requests:* Deshabilitada.
- *Number of Requests:* 8.
- *Enable Default Routing* (Cuando este campo es activado, el Advisor utiliza la dirección del campo *Default Routing IP Address* con el fin de resolver a través de este enrutador la dirección destino a probar): Habilitado.
- *IP Time To Live* (Configura la distancia en hops que puede alcanzar un Ping cuyo máximo valor es 255): 255.
- Inicie la prueba activa *IP Ping* y escriba el password de transmisión: "advisor" en la caja de diálogo que aparece.

10. Seleccione la medida *Pruebas Activas* y escoja *IP ARP*.

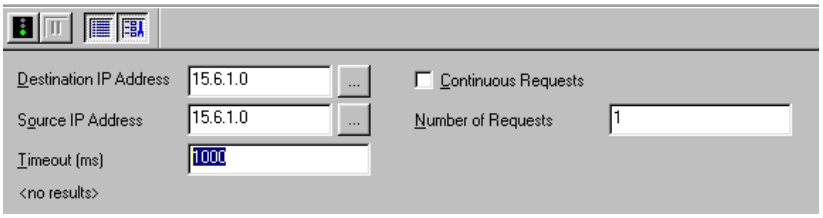


Figura 2.17. Prueba Activa IP ARP.

Introduzca los siguientes valores:

- *Destination IP Address:* 200.30.71.129 (Atenea).
- *Timeout (ms):* 1000.
- *Number of Request:* 2. Corra la prueba activa.

P 2.8. Utilizando el par anterior de pruebas activas llene la siguiente tabla:

Tabla 2.7. Utilización de las pruebas activas IP Ping y ARP.

IP Nodo Destino	Nodo Activo (Si / No)	Dirección(es) MAC
172.16.255.200 (hércules)		
200.30.71.131 (Odin)		
200.30.71.137 (Acuario)		
200.31.71.254 (Orbitel)		
216.239.51.100 (google)		
209.73.164.90 (altavista)		
64.58.79.230 (yahoo)		
198.133.219.25 (cisco)		
192.6.118.44 (Heweltt Packard)		

11. Cierre todas las medidas, vaya a la pestaña *Interface Protocols* y seleccione la opción *TX Auto Negotiate* del campo *Media Connection*.

12. Entre al *Decodificador,* presione el botón *Filter,* expanda el árbol *Station Filters* en su totalidad y seleccione la opción IP del campo *Type*. Escoja *Source <any Stn>* y digite en el campo *IP Address* la dirección IP del computador de trabajo (PC A) por ejemplo 172.16.41.105, de igual forma en el campo *Dest <any Stn>* escriba la dirección IP de otro equipo activo (PC B). Por último active la casilla *Reverse Direction* y presione *OK*. Responda afirmativamente al mensaje de advertencia que aparece a continuación.

P 2.9. Active el *Decodificador* y desde el PC A realice un *ping* dirigido hacia el PC B. Terminado el comando detenga el *Decodificador* y explique de forma detallada cada uno de los campos que conforman los *mensajes ICMP* de *solicitud* y *respuesta* de eco.

P 2.10. ¿Cuál es la diferencia fundamental a nivel de formato entre este par de mensajes?

13. Active el *Decodificador* y en el PC A ejecute el comando: C:\> ping –l 500 [Dirección IP PC B]. Luego repita el mismo comando sólo cambiando el parámetro *500* con un valor de *5000*. Detenga la medida y de acuerdo al campo *IP: Fragmentation Info* en ambos casos responda:

P 2.11. ¿Existe fragmentación, y de ser así, a partir de que valor en bytes se comienza este proceso?

14. Edite el filtro anteriormente creado, seleccione *Dest <any Stn>* y escriba en el campo IP Address la dirección IP de una máquina linux.

15. Active el *Decodificador* y ejecute desde la máquina linux el comando *ping –Q 88 [Dirección IP del PC A]*. Detenga la medida y observe el campo *IP: Type of Service= 88*.

P 2.12. ¿Cómo quedaron configurados los campos *Precedence* (prioridad), *Delay*, *Througtput* y *Reliability* con el parámetro 88?

16. Seleccione la prueba activa *IP RARP*.

    Introduzca los siguientes valores:

    - *Destination MAC Addr:* 00-C0-4F-01-39-96 (atenea).
    - *Timeout (ms):* 1000.
    - *Number of Request:* 5. Corra la prueba.

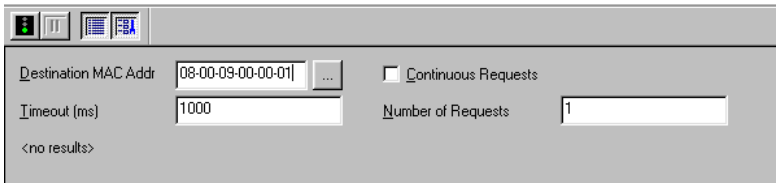


Figura 2.18. Prueba Activa IP RARP.

P 2.13. Con las direcciones MAC encontradas en la *Tabla 2.7* compruebe las direcciones IP. ¿Qué resultados obtuvo, explique?

17. Abra el *Decodificador* y elimine el filtro anteriormente creado.

18. Seleccione *IP Trace Route*.

    Introduzca los siguientes valores:

    - *Destination IP Address:* 216.239.51.100 (google).
    - *Timeout (ms):* 1000.
    - *Enable Default Routing:* Habilitar.
    - *IP Time To Live (TTL):* 255. Corra la medida.

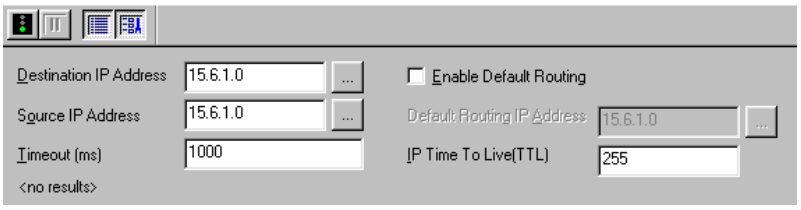


Figura 2.19. Prueba Activa IP Trace Route.

P 2.14. Realice la anterior prueba con los nodos de la Tabla 2.7. Anote el número de saltos y las direcciones IP de los Routers para aquel que complete la ruta.

19. Seleccione el menú *Setup*, escoja la opción *Workspace Options* y modifique los siguientes campos de la pestaña *LAN Addresses*:

- *Advisor IP Address:* 172.16.40.130.
- *Default Routing Addr:* 172.16.255.254.
- *DNS Server Addr*:172.16.255.200.(Hercules).

20. Seleccione la prueba activa *IP Active Net Discovery*.

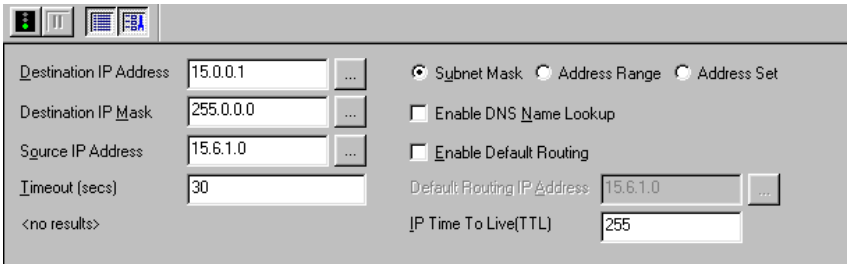


Figura 2.20. Prueba Activa IP Active Net Discovery.

Llene los campos con la siguiente información:

- Habilite *Subnet Mask:* Esta opción permite identificar el conjunto de *nodos activos* de la subred a la cual pertenece el host cuya dirección IP se introduce en el campo *Destination IP Address*.
- *Destination IP Address:* 172.16.41.103.
- *Destination IP Mask:* Es la máscara de Subnet correspondiente a la dirección IP destino introducida en el anterior campo. 255.255.255.0.
- *Timeout (sec):* 40.

- Habilite la casilla *Enable DNS Name Lookup:* Permite conocer los nombres de los nodos a descubrir.
- Habilite la casilla *Enable Default Routing*.
- *IP Time To Live (TTL):* 255.Corra la medida.

P 2.15. ¿Cuantas máquinas encontró?

21. Seleccione la opción *IP Active Net Discovery* y llene los campos con la siguiente información:

- Habilite *Address Range:* Esta opción permite identificar el conjunto de nodos activos entre el par de direcciones digitadas en los campos *Destination IP Address* y *Dest IP End Addr*.
- *Destination IP Address:* 172.16.41.101. (ryst01).
- *Dest IP End Addr:* 172.16.41.115. (ryst15).
- *Timeout (sec):* 40.
- Habilite la casilla *Enable DNS Name Lookup*.
- Habilite la casilla *Enable Default Routing*.
- *IP Time To Live (TTL):* 255. Corra la medida.

P 2.16. Tomando como referencia la *Tabla 2.1. Subredes Red de Datos Universidad del Cauca.* ¿Cuál es el número de hosts activos para cada subred?

- **CONCLUSIONES**

2.1.3. Práctica No 3. Configuración y Utilización de Filtros de Captura y Despliegue

- **OBJETIVOS:**

- Configurar y manejar los filtros de captura y despliegue tanto a nivel de *protocolos* como de *estación*.
- Buscar datos dentro de las tramas mediante el filtrado de bytes específicos.

- **MARCO TEÓRICO**

Filtros LAN: Se utilizan para *capturar* sólo tramas de interés, *excluir* aquellas que no lo sean o *detener* todas las medidas activas ante la presencia de una en particular liberando de esta manera al buffer de captura de información innecesaria. Cada filtro creado utiliza recursos de memoria y entre más complicado es, mayor es la cantidad de recursos que emplea. La etiqueta *Capture Filters* lista todos los filtros creados y la barra progresiva en la parte inferior de la misma indica la cantidad de recursos hardware usados por los filtros existentes y los recursos que aún están disponibles.

VLAN (Virtual LAN): Esta opción es una configuración global que afecta a todos los filtros de protocolos y estaciones. El panel derecho se utiliza para seleccionar el tipo e identificación de VLAN y posee los siguientes campos:

- *VLAN Type (Encapsulaciones):* Permite seleccionar el tipo de VLAN que se desea utilizar.
- *Cisco ISL:* Define un identificador VLAN de 15 bits.
- *802.1 p/Q:* Constituye el estándar IEEE 802.1 p/Q que define como los switches Ethernet pueden *clasificar tráfico* con el fin de entregar tráfico bajo condiciones críticas de tiempo, además, describe métodos importantes para el suministro de *calidad de servicio* a nivel MAC.
- *VLAN ID:* Este campo puede aceptar rangos separados por guiones o comas, así, "1-8,10" es un entrada válida. Además todas las entradas están limitadas por la capacidad de la tecnología VLAN (Por ejemplo, el ID VLAN para CISCO debe ser de 15 bits).
- *Reset:* Clarea todos los filtros LAN.

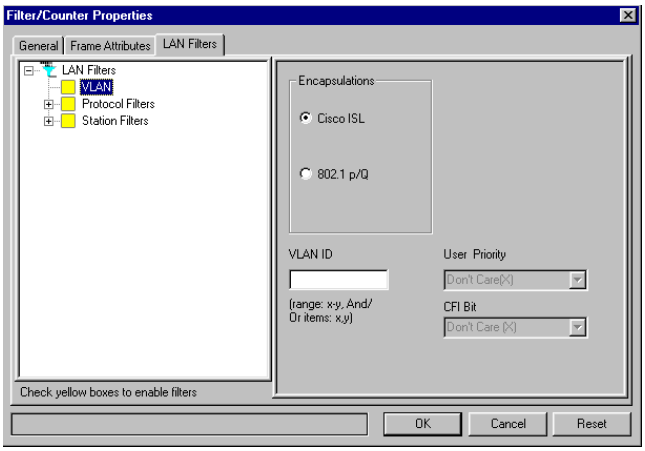


Figura 2.21. Filtros VLAN.

Filtros de Protocolo: Permiten capturar sólo las tramas que contienen los protocolos especificados por el usuario y además se puede filtrar más de uno de ellos a la vez. Algunos de los protocolos tienen opciones de encapsulación adicionales y se presentan a continuación:

Tabla 2.8. Protocolos soportados por los filtros del Advisor.

Protocolo/Stack	Encapsulación	Protocolo/snack	Encapsulación
802.2	No	SNA	No
SNAP	No	ARP	Yes
NetBEUI (NetBIOS/IBM)	No	IP	Yes
Net Beui/SMB	No	Novell	Yes
3COM/NetBIOS	No	Sun	Yes
AppleTalk AARP	Yes	AppleTalk DDP	Yes
Banyan VINES	Yes	LAT	Yes
DECnet	Yes	ISO	Yes
ISO CLNP	Yes	XNS-IDP	Yes
Other SAPs/Etypes Ethernet		Yes	

Filtros de estación: Permiten filtrar tráfico sobre direcciones de estaciones y combinaciones específicas de protocolos. Se puede buscar una estación teniendo una dirección MAC o una de protocolo de red en particular, filtrar el tráfico desde o hacia una estación o encontrar un host determinado que utiliza un protocolo específico. Cuando se define uno o más filtros mediante esta opción, el campo *Frame Data* en la pestaña *Frame Attributes* permite filtrar sobre contenidos de datos de trama específicos en combinación con las *direcciones de fuente y destino*.

Se tienen las siguientes opciones:

- *Type:* Se utiliza para filtrar sobre un protocolo específico.
- *Source <any Stn>:* En este campo se digita la dirección de la máquina fuente sobre la que se desea filtrar teniendo en cuenta que el formato debe coincidir con el protocolo seleccionado.
- *Dest <any Stn>:* En este campo se digita la dirección de la máquina destino sobre la que se desea filtrar teniendo en cuenta que el formato debe coincidir con el protocolo seleccionado.
- *Reverse Direction:* Este ítem invierte el sentido de filtrado de la fuente y destino seleccionados. Por ejemplo, si se filtra sobre la fuente A y se habilita la caja Reverse Direction, el filtro buscará las tramas que se originan y se dirigen hacia ella.
- *Advanced:* Proporciona opciones adicionales dependiendo del tipo de protocolo seleccionado en el campo *Type.*
- *Other Station Filters:* Adiciona un nuevo filtro de estación.

Pestaña Atributos de trama: Contiene dos etiquetas *Frame Data y Frame Attributes.* La primera permite especificar una *secuencia de bytes* con el propósito de filtrar aquellas tramas que concuerden con ésta. La máxima cantidad de bytes sobre la cual se puede operar para realizar el anterior proceso corresponde a los primeros 127 bytes (00-7F) de la trama de red Fast Ethernet. El filtro definido en la pestaña *Frame Attributes* y su correspondiente en la pestaña *LAN Filters* funcionan mediante una operación AND, esto es, las condiciones especificadas en ambas pestañas deben ocurrir simultáneamente en una trama para que se filtre.

La segunda etiqueta contiene condiciones de error de las tramas a nivel MAC Ethernet (*Bad FCS, Runts, Jabbers* y *Dribbles*) y por lo tanto permite un filtraje de tramas con estas características.

Filtros de despliegue: Operan sobre las tramas que están almacenadas en el *buffer de captura* (Modo Post-procesamiento) y son utilizados cuando se tiene un gran número de ellas y se desean observar de forma rápida sólo aquellas que interesan para el estudio en cuestión. Esta utilidad se despliega presionando el botón *Filter* en la barra de herramientas del *Decodificador* y posee dos pestañas: *Frame Attributes y LAN Filters* cuyo funcionamiento es idéntico a sus homólogas en los *filtros de captura*.

Formato de la trama Fast Ethernet: El formato de trama utilizado en las redes Fast Ethernet es la trama 802.3, con una longitud mínima de 64 bytes y una longitud máxima de 1512 bytes.

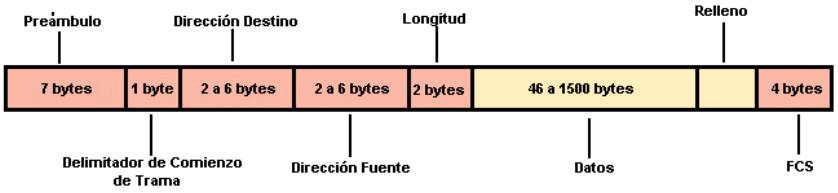


Figura 2.22. Trama Fast Ethernet.

Cada trama se divide en 8 campos, de longitud fija todos excepto dos, los de *datos y relleno*.
Los campos de la trama son los siguientes:

- *Preámbulo:* Tiene una longitud de 7 bytes, formada por la siguiente combinación de unos y ceros: 10101010. Este campo hace posible la sincronización para que el resto de los campos sean recibidos correctamente.
- *Delimitador de Comienzo de Trama:* Está compuesto por el siguiente octeto: 10101011. Aparece a continuación del preámbulo.
- *Dirección destino:* Tienen una longitud de 2 o 6 bytes, en cualquier caso fija para cada aplicación. El primer bit de la dirección destino indica si es una dirección individual o la dirección de un grupo de DTE's. Este bit es conocido como bit I/G. Cuando todos los bits de la trama se encuentran en 1, se trata de una trama de difusión, y la trama será recibida por todos los DTE's de la LAN.

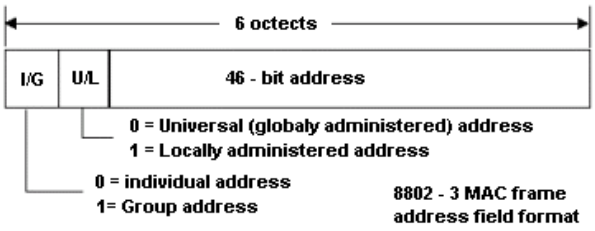


Figura 2.23. Campo Destino.

- *Dirección fuente:* Tiene el mismo formato que el campo de dirección destino y sirve para especificar la dirección de la estación emisora.
- *Longitud de Datos:* Está compuesto de 2 bytes en los que se codifica el número de bytes que ocupa el campo de datos.
- *Datos:* Este campo es de longitud variable y son los datos que se transmiten en la trama.
- *Relleno:* Como el campo de datos es de longitud variable, es posible que la trama final resultante no cumpla el requerimiento de longitud mínima de la trama, que es de 64 bytes. En este caso, a continuación del campo de datos se colocan los bits de relleno que falten para completar la trama de longitud mínima.

- *FCS:* Este campo contiene información para que el destino compruebe si la trama recibida no ha sufrido alteraciones durante el trayecto.

❑ **EQUIPO UTILIZADO**

- Internet Advisor WAN HP J2300D.
- Cable de conexión RJ-45 100Base-TX.
- Computador con punto de red (Puerto de un Hub).

❑ **PROCEDIMIENTO**

A. Creación de un filtro de captura de protocolos.

1. Encienda el equipo, realice una conexión en **Modo Nodo** y entre al software LAN Fast Ethernet Undercradle.

2. Realice una conexión en **Modo Nodo** y especifique los parámetros de la ventana de configuración principal para realizar un *monitoreo autonegociado* que capture tráfico durante 5 minutos. Mantenga el tamaño del buffer de captura a 26 Mb.

3. Seleccione la pestaña *Capture Filters* y escoja la opción *Add*. Escriba en el campo *Label* **"**Tráfico WWW" y en el campo *Description* "Filtro que captura solo tráfico Web".

4. Seleccione las casillas *On y Store Frame* en las opciones *State y Action* respectivamente.

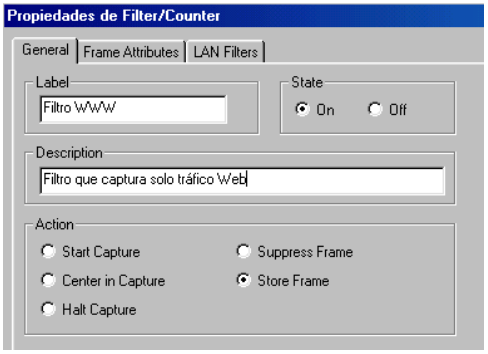


Figura 2.24. Creación filtro de captura WEB.

5. Seleccione la pestaña *LAN Filters*, expanda secuencialmente el árbol *Protocol Filters* e *IP*, luego señale la casilla *Other TCP/UDP Port*. En el panel derecho habilite la casilla *TCP*, en el campo

Source digite *3128* y en el campo *Name* escriba "Trafico WEB". Presione *Add*, habilite la casilla *Tráfico WEB* en el *árbol IP* y presione *OK*.

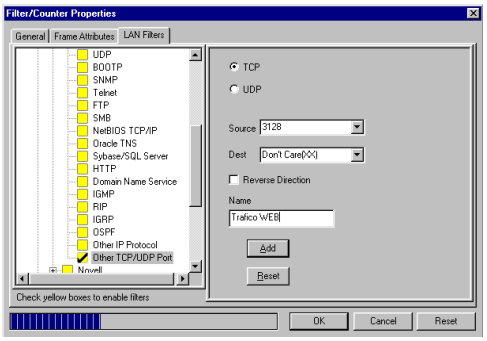


Figura 2.25. Filtro de captura WEB empleando el puerto TCP 3128.

6. Realice una copia del filtro anteriormente creado, edítela y realice los siguientes cambios:
   - *Label:* "Tráfico no WWW".
   - *Description:* "Captura todo tráfico a excepción del Web".
   - *State:* Of.
   - *Action:* Suppress Frame.

7. Adicione un filtro de protocolo que *capture tráfico ARP*, almacene todas las tramas que concuerden con él, cuyo estado se encuentre activo y que utilice la *encapsulación Ethernet ARP*. Asimismo adicione dos filtros para Telnet y DNS. El resultado final de los filtros creados se ilustra a continuación:

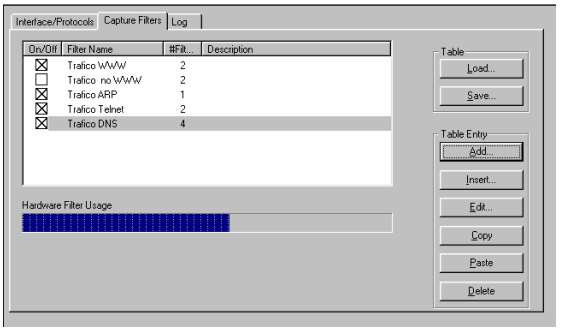


Figura 2.26. Filtros de captura creados.

P 3.1. ¿Por qué al crear el filtro WEB no se seleccionó el protocolo HTTP en el árbol IP?

8. Guarde los filtros en la carpeta *C:\\My Documents\Archivos de Datos\Practica No 3* e inicie la captura de tráfico. Responda *afirmativamente* a la caja de diálogo.

9. Entre al *Decodificador* y habilite sólo las *vistas resumida* y *detallada*. Con el *botón derecho del mouse* despliegue las opciones de esta herramienta y siga la ruta | Display Options | Lines | Multi|, con el propósito de organizar la información en líneas múltiples para su mejor visualización.

P 3.2. ¿Con cuales campos del formato de protocolo proporcionados por el par de vistas, se puede comprobar que las tramas son efectivamente ARP, Telnet, DNS y Web?

B. Filtro de captura para estación fuente.

10. Cierre el *Decodificador* y elimine los filtros anteriores.

11. Seleccione *Add***,** escriba en el campo *Label* **"**Filtro 2" y en el campo *Description* "Filtra todo tráfico proveniente del FTP (Odin.unicauca.edu.co) hacia cualquier destino". Habilite las casillas *On y Store Frame* en las opciones *State y Action* respectivamente.

NOTA: En realidad este filtro recoge todo el tráfico proveniente del FTP pero que se dirige al dominio de colisión (Hub al cual está unido el Advisor) al cual está conectado el equipo.

12. Seleccione la pestaña *LAN Filters*, expanda el árbol *Station Filters*, luego el de *Source <any Stn> Dest <any Stn>* y habilítela.

13. Señale *Type IP* y seleccione en el campo etiquetado con *Type* la opción *IP*.

14. Señale *Source* <any Stn> y escriba 172.16.255.131 (odin.unicauca.edu.co) en el campo *IP Address.* Presione *OK*. Guarde el filtro e inicie la captura de tráfico.

15. Ejecute el Internet Explorer y coloque en el campo de localización ftp://172.16.255.131 o ftp://odin.ucauca.edu.co o ftp://ftp.ucauca.edu.co. Descargue un archivo cualquiera a través de este servicio.

P 3.3. Finalizada la captura entre al *Decodificador* y verifique la *fuente* de todos los paquetes. ¿Cuáles son los números de puertos que utiliza el servicio FTP?

C. Filtro de captura para estación destino.

16. Elimine el filtro creado anteriormente, presione el botón *Add***,** escriba en el campo *Label* **"**Filtro 3" y en el campo *Description* "Captura todo tráfico dirigido hacia un destino específico". Habilite las casillas *On* y *Store Frame* en las opciones *State* y *Action* respectivamente.

17. Realice los pasos 12 y 13. Señale *Dest <any Stn>* y escriba la dirección IP del computador que le fue asignado para esta práctica . Presione *OK*.

18. Guarde este filtro, vaya a la pestaña *Interface/Protocols* y modifique el tiempo de captura a 3 minutos e inicie la captura de tráfico.

19. Desde otro computador (PC B) baje un archivo de una página web (p.e. www.cybercursos.net) y ejecute un ping a la IP del PC asignado. Desde este último descargue un archivo del ftp de la universidad. Utilizando el *Decodificador* verifique que efectivamente el tráfico capturado tiene como destino único la dirección IP configurada en el filtro.

D. Filtro de captura para estaciones fuente y destino en ambas direcciones.

20. Cierre el *Decodificador* y elimine el filtro creado anteriormente. Presione el botón *Add***,** escriba en el campo *Label* **"**Filtro 4" y en el campo *Description* "Captura todo el tráfico cursado entre una fuente y un destino". Habilite las casillas *On* y *Store Frame* en las opciones *State* y *Action* respectivamente.

21. Escoja la pestaña *LAN Filters* y expanda el árbol *Station Filters* en su totalidad. En *Type IP* seleccione *IP*, en *Source* <any stn> escriba 172.16.255.131 (odin.unicauca.edu.co) , en *Dest* <any stn> digite la dirección IP del computador que le ha sido asignado y habilite la casilla *Reverse Direction*. Presione *OK*.

22. Guarde este filtro e inicie la captura de tráfico. Abra dos sesiones de FTP, una con jano (ftp://jano.ucauca.edu.co/) y otra con el ftp de la universidad (ftp://ftp.ucauca.edu.co/), seleccione uno o varios archivos en cada caso y descárguelos al computador asignado. Además copie archivos empleando el entorno de red y páginas de Internet. Compruebe que el tráfico capturado pertenece sólo a la conexión entre odin y el computador asignado.

NOTA: Si por alguna razón alguno de los servidores *Jano* u *Odin* no se encuentra en servicio realice el filtro, con cualquier otro servidor que conozca.

E. Filtro de captura utilizando puertos para estaciones en ambas direcciones.

23. Elimine el filtro creado anteriormente. Presione el botón *Add***,** escriba en el campo *Label* "Filtro 5" y en el campo *Description* "Captura tráfico POP 3 y SSH". Habilite las casillas *On* y *Store Frame* en las opciones *State* y *Action* respectivamente.

24. Escoja la pestaña *LAN Filters* y expanda el árbol *Station Filters* en su totalidad. En *Type IP* seleccione *TCP*. Señale *Source <any stn>* y en el campo *Source TCP Port#* digite el número *110 (POP 3),* señale *Dest <any stn >* y escriba en el campo *IP Address* la IP del equipo asignado. Habilite la casilla *Reverse Direction*.

25. Señale *Other Station Filters* y presione el botón *Press here to add a station filter*. En *Type IP* seleccione *TCP*. Señale *Source <any stn>* y en el campo *Source TCP Port#* digite el número *22 (SSH),* señale *Dest <any stn >* y escriba en el campo *IP Address* la IP del equipo asignado. Habilite la casilla *Reverse Direction*. Presione *OK*.

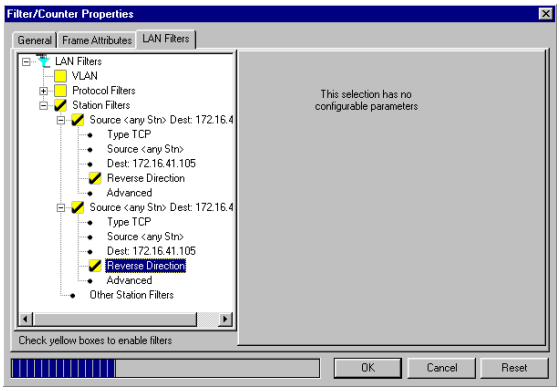


Figura 2.27. Filtros de captura para los servicios POP 3 y SSH.

26. Guarde el filtro, corra la medida y consulte su cuenta de correo electrónico con la Universidad empleando los programas SSH y Outlook Express desde el computador asignado y otro PC. Verifique el correcto funcionamiento del filtro.

F. Filtros de captura entre una fuente y múltiples destinos.

27. Elimine el filtro creado anteriormente. Presione el botón *Add***,** escriba en el campo *Label* "Filtro 6" y en el campo *Description* "Filtro entre una fuente y múltiples destinos". Habilite las casillas *On* y *Store Frame* en las opciones *State* y *Action* respectivamente.

28. Escoja la pestaña *LAN Filters* y expanda el árbol *Station Filters* en su totalidad. En *Type IP* seleccione *TCP*. Señale *Source <any stn>* y escriba en el campo *IP Address* 172.16.255.163 (jano.ucauca.edu.co) y *Don`t Care(X)* en el *campo Source TCP Port#.* Señale *Dest <any stn>* e introduzca la dirección IP del computador asignado y seleccione *Don`t Care(X)* en el campo *Dest TCP Port#* . Habilite la casilla *Reverse Direction*.

29. Señale *Other Stations Filters* y presione el botón *"Press here to add a station filter".* Expanda el árbol *Source <any stn> Dest <any stn>* y realice el anterior procedimiento *dos veces* más cambiando únicamente la dirección *IP Address de destino* por las de otros dos computadores en la sala que se encuentren conectados a Internet y posean el mismo dominio de colisión.

30. Guarde el filtro, corra la medida, establezca una conexión a ftp://jano.ucauca.edu.co/ en cada uno de los computadores escogidos y descargue archivos desde éstos. Además navegue a otras páginas web y copie archivos a través del entorno de red.

31. Abra el *Decodificador* una vez la medida haya terminado y verifique que los paquetes capturados tienen como *fuente/destino* jano o cualquiera de los tres computadores.

P 3.4. Realice el siguiente filtro (Un solo destino y múltiples fuentes), guárdelo y corra la medida: Filtro que capture todo el tráfico hacia un solo *destino* (Computador asignado) y desde múltiples fuentes: 172.16.255.200 (DNS), dirección IP de un equipo activo en la sala, IP proxy para el equipo asignado, 172.16.255.129 (atenea), el ftp de la universidad (172.16.255.131).

G. Filtro de despliegue para protocolos.

32. Abra el siguiente archivo: C:\ Advisor\Lan\Data\Archivos de practicas\LabTelematica1.dat, luego el *Decodificador* y presione el botón *Filter* que se encuentra en la barra de herramientas de esta medida.

33. Seleccione la etiqueta *LAN Filters*, expanda el árbol *Protocol Filters*, active la casilla *Novell* y presione *Aceptar*.

P 3.5. Repita el anterior procedimiento para los *stacks de protocolos* SUN, y NetBEUI (NetBios/IBM) y ARP (uno a la vez). Anote la estructura a nivel de encabezados de las tramas de estos cuatro stacks.

H. Filtrado de bytes específicos.

34. Borre el último filtro de despliegue, seleccione la pestaña *Frame Attributes* y escriba en el área de texto de la ventana *Frame Data* la secuencia: 03 00 00 00 00 01 00 00 21 6f 22 c9 00 2f f0 f0 empezando desde *el primer byte.*

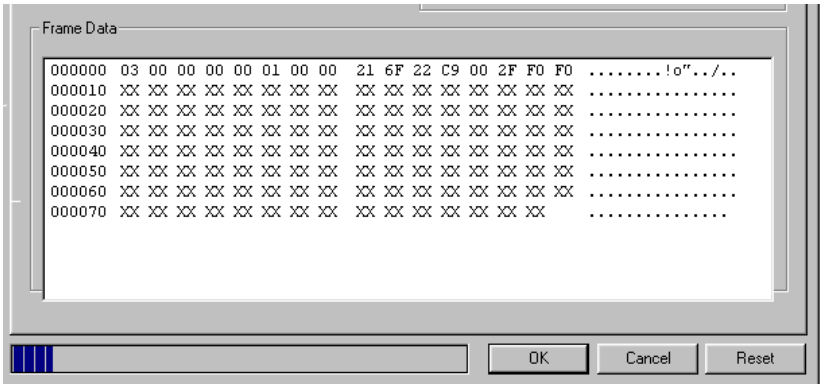


Figura 2.28. Búsqueda de trama con secuencia especial de bytes.

P 3.6. ¿Cuál sería la secuencia de datos y su ubicación dentro del área de texto de la ventana *Frame Data* si se desea encontrar el conjunto de tramas cuya dirección fuente es 200.21.83.160?

- **CONCLUSIONES**

2.1.4. Práctica No 4. Monitoreo de Errores de Capa Física

- **OBJETIVOS:**

- Detectar y analizar errores de nivel físico, observar su porcentaje, su origen y su naturaleza
- Detener las medidas del Advisor en presencia de un error o evento en particular.
- Determinar que stack de protocolos (TCP/IP, Novell, NetBEUI, otros) y que protocolos del Stack TCP/IP (HTTP, FTP, Telnet, SNMP, SMTP, etc.) están siendo utilizados por los equipos dentro del segmento que se está midiendo y la proporción de utilización de cada uno de ellos.

- **MARCO TEÓRICO**

Errores en redes Ethernet: Es importante considerar que los errores no son siempre críticos en redes Ethernet, las colisiones por ejemplo son una parte normal y solo deberían ser investigadas cuando han sufrido un incremento considerable con respecto al *baseline* (Medida y registro del estado de operación de la red sobre un periodo de tiempo, que sirve de base para operación y control). Los errores FCS son más críticos y pueden degradar severamente el desempeño de la red hasta niveles muy bajos. Cuando se examina el tipo de error capturado durante una sesión de análisis de protocolo es importante verificar con mucho cuidado el tipo de éste y cualquier dirección Ethernet asociada en la trama con el fin de identificar la causa.

Colisiones de red: El acceso a una red Ethernet es regulado por el algoritmo CSMA-CD en el cual una estación Ethernet escucha la red para determinar si hay tráfico presente, cuando la red está libre, ésta transmite y escucha nuevamente para ver si los datos colisionaron con el tráfico de otra estación. Si todo está claro, la trasmisión se completa, si una colisión ocurre, la estación espera una cantidad corta de tiempo aleatoria y retransmite la información. Así es un error tratar de eliminar completamente las colisiones, ya que éstas son una propiedad natural de las redes Ethernet.

Conforme la utilización de la red crece, la tasa de colisiones también crecerá. La pregunta es cual es la cantidad normal o anormal de colisiones. Las redes pueden tener lapsos cortos (Generalmente un segundo) donde la tasa de colisiones crece hasta un 20% o 25% lo cual es normal, pero si la tasa de colisiones excede un promedio del 5% se debe considerar dividir la red. Los segmentos de red con lapsos cortos de colisiones de un 30% deben ser estudiadas cuidadosamente. La única forma de reducir la tasa de colisiones sobre un segmento es disminuyendo el tráfico sobre éste y la forma más efectiva es realizando una división con un bridge, router o un switch Ethernet.

Las colisiones no afectan el desempeño de la red tan negativamente como se podría pensar. Si una de éstas ocurre dentro de los primeros 64 bytes de una trama Ethernet, la trama es retransmitida por los circuitos de la NIC en un tiempo insignificante, sin involucrar mecanismos superiores a la capa enlace de datos.

Colisiones Remotas: Ocurren cuando se recibe un fragmento el cual es probablemente el resultado de una colisión en otro sector de la red. El fragmento debe ser más corto de 64 bytes, tener un FCS erróneo y contener un patrón alternado de 1's y 0's.

Colisiones tardías: Estas ocurren después de que los 64 bytes iniciales de una trama han sido transmitidos y causan la retransmisión por capas de protocolo superiores, usualmente la capa de transporte, degradando notoriamente el desempeño de la red. Estas suelen ser desplegadas como Bad FCS's o errores de alineación y deben ser eliminadas de la red.

Si una red Ethernet está construida con todas las especificaciones (Se utiliza el cableado adecuado, los segmentos de cable no exceden las longitudes máximas y el número de repetidores/Hubs están dentro de los límites), entonces todas colisiones deberían ser detectadas adecuadamente y las tramas retransmitidas por la capa de enlace de datos, sin la presencia de colisiones tardías.

Colisiones tardías remotas: Ocurren cuando se recibe un fragmento el cual es probablemente el resultado de una colisión tardía en otro sector de la red. El fragmento debe ser más largo de 64 bytes, tener un FCS erróneo y contener un patrón alternado de 1's y 0's.

FCS: Estos errores pueden resultar de NICs defectuosas o pueden ser el resultado de colisiones tardías (De hecho muchos errores FCS pueden realmente ser colisiones tardías). Este tipo de errores tienen el mismo efecto que las colisiones tardías, las tramas deben ser retransmitidas por los protocolos de capas superiores, usualmente la capa de transporte, con un resultado negativo sobre el desempeño de la red.

Si remplazando la NIC en la estación sospechosa no se eliminan los FCSs erróneos, se debe revisar que la longitud de los cables no excedan el máximo permitido o que no exista un número excesivo de repetidores/Hubs. Otras causas de estos errores incluyen cables coaxiales puestos de forma incorrecta a tierra, interferencia electromagnética (EMI) producida por luces fluorescentes, conectores dañados, cables retorcidos o de baja calidad.

Si estos errores son detectados en un segmento o área de la red es conveniente utilizar un probador DTR (Time Domain Reflectometer) para confirmar que el cable en esa área cumple las especificaciones.

NOTA: Cuando se implemente una red Ethernet es conveniente utilizar la regla 5-4-3 para el número de repetidores. No más de 5 segmentos con repetidores, no más de 4 repetidores entre cualquier par de estaciones y solo 3 de esos segmentos pueden contener estaciones (Los otros dos deben ser segmentos de enlace, conectando 2 repetidores sin estaciones).

RUNTs: Son tramas cuya longitud es menor a 64 bytes usualmente el resultado de colisiones, sin embargo, si una trama runt está bien formada (Posee un FCS válido), entonces ésta es el resultado de una NIC defectuosa o su driver. Se detectan con el Internet Advisor cuando se observa un incremento regular en el conteo de RUNTs, sin una correspondiente actividad de FCSs, en cuyo caso es necesario determinar que estación está enviando esas tramas, observando la dirección fuente en el Decodificador.

JABBERs: Son tramas largas que exceden 1518 bytes causadas generalmente por el mal funcionamiento de una interfaz que no paró su transmisión. Estos errores deben ser eliminados porque evitan el acceso de otros nodos a la red. Si un jabber tiene un FCS erróneo, éste es probablemente el resultado de una NIC defectuosa, si posee un FCS correcto, éste puedo haber sido causado por los drivers de la NIC.

MISALIGNS (Pérdida de alineación o sincronismo): Son tramas que poseen un número de bits que no es divisible por ocho y un FCS erróneo, causadas generalmente por desadaptación de impedancia en componentes hardware.

DRIBBLE: Es una trama intermitente recibida sin errores pero que posee uno a más bits extraños al final.

NOTA: Cuando se experimentan problemas intermitentes, como un alto nivel de errores sobre una red Ethernet, se pueden utilizar las técnicas de generación de tráfico para cargar la red con el fin de hacer evidentes las causas de estos errores. Generando tráfico adicional sobre la red, ésta se puede tensionar lo suficiente para causar que ciertas fallas en los componentes salgan a la superficie.

TRIGGERS: Son acciones que ocurren ante la presencia de determinados eventos o condiciones y son utilizados y configurados en tres tipos de medidas.

1. Condiciones en filtros de captura: Corresponden a las acciones en la pestaña General de la ventana *Filter/Counter Propierties* y su descripción se presenta a continuación.

- ✓ *Start Capture:* Cuando se observa una trama que concuerda con el filtro inicia la captura y detiene esta operación cuando el buffer se ocupa en su totalidad.
- ✓ *Center in capture:* Almacena la primera trama que concuerde con el filtro de captura y detiene esta operación.
- ✓ *Halt Capture:* Detiene todas las medidas activas cuando se detecta que una trama coincida con el filtro de captura.
- ✓ *Suppress Frame:* Las tramas que concuerdan con el filtro son excluidas del buffer.
- ✓ *Store Frame:* Es la opción habilitada por defecto y almacena todas las tramas que concuerden con el filtro.

2. Umbrales en Estadísticas Vitales de Protocolo: Se encuentran en la ventana de configuración de la medida, se habilitan en la columna *Stop-on* y detienen las medidas activas cuando se excede uno de los *umbrales* para la estadística a analizar en el stack de protocolo respectivo.

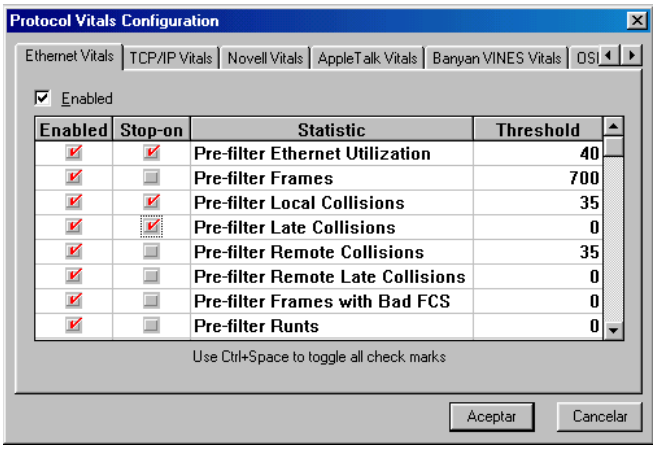


Figura 2.29. Utilización de Triggers en Estadísticas Vitales de Protocolo.

3. Eventos en el Comentador: Se activan en la *ventana de configuración* del *Analizador Experto* y detienen las medidas activas ante la presencia de un evento (*Alerta*, *Warning* y *Normal*) en particular.

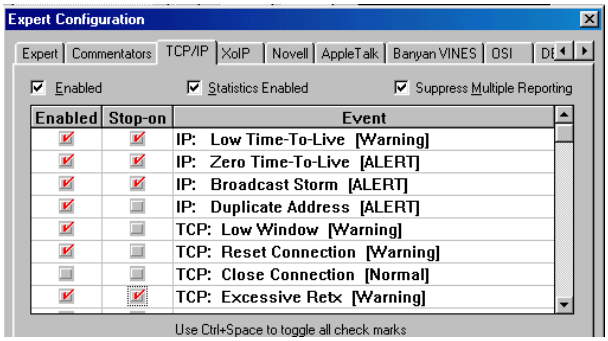


Figura 2.30. Utilización de Triggers en el Comentador.

- **EQUIPO UTILIZADO**
  - Internet Advisor WAN HP J2300D.
  - Cable de conexión RJ-45 100Base-TX.
  - Computador con punto de red (Puerto de un Hub).

- **PROCEDIMIENTO**

A. Análisis en modo de Post – Procesamiento.

1. Encienda el equipo, entre al software LAN Fast Ethernet Undercradle y abra el siguiente archivo: C:\ Advisor\Lan\Data\Archivos de practicas\ LabTelematica2.dat.

2. Abra la medida *Estadísticas Vitales de Protocolo*, expanda el árbol *Pre-filter Ethernet Utilization*, presione el botón *Run From Buffer* de la barra de herramientas de la medida, seleccione *All Frames* en la caja de diálogo *Run From Capture Buffer* y presione *OK*.

P 4.1. Consigne los valores en la siguiente tabla:

Tabla 2.9. Estadísticas de tramas erróneas en un segmento de red.

Medida	Average	Peak	Threshold Exceeded
Tramas Pre-filtradas			
Colisiones locales			
Colisiones tardías			
Colisiones remotas			
Colisiones tardías remotas			

Tramas con FCS erróneo			
Runts Pre-filtrados			
Misaligns			
Runts con Buen FCS			
Jabbers Post-filtrados			
Jabbers con FCS erróneo			
Dribbles Post-filtrados			

3. Abra la medida *Estadísticas de Nodo MAC*, presione el botón *Run From Buffer* de la barra de herramientas de la medida, seleccione *All Frames* en la caja de diálogo y presione *OK*. Por defecto la tabla de datos viene ordenada con los 20 nodos cuyo porcentaje de transmisión es *más alto*. Para identificar los nodos que están generando la mayor cantidad de errores, seleccione la columna *errors* con el *botón derecho del mouse* y escoja *Sort by this Column*. Presione *OK* en la caja de diálogo y vuelva a correr la medida utilizando el botón *Run From Buffer*.

P 4.2. Consigne los resultados en la siguiente tabla para los cinco primeros nodos generadores de errores:

Tabla 2.10. Fuentes generadoras de errores físicos.

Dirección Nodo / Nombre	No de errores	Tipo de errores	Porcentaje del total de errores

NOTA: Los tipos de errores tales como *FCS's erróneos*, *Jabbers*, *Runts* y *Dribbles* están representados respectivamente por las letras *F*, *J*, *R* y *D* en la columna *errors*.

4. Sobre la columna *Node Addr/Name* señale la celda correspondiente al primer nodo generador de errores y haga *doble click* sobre él para entrar al *Decodificador* (Crea un filtro de despliegue automático que muestra las tramas relacionados con ese nodo). Para analizar aquellas tramas que poseen errores, presione el botón *Filter* de la barra de herramientas del *Decodificador*, seleccione la pestaña *Frame Attributes* y habilite las casillas *Bad FCS Frame* , *Jabbers*, *Runts* y *Dribbles*. Presione *OK*.

5. Observe las características de las tramas *como longitud, estado del FCS* o *CRC*, los *mensajes de error desplegados en la ventana Detailed* y *secuencias de bits especiales en la ventana Hex***.**

P 4. 3. Determine el *tipo de error* predominante y la causa más probable de su origen.

P 4.4. Repita los pasos 4 y 5 para los cuatro nodos restantes de la Tabla 2.10.

P 4.5. Determine la dirección IP y MAC para los nodos de la Tabla 2.10, donde sea posible.

P 4.6. ¿Cómo se reconoce una *colisión remota* utilizando la vista Hex del *Decodificador*?

6. Vaya a la medida *Estadísticas de Nodo MAC* y con la opción *Delete Column(s)* desplegada con el *botón derecho del mouse* al ubicarse sobre la columna de la estadística respectiva elimine las columnas *frames tx/sec*, *frames rx/sec* y *errors/sec*. Adicione las columnas *frames tx, frames rx, broadcast* y m*ulticast*.

P 4.7. Llene la siguiente tabla y determine que porcentaje del *ancho de banda* utilizado corresponde a tráfico de broadcast y multicast. Verifique si los niveles medidos de tráfico Broadcast están dentro de lo permitido.

	Tramas tx	**Tramas rx**	**Broadcast**	**Multicast**	**% tx**	**% rx**	**% Broadcast**	**% Multicast**
Total								

NOTA: Para *broadcast* el tráfico en una red Ethernet no debe superar el 2% del ancho de banda del canal.

7. Abra la ventana de configuración de *Estadísticas de Nodo MAC*, cambie *# of Nodes To Track a 5* y presione *OK* (Para hacer efectivo este cambio es necesario volver a presionar el botón *Run From Buffer* desde la barra de herramientas de la medida).

P 4.8. Utilizando la opción *Sort by this Column* determine los *cinco* nodos que consumen *mayor ancho de banda*, que *reciben la mayor cantidad de tráfico*, que *generan* la mayor cantidad de *broadcast* y *multicast***.** Llene la siguiente tabla:

Tabla 2.11. TOP 5 utilizando Estadísticas de Nodo MAC.

TOP 5	Nodo 1	Nodo 2	Nodo 3	Nodo 4	Nodo 5
	Nombre / MAC				
Mayor BW en Tx					
Mayor BW en Rx					
Generan Broadcast					
Generan Multicast					

8. Seleccione la opción *Close (Data)* del menú *File* y realice una conexión en **Modo Nodo**. Especifique los parámetros de la ventana de configuración principal para realizar un *monitoreo autonegociado* durante 5 minutos e inicie las medidas.

9. Finalizada la captura guarde el registro mediante el menú *File / Save (Data)* en la carpeta C:\My Documents\Archivos de Datos\Practica No 4. En el campo **Save Options** deje habilitadas las casillas **Decode Data, MAC Node Stast** y **Protocol Vitals** y presione **Save.** Ver Figura 2.31.

P 4.9. Repita el análisis realizado entre los puntos 3 a 7.

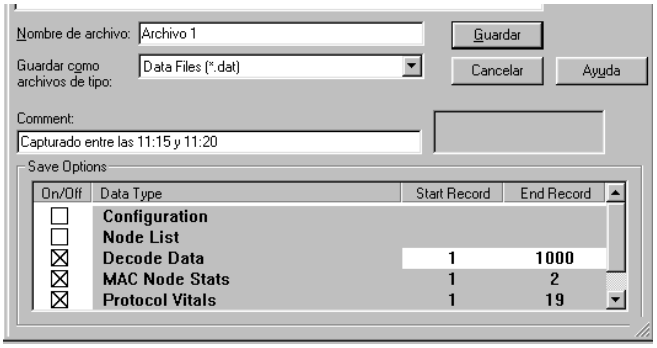


Figura 2.31. Almacenamiento de un registro para análisis en el modo de Post – Procesamiento.

B. Utilización de Triggers.

10. Abra la medida *Estadísticas Vitales de Protocolo,* posteriormente su ventana de *configuración* y seleccione la pestaña *Ethernet Vitals*. Active la casilla *Pre-filter frames* en la columna *Stop-on* e introduzca el número 200 en el campo *Threshold*. Presione *OK* y corra la medida.

11. Cuando se supere el límite, responda afirmativamente a la caja de diálogo la cual indica la causa de detención de las medidas.

12. Expanda el árbol *Pre-filter Ethernet Utilization* y observe el número de tramas que sobrepasaron el umbral para la estadística *Pre-filter Frames*. Deshabilite el T*rigger* anteriormente creado y restaure su valor con el número 700.

13. Seleccione la pestaña *TCP/IP Vitals* y active las casillas en la columna *Stop-on* correspondientes a las estadísticas *IP Broadcast, IP Utlization* y *ARP Packets*. Cambie los valores bajo la columna *Threshold* para las dos últimas estadísticas a 5 y 35 respectivamente. Presione *OK* y corra la medida.

14. Cuando se supere el límite, responda afirmativamente a la caja de diálogo, expanda el árbol *IP Utilization* y observe el valor actual de las tres estadísticas anteriores. Deshabilite los *Triggers* y restaure sus valores originales: 20 (IP Utilization) y 10 (ARP Packets).

15. Abra la medida *Analizador Experto* y luego su ventana de *configuración*, seleccione la pestaña *TCP/IP* y habilite las casillas *Stop-on* correspondientes a los eventos *IP: Low Time to Live*, *IP: Duplicate Address*, *TCP: Reset Connection* y *RIP: Router Change*. Presione *OK* y corra la medida.

P 4.10. Identifique la causa de detención y presione *OK* a la caja de diálogo que aparece. Deshabilite los anteriores *Triggers.*

C. Porcentaje de utilización por protocolos.

16. Cierre todas las medidas y especifique los parámetros de la ventana de configuración principal para realizar un *monitoreo autonegociado* durante 5 minutos. Mediante el menú *File/Open Measurement* abra la carpeta C:\Advisor\Lan\Measure, seleccione *Protocol Stats Stk.msx* y presione *Open*, posteriormente realice el mismo procedimiento con las medidas *Protocol Stats IP.msx* y *Protocol Vitals.msx*. Corra las medidas.

P 4.11. Finalizada la captura utilice la medida *Protocol Stats Stk* y determine el porcentaje de tramas y de bytes con respecto al total de ellas para cada stack de protocolos. De forma similar determine el porcentaje de utilización de los protocolos IP utilizando *Protocol Stats IP*. Finalmente desde la ventana *Estadísticas Vitales de Protocolo* determine la utilización promedio del medio para los stacks y llene la siguiente tabla.

Tabla 2.12. Tendencias de protocolos.

STACK DE PROTOCOLOS / PROTOCOLO	TRAMAS (%)	BYTES (%)	Utilización Promedio del medio(%)
IP			
Proxy Nexus 3128			
WWW – HTTP 80			
NetBIOS 137 – 139			
Puertos de Usuario TCP/UDP (> 1000)			
FTP 20, 21			
Telnet 23			
SMTP 25			
POP3 110			
DNS 53			
ICMP 1			
ARP / RARP			
SNMP 161,162			
Puerto TCP/UDP 554			
HTTP sobre TLS/SSL 443			
TCP/UDP Port 22			
Novell			
NetBEUI			
Otros			

De acuerdo con los valores obtenidos.

P 4.12. ¿La utilización de los diferentes stacks de protocolos concuerda con los resultados esperados?

P 4.13. ¿Cómo es la utilización de los protocolos IP?. Concuerdan con los servicios prestados en la red de la Universidad del Cauca.

P 4.14. ¿Por qué NETBIOS 137 – 139 es uno de los más utilizados?

P 4.15. ¿Cuál es la funcionalidad de Proxy Nexus 3128, POP3 110, AUTH, RIP UDP-520 y BOOTP 67-68 ?

P 4.16. ¿Para que se utiliza el Puerto TCP/UDP 554?

17. Seleccione la ventana *Protocol Stats Stk* y en el menú *View* seleccione *Display Frame Leghts*.

P 4.17. Llene la siguiente tabla:

Tabla 2.13. Estadística de los tamaños de tramas Ethernet.

Longitud de Tramas	< 64	64 - 127	128 – 255	256 - 511	512 -1023	1024 - 1518	>1518
Porcentaje							

- **CONCLUSIONES**

2.1.5. Práctica No 5. Generación de Tráfico Real mediante el HP J2300D

- **OBJETIVOS:**

- Emplear el conjunto de funcionalidades que presentan las herramientas *Traffic Generator* y *Edit and PlayBack*.
- Generar tráfico real a partir de tramas definidas por el estudiante con el propósito de colocar una carga predecible sobre la red.

- **MARCO TEÓRICO**

TRAFFIC GENERATOR: Esta prueba activa se utiliza para probar los límites de una red mediante la *transmisión de tramas de longitud y contenido variables* a través de una ejecución controlada. De esta manera se puede observar el comportamiento de la red cuando se desea introducir un nuevo dispositivo o conocer la conducta de la misma ante determinado volumen y tipo de tráfico brindándole al administrador un criterio para la toma de decisiones seguras y racionales al momento de modernizar la red o ejecutar pruebas que midan el desempeño de la misma.

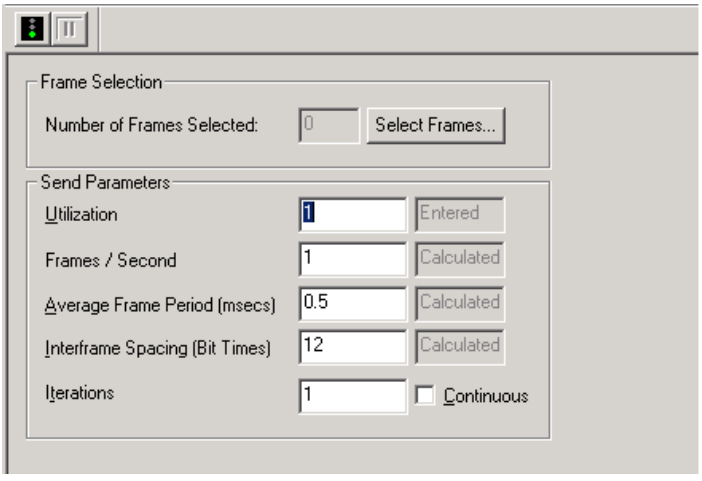


Figura 2.32. Prueba Activa Generador de Tráfico y sus correspondientes campos.

Las opciones que presenta esta herramienta son:

- *Select Frames:* Esta caja de diálogo permite crear, editar, seleccionar y configurar tramas para la generación de tráfico. Una vez se ha escogido esta opción se presenta una ventana de la siguiente forma:

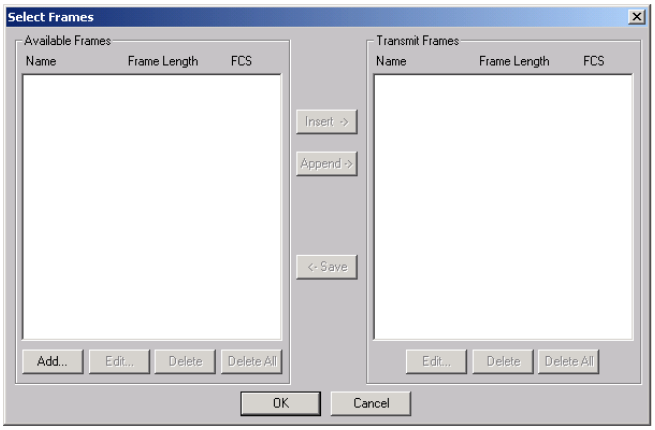


Figura 2.33. Ventana Seleccionar Tramas.

Hay dos listas de secciones denominadas *Available Frames* y *Transmit Frames* con diversos botones entre ellas. La primera muestra todas las tramas que pueden ser adicionadas, permite crear y/o editar tramas y luego moverlas a la segunda sección en el orden deseado. *Transmit Frames* despliega las tramas que efectivamente serán enviadas mostrando sus nombres, longitudes y FCS's.

El Botón *Insert* coloca la trama disponible seleccionada al *principio* de la lista *Transmit Frames*, *Append* ejecuta una operación similar sólo que coloca la trama al *final* y *Save* mueve la trama a transmitir seleccionada a la sección *Available Frames* permitiéndole ser utilizada en otros bloques.

- *Utilization:* Es el porcentaje de ancho de banda disponible el cual será utilizado.
- *Frames/Second:* Esta caja de texto define el rendimiento en términos de tramas por segundo. Este valor es promediado cuando las tramas en el bloque son de diversas longitudes. Si se decrementa este valor, se disminuye la utilización.
- *Average Frame Period (msecs):* Define el tiempo en milisegundos que será insertado entre el comienzo de una trama y el inicio de la siguiente durante la transmisión. Incrementando el retardo disminuye la utilización. Para generación de tráfico FDDI, las tramas dentro del

bloque son transmitidas secuencialmente y el *interframe spacing* ocurre después del bloque de tramas.

- *Interframe Spacing (Bit Times):* Constituye el tiempo, en tiempo de bit, entre el final de una trama y el comienzo de la siguiente. Disminuyendo este valor se incrementa la utilización.
- *Iterations:* Especifica el número de veces que se transmite el conjunto de tramas seleccionadas.

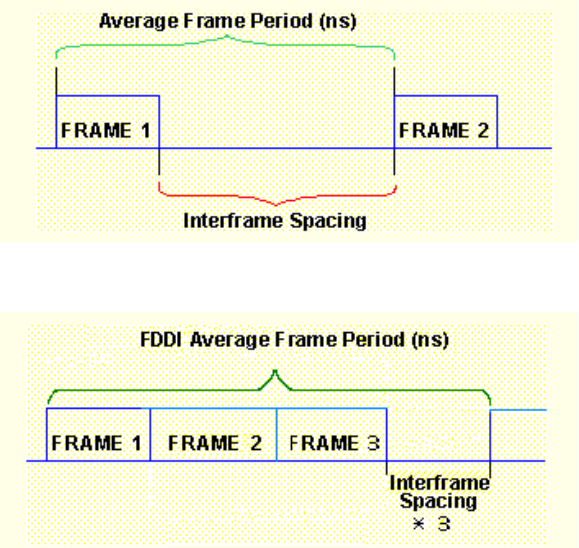


Figura 2.34. Periodo de Trama Promedio y espaciamiento entre tramas para tráfico Ethernet y FDDI.

NOTA: Estos parámetros de envío despliegan diferentes maneras de mostrar la misma información. Cuando se introduce un valor en cualquiera de los campos a excepción del etiquetado con *Iterations*, los valores para los otros son recalculados y desplegados automáticamente. Además, existe un área al lado derecho de cada campo que indica si el parámetro fue introducido o calculado.

EDIT FRAME: Como su nombre lo indica permite editar tramas en el buffer de captura para ser transmitidas sobre la red. Cuando se presiona este botón aparece una ventana muy similar a la de edición de tramas de la prueba activa *Traffic Generator* sólo que se presentan dos nuevos campos: *Frame Number* y *Delta Time*.

Posee los siguientes campos:

- *Frame Number:* Indica el número de la trama en el *Decodificador* a ser editada.
- *Data Length:* Muestra el tamaño actual de la trama a editar menos cuatro bytes correspondientes al campo FCS, debido a que esta ventana no lo tiene en cuenta. El rango de variación de este campo es de 16 a 3996 bytes, sin embargo si se fija a un valor por debajo de *64* bytes o mayor a *1518* bytes, un error se ilustra en el área detallada de la trama que está siendo editada.

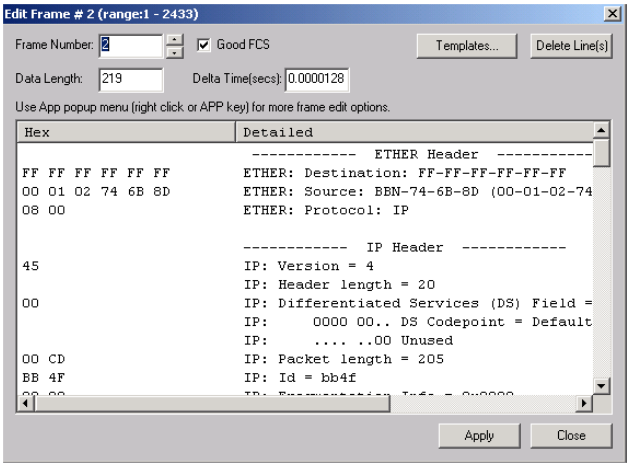


Figura 2.35. Ventana Editar Trama.

- *Delta Time:* Permite ajustar el tiempo de trama relativo a la primera de ellas en el buffer de captura. Por consiguiente, para esta última no tiene relevancia este concepto.
- *Good FCS:* Determina si la trama a enviar debe poseer un CRC bueno o malo.
- *Templates:* Abre una ventana que permite seleccionar de una lista un tipo de encapsulación.
- *Delete Line(s):* Elimina una línea de datos previamente seleccionada o un conjunto de ellas si es requerido.

PLAYBACK: Proporciona la configuración del modo, temporización y retardos para el envío de las tramas sobre la red. Tiene las siguientes opciones:

- *Entire Buffer:* Transmite el buffer de captura en su totalidad.
- *Frames:* Envía un rango de tramas definidas por el usuario.
- *Filtered Frames:* Transmite aquellas tramas que concuerden con un filtro de despliegue previamente definido.

- *Mode:* Esta opción permite repetir la(s) trama(s) de forma continua o un número determinado de veces (Desde 1 hasta 65535).
- *Delay between Replays:* Constituye el retardo entre transmisiones sucesivas del buffer de captura.
- *Use Minimun Delay:* Transmite el buffer de captura tan pronto como sea posible de acuerdo al tipo de interfaz seleccionada.
- *Use Delay of:* Una vez se ha enviado el buffer, se espera entre un 1 milisegundo y 999 segundos para transmitirlo de nuevo.
- *Use Buffer Timing:* Utiliza el mismo espaciamiento de trama de los datos capturados en el buffer.
- *Multiply Interframe Delay by:* Incrementa el tiempo entre tramas y su rango va desde 2 hasta 65535.
- *Divide Interframe Delay by:* Decrementa el tiempo entre tramas y su rango va desde 2 hasta 65535.
- *Fixed Interframe Delay:* Permite escoger entre 0.001 y 100000 microsegundos para obtener el mismo tiempo entre el envío de cada trama.
- *% Utilization:* Es la medida de la cantidad de tiempo que la red es utilizada para la transmisión de datos, es decir, indica que *porcentaje del ancho de banda* se está empleando.
- *Start Replay:* Inicia la transmisión de las tramas editadas.

PROGRAMA ETHERNET SW EDITION (PREVIOUS CARD): Es un software *Analizador de Protocolos* robusto diseñado para ayudar a encontrar fallas y analizar el comportamiento de redes Ethernet y Fast Ethernet. Este software se puede utilizar en un computador personal equipado con una tarjeta de interfaz de red (NIC) o una tarjeta PCMCIA sin tener el hardware de adquisición de datos LAN. El Ethernet *SW Edition* se puede usar para:

- Prevenir problemas de red antes que afecten a los usuarios.
- Resolver problemas de red rápida y efectivamente.
- Optimizar el desempeño de la red.
- Observar de forma rápida la vitalidad, utilización y actividad a nivel de protocolos sobre la red.
- Examinar el nivel físico para observar si los nodos sobre la red pueden conectarse y comunicarse.
- Identificar quienes están enviando la mayoría de tráfico y que protocolos están utilizando.

- Determinar cuales estaciones se encuentran estableciendo conexiones.
- Encontrar los errores de protocolo ocurriendo sobre la red.
- Descubrir nodos sobre la red.

Este programa posee las mismas características que el software Fast Ethernet Undercradle del Internet Advisor para análisis LAN. Además posee la herramienta *Switch Advisor* que permite buscar y monitorear remotamente cualquier dispositivo que soporte SNMP (Simple Network Management Protocol) -incluyendo switches - para observar la actividad en la red, permitiendo el acceso a la *MIB* (Management Information Base) e información *RMON* (Remote Monitoring). Permite acceder remotamente y desplegar datos desde cualquier conexión LAN en una red de datos. Además se puede recolectar información SNMP desde cualquier dispositivo que esté experimentando un problema mientras él se encuentra suministrando datos a la red LAN, WAN o ATM.

Los inconvenientes del *Software Edition* son:

- Se debe adquirir la licencia del producto para que funcione de forma permanente de lo contrario funciona sólo por 45 días.
- Para trabajar en **Modo Monitor** se requieren *dos tarjetas* de red en el computador donde se instala el paquete.

- **EQUIPO UTILIZADO**
  - Internet Advisor WAN HP J2300D.
  - Cable de conexión RJ-45 100Base-TX.
  - Computador con punto de red (Puerto de un Hub).
  - Punto de red (Para el Internet Advisor).

- **PROCEDIMIENTO**

A. Creación, edición y transmisión de una trama utilizando la opción software Generador de Tráfico del programa Software Edition.

1. En el computador de trabajo (PC A) instale el programa *Ethernet Software Edition* (SWEdition12.exe) el cual se encuentra en el *CD anexo a la Monografía* y consulte la MAC de la máquina.

2. Ejecute el programa *Ethernet SW Edition* y escoja la opción *Ethernet SW Edition (previous card).*

3. Seleccione la prueba activa *Traffic Generator*. Escoja la opción *Select Frames* (Figura 2.33), seleccione todas las tramas que aparezcan en la sección *Transmit Frames* (Si las hay), elimínelas y luego presione el botón *Add*. En la ventana *Edit Frame* seleccione *Templates* y escoja *Ethernet ARP Request.* Presione *OK.*

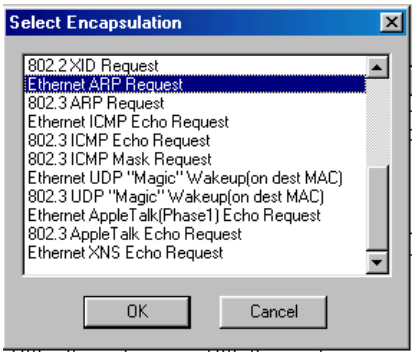


Figura 2.36. Selección del tipo de encapsulación a utilizar.

4. En la ventana *Edit Frame* modifique los siguientes campos realizando *doble click* sobre sus valores en hexadecimal:

   ETHER: Source: Dirección MAC del PC A (Debe estar en red).
   ARP: Source protocol address = Dirección IP del PC A en hexadecimal (Haga la conversión).
   ARP: Target protocol address = Dirección IP del Advisor. AC 10 29 82 (172.16.41.130).

5. En el campo *Frame Name* escriba *ARP Request* y presione *OK*. En la ventana *Select Frames* presione el botón *Insert* y luego *OK*. Introduzca en los campos *Utilization* e *Iterations* los valores de 5 y 100 respectivamente, es necesario realizar un click en cualquiera de los cuatro campos restantes con el fin de *actualizar* el valor de dichos campos de acuerdo al introducido en *Utilization*.

6. Encienda el Internet Advisor, entre al software LAN Fast Ethernet Undercradle, realice una conexión en **Modo Nodo** y especifique los parámetros de la ventana de configuración principal para realizar un *monitoreo autonegociado* y en *modo continuo*. Mantenga el tamaño del buffer de captura a 26 Mb.

7. Cree un *filtro de captura para estación fuente* que almacene las tramas que concuerden con la dirección MAC del PC A. Active el filtro, el *Decodificador* e inicie la captura de tráfico.

8. Transmita las *100 tramas ARP Request* a la red desde el programa *Sofware Edition*, escriba el password "advisor" y verifique que el Internet Advisor captura efectivamente las 100 tramas deteniendo la medida.

9. Escoja de nuevo *Select Frames* en el programa *Sofware Edition*, señale la trama *ARP Request* en la ventana *Available Frames* y realice una copia de la misma, *edítela*, *deshabilite* la casilla *Good FCS* y *presione OK*. Inserte esta última trama en la ventana *Transmit Frames* y haga efectivo los cambios.

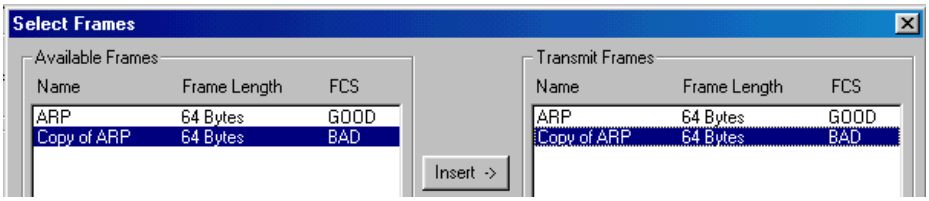


Figura 2.37. Transmisión de tramas ARP Request con FCS bueno y erróneo.

10. En el campo *Iterations* introduzca el valor de 1 y transmita este par de tramas a la red asegurándose primero de activar de nuevo el *Decodificador* en el Internet Advisor.

P 5.1. Detenga el *Decodificador* una vez se haya terminado el envío de las tramas. Compare estas tramas a nivel de FCS. ¿Nota alguna diferencia?, ¿Qué cree que sucedió?

11. Edite la trama *ARP Request* en la ventana *Transmit Frames* haciendo los siguientes cambios:
    ETHER: Destination: Dirección MAC de otro computador de la sala que se encuentre activo y en red (PC B). Por ejemplo ryst3 (00 - B0 - D0 - C2 - B1 - 1F)
    ARP: Target protocol address = Dirección IP del PC B en hexadecimal. Presione *OK*.

12. En el Internet Advisor edite el filtro de captura para estación fuente y cambie los siguientes campos:

    Source <any Stn> = Dirección MAC del PC B.
    Dest <any Stn> = Dirección MAC del PC A en el campo *User Specified*.

Active el filtro, el *Decodificador* y corra esta medida.

13. Elimine la *copia* de la trama *ARP Request* de la ventana *Transmit Frames.* Envíe *100* tramas ARP desde el *Software Edition.* Observe el formato de trama *ARP Reply* recibido en el *Decodificador* del Advisor.

P 5.2. Edite la trama *ARP Request* y envíe *una de ellas* al equipo 172.16.255.190 (olimpo.ucauca.edu.co) cuya MAC es 00-00-0C-75-C5-D2. Modifique el filtro anterior para capturar la petición y la respuesta ARP. Analice el resultado de las *dos tramas* capturadas.

B. Generar tráfico en un segmento de red utilizando la prueba activa Generador de Tráfico del Internet Advisor.

14. En el *Ethernet SW Edition* seleccione la medida *Estadísticas Vitales de Protocolo*, abra su *ventana de configuración* y *deshabilite* todos los *stacks de protocolos* con excepción de *Ethernet Vitals*. Presione *Aceptar*. En la ventana de *configuración principal* cambie el *tipo de monitoreo* a *Timed* con una duración de 1 minuto (Mínimo posible).

15. En el Advisor abra el siguiente archivo: C:\ Advisor\Lan\Data\Archivos de practicas\LabTelematica1.dat. Abra el *Generador de Tráfico*, suprima todas las tramas que aparecen en la ventana *Select Frames* y escoja una trama *Ethernet IP FTP*. Presione *OK*.

16. Edite los siguientes campos en la ventana *Edit Frame*:

    ETHER: Destination: MAC de otro computador activo en la sala. Por ejemplo ryst 1 (00 - B0 - D0 - C2 - B7 - 00).
    ETHER: Source: 00 - 10 - 4B - CC - EF - A3 (MAC del computador cuya IP es 172.16.40.101 - PC que el Internet Advisor suplantará).
    IP: Source address: AC 10 28 65 (172.16.40.101).
    IP: Destination address: AC 10 29 65 (172.16.41.101).
    En la caja de texto *Frame Name* escriba Trama FTP y en *Data Lenght* introduzca el número 100. Presione el botón *Append* y luego *OK*.

NOTA: En el siguiente punto se va a copiar el *formato de una trama* de cualquier protocolo perteneciente al stack TCP/IP, capturada previamente por el Internet Advisor. En este caso se escogerá la trama No 1 del archivo.

17. En el Internet Advisor abra el *Decodificador*, seleccione el *Frame No 1*, presione el botón *Edit Frame*. Despliegue las *opciones del botón derecho del mouse* sobre el área de texto de la ventana, escoja *Select All* y luego *Copy*. Cierre la ventana, presione el botón *Select Frames*, luego *Add* que abre la ventana *Edit Frame* del *Generador de Tráfico*, despliegue las *opciones del botón derecho del mouse* sobre el área de texto, escoja *Select All* y luego *Paste*. En el campo *Frame Name* introduzca el nombre "Trama TCP" y presione *OK*. *Inserte* la trama en la sección *Transmit Frames* mediante el botón *Append* y luego presione *OK*.

18. Repita el paso anterior para las tramas número 2 (*HTTP*), 12 (*UDP*), 48 (*ICMP*) y 632 (*DNS*).

19. *Edite* cada una de las últimas cinco tramas en la ventana *Transmit Frames* y cambie la *dirección destino* (MAC e IP) en **donde sea necesario** con la de equipos pertenecientes a la sala en la cual se está realizando la práctica con el propósito de cargar el segmento de red al cual está conectado el Internet Advisor (No utilizar como destino el PC A). Verifique que la longitud de las tramas en el campo *Data Lenght* de la ventana *Edit Frame* que tiene el *Advisor* se encuentre en el rango 60 – 1514.

Tabla 2.14. Equipos Laboratorio de Telemática del Departamento de Telecomunicaciones.

Nombre	MAC	IP	IP en Hex
Ryst1	00 - B0 - D0 - C2 - B7 - 00	172.16.41.101	AC 10 29 65
Ryst2	00 - B0 - D0 - C2 - 94 - 7F	172.16.41.102	AC 10 29 66
Ryst3	00 - B0 - D0 - C2 - B1 - 1F	172.16.41.103	AC 10 29 67
Ryst4	00 - B0 - D0 - C2 - B7 - 3E	172.16.41.104	AC 10 29 68
Ryst5	00 - B0 - D0 - D9 - 9D - D7	172.16.41.105	AC 10 29 69
Ryst6	00 - B0 - D0 - D9 - 9D - DA	172.16.41.106	AC 10 29 6ª
Ryst7	00 - B0 - D0 - C2 - 93 - A6	172.16.41.107	AC 10 29 6B
Ryst8	00 - B0 - D0 - C2 - D7 - 76	172.16.41.108	AC 10 29 6C
Ryst9	00 - B0 - D0 - D9 - 9D - ED	172.16.41.109	AC 10 29 6D
Ryst11	00 - B0 - D0 - D9 - 9D - EF	172.16.41.111	AC 10 29 6F
Ryst12	00 - B0 - D0 - C2 - B1 - 1B	172.16.41.112	AC 10 29 70

Ryst13	00 - B0 - D0 - D9 - 98 - 7C	172.16.41.113	AC 10 29 71
Ryst15	00 - B0 - D0 - C2 - 93 - 4A	172.16.41.115	AC 10 29 73
Ryst16	00 - B0 - D0 - C2 - D0 - 49	172.16.41.116	AC 10 29 74

20. En el *Software Edition*, vaya a la medida *Estadísticas Vitales de Protocolo* y expanda el árbol *Pre – Filter Ethernet Utilization.*

21. En el Internet Advisor, varíe el parámetro de envío *Utilization* del *Generador de Tráfico* de *1% a 15%* y transmita las tramas de *forma continua*, activando primero el *Generador de Tráfico* y luego el *Software Edition*.

NOTA: Debido a la ausencia de un hardware especializado para capturar y transmitir tráfico en el PC es posible que el programa *Ethernet Software Edition* se bloquee.

P 5.3. Tome muestras cada minuto con el *Ethernet SW Edition* y llene la siguiente tabla.

Tabla 2.15. Grado de utilización del BW de un segmento de red con carga.

Utilization Traffic Generator (%)	Colisiones Acumuladas	Pre–filter Frames Acumuladas	% de tramas que colisionan	Pre–filter Ethernet Utilization (Average)
1				
3				
5				
7				
9				
11				
13				
15				

* Colisiones acumuladas = locales + tardías + remotas + tardías remotas

P 5.4. Realice dos gráficas de *Ethernet Utilization (Average)* Vs *Utilization Traffic Generator* y *de % de tramas que colisionan* Vs *Utilization Traffic Generator* de acuerdo a la tabla anterior.

C. Cargar el segmento de red utilizando la herramienta playback.

22. Realice un filtro IP de captura para *estación* en el *Ethernet Software Edition* que tenga como destino la dirección IP de un computador en la sala. Utilizando la opción *Other Station Filters* adicione tres nodos destinos más siguiendo el proceso inmediatamente anterior y corra la medida. Los cuatro PCs deben estar activos en red.

23. Capture tráfico por 3 minutos con el *Ethernet Software Edition*. Abra el *Decodificador*, presione el botón *Playback* y escoja las siguientes opciones: *Frames* (1 Through 15), *Replay Continuously* y *Use Minimum Delay*. Espere hasta reconfigurar el Advisor.

24. En el Advisor *deshabilite* el filtro de captura presente, configure el *tipo de monitoreo* a *1 minuto* y abra la medida *Estadística Vitales de Protocolo.* Inicie la transmisión en el *Software Edition* y la captura de los datos en el Advisor.

P 5.5. Varié el parámetro *Utilization* de 1% a 10% en el *Software Edition* y llene la siguiente tabla:

Tabla 2.16. Variación del ancho de banda en un segmento de red empleando la herramienta Playback del Decodificador.

Utilization Traffic Generator (%)	*Colisiones Acumuladas	Pre–filter Frames Acumuladas	% de tramas que colisionan	Pre–filter Ethernet Utilization (Average)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

* Colisiones acumuladas = locales + tardías + remotas + tardías remotas

P 5.6. Realice dos gráficas de *Ethernet Utilization (Average)* Vs *Utilization Traffic Generator* y de *% de tramas que colisionan* Vs *Utilization Traffic Generator* de acuerdo a la tabla anterior.

P 5.7. Compare los resultados obtenidos al cargar el segmento de red con el *Generador de Tráfico* y con la herramienta *Playback*.

25. Seleccione la opción *Entire Buffer* en la ventana *Playback Buffer* del *Software Edition* y varíe la utilización con los mismos valores de la tabla anterior.

P 5.8. Compare los resultados obtenidos transmitiendo el buffer completo con respecto al envío de las 15 primeras tramas.

P 5.9. Realice las siguientes gráficas *manteniendo constante* el parámetro *Utilization* a *10 %*. Donde X es *No de tramas enviadas* empleando la herramienta *Playback* del *Software Edition*, Y es el *porcentaje de Utilización Promedio* medido en *Estadísticas Vitales de Protocolo* en el Internet Advisor. X' es *No de tramas enviadas* empleando la herramienta *Playback* del *Internet Advisor* y Y' es el *porcentaje de Utilización Promedio* medido en *Estadísticas Vitales de Protocolo* en el *Software Edition*.

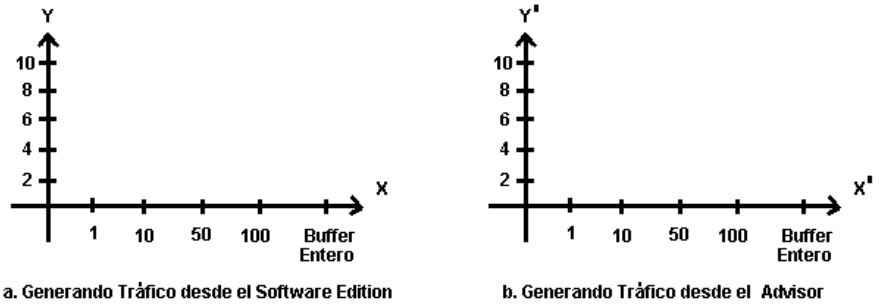


Figura 2.38. Empleo de la herramienta Playback con utilización constante del 10 %.

P 5.10. Realice las siguientes gráficas *manteniendo constante* el número de tramas capturadas a enviar (*Frames: 1 Throught 500).* Donde X es el valor del parámetro *Divide Interframe Delay* de la herramienta Playback en el Software Edtion y Y es el *porcentaje de Utilización Promedio* medido en *Estadísticas Vitales de Protocolo* en el Internet Advisor. X' es el valor del parámetro *Divide Interframe Delay* de la herramienta Playback en el Internet Advisor y Y' es el *porcentaje de Utilización Promedio* medido en *Estadísticas Vitales de Protocolo* en el *Software Edition*.

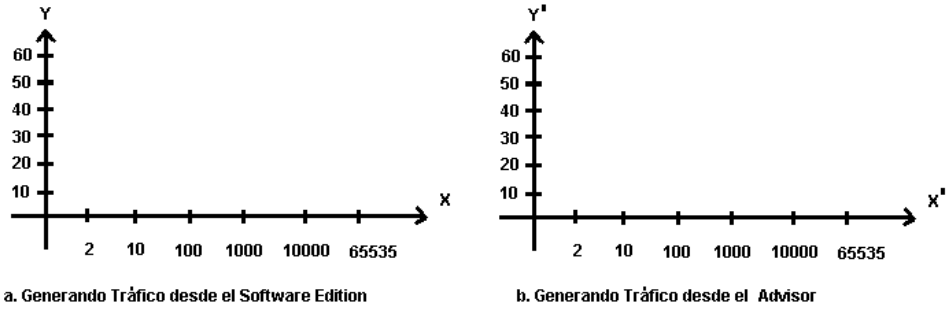


Figura 2.39. Empleo de la herramienta Playback manteniendo constante el número de tramas enviadas.

P 5.11. ¿En su concepto, a que atribuye la diferencia en las gráficas anteriores?

- **CONCLUSIONES**

2.1.6. Práctica No 6. Análisis del Estándar IEEE 802.1 Q/p y Gestión Remota de Dispositivos de Internetworking

- **OBJETIVOS:**

- Utilizar la herramienta *Estadísticas VLAN* mediante la creación y configuración de un par de VLANs empleando los Switches 3Com SuperStack 3300XM, Cisco Catalyst 2900 Series XL y el hub SuperStack II Dual Speed Hub 500 de 3 COM.
- Aplicar la herramienta *Switch Advisor* del programa *Ethernet Software Edition* para monitorear el Switch 3Com SuperStack 3300XM.

- **MARCO TEÓRICO**

SWITCH 3COM SUPERSTACK 3300XM: Tiene 24 puertos los cuales pueden ser configurados a 10BASE -T half duplex, 10BASE -T full duplex, 100 BASE –TX half duplex y 100 BASE –TX full duplex. Todos los puertos son configurados como MDIX (cross-over) y si se requiere hacer una conexión a otro puerto MDIX, se debe emplear un *cable cruzado* (croos-over).

El Switch puede ser configurado y gestionado mediante tres métodos:

- *Interfaz Web:* El Switch posee un conjunto interno de páginas Web que permiten administrarlo utilizando un browser Web.
- *Interfaz Línea de Comandos:* Se utiliza conectando un cable Null MODEM entre la estación de gestión y el puerto de consola del Switch empleando la herramienta *Hyper Terminal* o remotamente ejecutando un *Telnet* a través de uno de los 24 puertos.
- *Gestión SNMP:* Se puede administrar el Switch usando cualquier gestor de red que corra el Protocolo de Gestión de Red Simple (SNMP) como el software 3Com Trascend Enterprise Manager o Trascend Network Supervisor.

Análisis Roving: Es un sistema que permite conectar un analizador de protocolos a un puerto y utilizarlo para monitorear el tráfico de otros puertos en el switch. Permite definir un puerto de análisis (Conectado al analizador) y un puerto monitor (Puerto a ser monitoreado), así, el 3Com 3300XM toma todo el tráfico entrante y saliente del puerto monitor y lo copia al puerto de análisis.

LANs Virtuales: Una VLAN es un grupo flexible de equipos que pueden ser ubicados en cualquier lugar de una red, pero que se comunican como si estuvieran localizados en el mismo segmento físico. Una de las ventajas de este tipo de redes con respecto a las tradicionales es permitir la segmentación de la red sin restricciones por conexiones físicas. Por ejemplo la red se puede segmentar para diferentes grupos de trabajo como:

- *Grupos departamentales:* Donde exista una VLAN para el departamento de mercadeo, otra para el departamento de finanzas y otra para el departamento de producción.
- *Grupos jerárquicos:* Se puede tener una VLAN para directores, otra para gerentes y otra para el cuerpo administrativo general.
- *Grupos de usuarios:* Se puede tener una VLAN para usuarios de e-mail y otra para usuarios que cursen tráfico multimedia.

ETIQUETAMIENTO 802.1 Q/802.1 p: Este esquema de etiquetamiento adiciona 4 bytes a la trama Ethernet insertados después del campo MAC Source Address y antes del campo Ethertype (Ethernet Versión 2) o Lenght (IEEE 802.3) de acuerdo al tipo de encapsulación empleada.

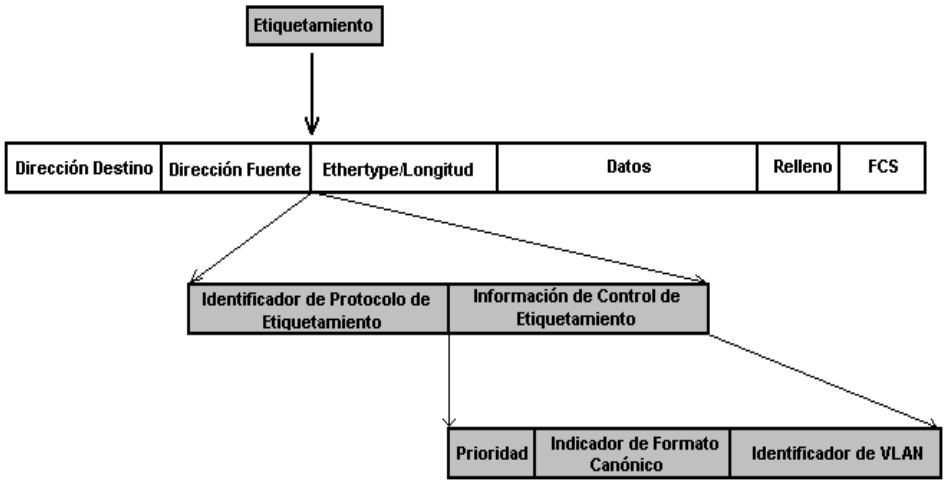


Figura 2.40. Formato de trama con etiquetamiento 802.1 Q/802.1p.

Dirección Destino: Dirección MAC Destino.

Dirección Fuente: Dirección MAC Fuente.

Identificador de Protocolo de Etiquetamiento (TPID): Posee un valor fijo de 0 x 8100, el cual indica que la trama transporta información de etiquetamiento 802.1 Q/p.

Información de Control de Etiquetamiento (TCI): Tiene los siguientes subcampos.

- *Prioridad:* Permite a la trama etiquetada transportar a través de diversas LANs información con prioridad de usuario. Puede representar hasta ocho niveles de prioridad y es empleado principalmente por el estándar IEEE 802.1 p.
- *Indicador de Formato Canónico (CFI):* Un valor de 0 indica formato canónico y un valor de 1 lo contrario.
- *Identificador de VLAN (VID):* Identifica unívocamente la VLAN a la cual pertenece la trama, puede definir hasta 4096 VLANs donde la 0 y 4095 son reservadas. Este campo es usado principalmente por el estándar IEEE 802.1 Q.

Las tramas Ethernet normales no pueden exceder los 1518 bytes, por lo tanto, si una trama de tamaño máximo tiene etiquetamiento 802.1 Q/p su tamaño se incrementará a 1522 bytes.

ARQUITECTURA DE GESTIÓN DE RED: El modelo empleado para la gestión de red incluye elementos claves como la Estación Gestora – NMS, el Agente de Gestión – NMA, la Base de Información de Gestión – MIB y el Protocolo de Gestión de Red – SNMP.

Network Management Station (NMS): Constituye la interfaz para el Administrador de la red con el sistema de red a gestionar. Se caracteriza por:

- Un grupo de aplicaciones para el análisis de datos, graficación y recuperación ante fallas.
- Una interfaz para monitorear y controlar la red.
- La capacidad para trasladar los requerimientos de los administradores de red en elementos de monitoreo y control de los dispositivos remotos.
- Una base de datos de la información extraída de las MIBs de todas las entidades de gestión de la red.

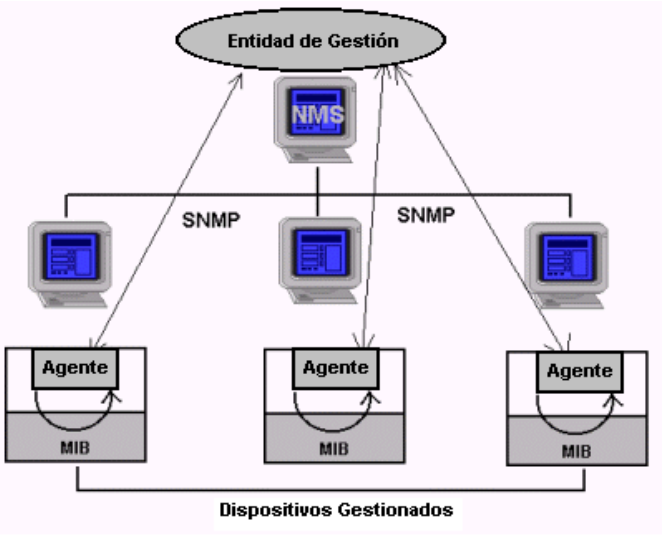


Figura 2.41. Arquitectura de Gestión de Red.

Network Management Agent (NMA): Es un módulo software de gestión de red que reside en el dispositivo gestionado, tiene conocimiento local de la información de gestión y la traduce a una forma compatible con SNMP. Los elementos de red deberán poseer alguno si van a ser gestionados y dichos agentes responden a los requerimientos de información y de acciones que efectúa una estación de gestión además de emitir información no solicitada.

Management Information Base (MIB): SNMP define un estándar separado para los datos gestionados por el protocolo. Este estándar define los datos mantenidos por un dispositivo de red, así como las operaciones que están permitidas. Los datos están estructurados en forma de árbol; en el que sólo hay un camino desde la raíz hasta cada variable. Esta estructura en árbol se llama Management Information Base (MIB) y se puede encontrar información sobre ella en varios RFC's. La versión actual de TCP/IP MIB es la 2 (MIB-II) y se encuentra definida en el RFC-1213. En ella se divide la información que un dispositivo debe mantener en *ocho categorías* donde cualquier *variable* ha de estar en una de ellas.

Tabla 2.17. Categorías MIB II.

Categoría	Información
System	Información del sistema operativo del host o router.
Interfaces	Información de las interfaces de red.
Addr-translation	Información de traducción de direcciones
Ip	Información sobre el protocolo ip.

Icmp	Información sobre el protocolo icmp.
Tcp	Información sobre el protocolo tcp.
Udp	Información sobre el protocolo udp.
Egp	Información sobre el protocolo Exterior Gateway.

Simple Network Management Protocol (SNMP): SNMP es una extensión del protocolo de gestión de red para *gateways* SGMP (*Simple Gateway Monitoring Protocol*, Protocolo Sencillo de Supervisión de Pasarelas), que se convirtió en 1.989 en el estándar recomendado por Internet. Está dirigido a proporcionar una gestión de red centralizada que permita la observación, el control y la gestión de las instalaciones. Utilizando SNMP, un administrador de red puede direccionar preguntas y comandos a los dispositivos de la red. Algunas de las funciones que proporciona SNMP son:

- Supervisión del rendimiento de la red y su estado.
- Control de los parámetros de operación.
- Obtención de informes de fallos.
- Análisis de fallos.

Las capacidades claves que incluye son:

- *Get:* Permite a la estación de gestión obtener los valores que tienen las variables en la MIB.
- *Set:* Habilita a la estación de gestión para fijar valores en las variables de la MIB.
- *Trap:* Capacita al agente para informar a la estación de gestión de eventos significativos.

- **EQUIPO UTILIZADO**
  - Internet Advisor WAN HP J2300D.
  - Cable de conexión RJ-45 100Base-TX.
  - 4 Computadores con punto de red (Puerto de un Hub).
  - Punto de red (Para el Internet Advisor).
  - Switch 3Com SuperStack 3300 XM (24 puertos).
  - Switch Cisco Catalyst 2900 Series XL (24 puertos).
  - Hub 3 COM SuperStack II Dual Speed Hub 500 (12 puertos).
  - 4 cables directos y 3 cables cruzados con conectores RJ-45.
  - Un cable Null MODEM estándar tipo DB9.

- **PROCEDIMIENTO**

A. Creación, configuración y análisis de tráfico VLAN.

1. Encienda los cuatro PCs y verifique por entorno de red que cada uno de ellos posee una carpeta compartida. De lo contrario entre con permisos de administrador y realice esta operación.

2. Encienda el Switch 3300 XM y conéctelo a uno de los cuatro computadores asignados para esta práctica (PC A) empleando el cable Null MODEM estándar.

3. En el PC A ejecute la aplicación de comunicaciones *Hyper Terminal* y configure los parámetros necesarios para entrar a la interfaz de línea de comandos del switch.

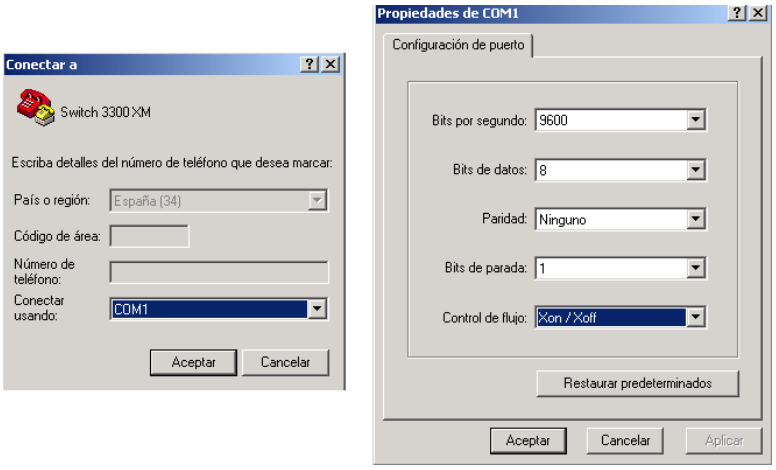


Figura 2.42. Establecimiento de la conexión con el switch 3300 XM utilizando Hyper Terminal.

4. Espere algunos segundos e introduzca la palabra *"security"* como *login* y como *password*.

5. Configure la dirección IP del switch así: A continuación del mensaje *"Select menu option:"* escriba la palabra *ip* y presione *enter*. Luego digite la palabra *interface*, presione *enter* y posteriormente la palabra *define*. En seguida de *Enter ipAddress [x.x.x.x]* introduzca una dirección IP disponible para el segmento de red donde está conectado el switch por ejemplo 172.16.41.131. Presione *enter* sucesivamente hasta llegar al menú del comando *define*. Luego presione *"q"* hasta llegar a *Menu options:-------- 3Com SuperStack 3 Switch 3300XM--------* y digite *logout* para cerrar la sesión con el switch. Cierre el programa *Hyper Terminal*.

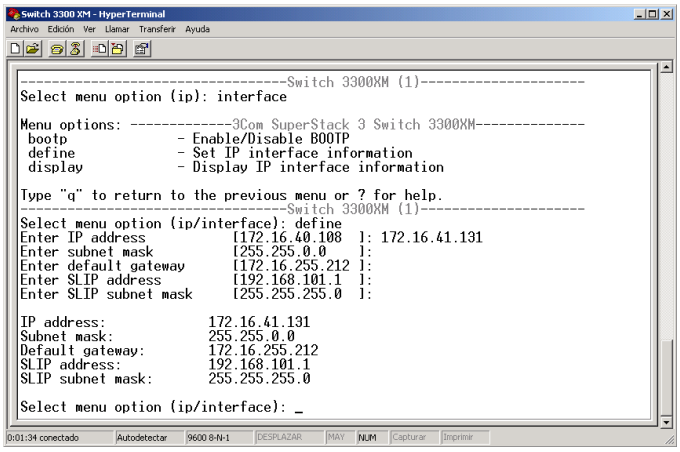


Figura 2.43. Configuración de la dirección IP del switch 3300 XM.

6. Conecte el *puerto No 10* del switch a un punto de red libre utilizando un *cable cruzado*. Ejecute el *browser Internet Explorer* en el PC A y en el campo de localización introduzca la dirección IP del switch. Usar el mismo *login* y *password* anteriormente empleado.

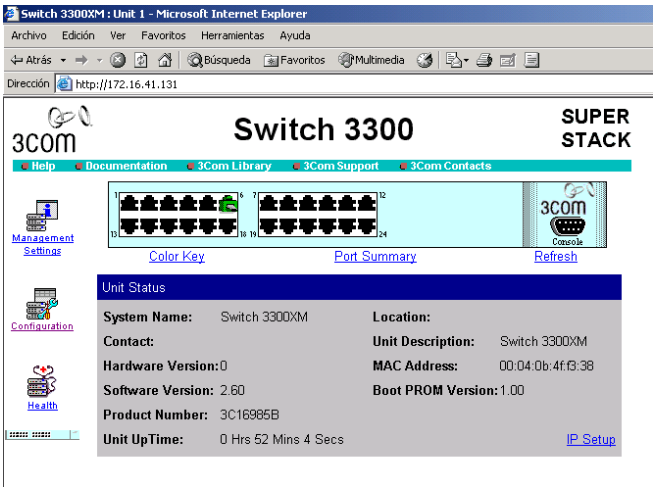


Figura 2.44. Interfaz Web Principal del switch 3300 XM.

7. Haga un click sobre el ícono *Configuration* y luego sobre el hipervínculo *Initialize*. Seleccione la casilla *Yes* de la ventana *Initialization* y luego presione *Apply*. Mediante esta acción se inicializa el switch a sus valores por defecto manteniendo constante la configuración IP anteriormente realizada.

8. Haga click sobre el ícono *Configuration* y luego sobre el hipervínculo *VLANs*.

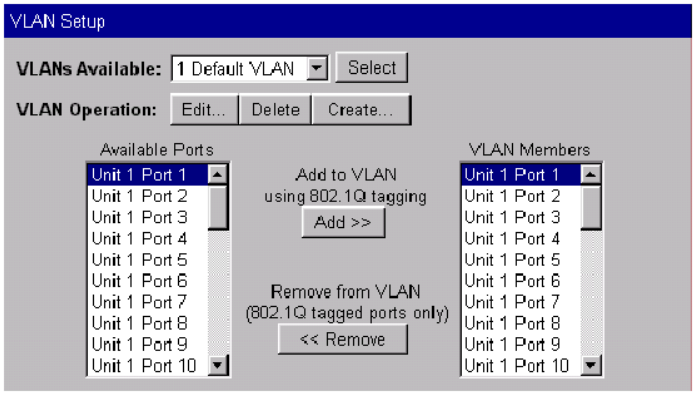


Figura 2.45. Página de configuración VLAN del switch 3300 XM.

Por defecto todos los puertos del switch pertenecen a la *VLAN 1* (Default VLAN).

9. Presione el botón *Create* y realice la siguiente configuración: en *VLAN Name* introduzca el nombre *"Ingenierías",* en *802.1Q VLAN ID* digite el *número 2* y para *Local ID* escoja el número *2.* Haga efectiva esta configuración y repita el anterior procedimiento creando la *VLAN " Servidores"* con un identificador *VLAN* y *Local* igual a *3*.

10. Para reconfirmar los valores de configuración por defecto haga un click sobre el ícono *Unit* (Dibujo ubicado debajo del ícono *Health*) y presione el botón *Apply* sucesivamente hasta terminar. Seleccione el puerto número 1 sobre la gráfica del switch.

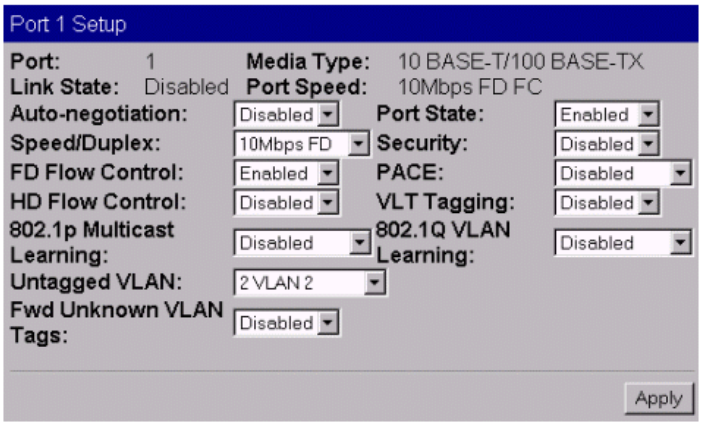


Figura 2.46. Página de configuración del puerto No 1 para el switch 3300 XM.

Escoja las opciones para los siguientes campos:

- *Auto-negotiation:* Enabled
- *Speed/Duplex:* Auto
- *FD Flow Control:* Auto
- *HD Flow Control:* Enabled
- *802.1p Multicast Learning:* Disabled
- ***Untagged VLAN:*** **2 Ingenierías** (Se adiciona el Puerto No 1 a la VLAN Ingenierías)
- *Fwd Unknown VLAN Tags:* Disabled
- *Port state:* Enabled
- *Security:* Disabled
- *PACE:* Disabled
- *VLT Tagging:* Disabled
- *802.1Q VLAN Learning:* Disabled. Por último presione el botón *Apply.*

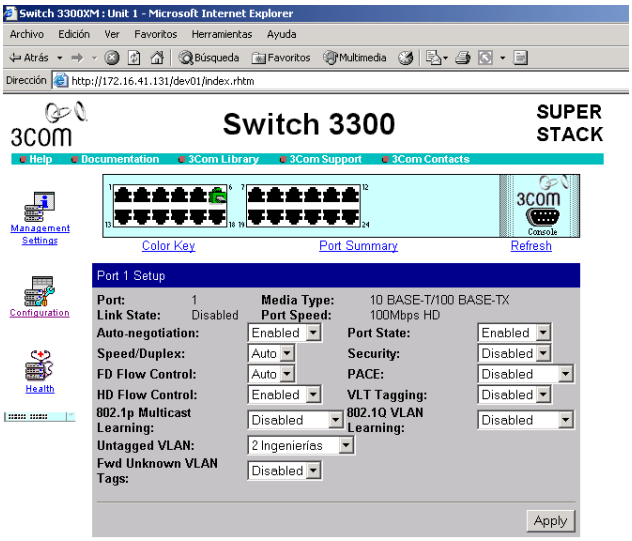


Figura 2.47. Configuración del puerto No 1 y adición a la VLAN Ingenierías.

11. Repita el anterior procedimiento para el *puerto No 7* y adiciónelo a la *VLAN Ingenierías.* De igual forma adicione los *puertos No 19 y 24* a la *VLAN Servidores* (**Sólo varía el campo Untagged VLAN**).

12. Haga un click sobre el ícono *Configuration* y posteriormente sobre el hipervínculo *VLANs*. Escoja de la caja de lista *VLANs Available:* la opción *2 Ingenierías* y presione el botón *Select*. En la sección *Available Ports* seleccione **Unit 1 Port 12** y presione el botón *Add>>* para adicionar ese puerto a la VLAN Ingenierías (VLAN 2) y **soportar** además **etiquetamiento 802.1 Q**.

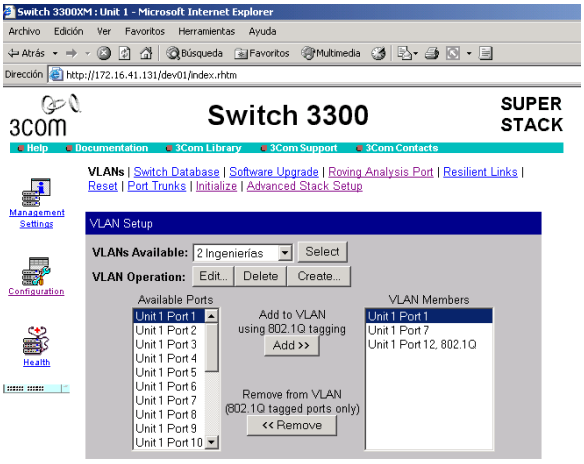


Figura 2.48. Adición puerto No 12 a la VLAN Ingenierías utilizando etiquetamiento 802.1 Q.

13. Adicione el puerto número *12* a la *VLAN Servidores (VLAN 3)* de **igual forma** que en el anterior paso.

14. Cierre el Internet Explorer, conecte dos computadores (PC B y PC C) desde sus tarjetas de red a los puertos del switch *No 1 y 24* empleando un par *cables directos*. Verifique que el PC A tenga instalado el *jsdk (Java)* o de lo contrario proceda a instalarlo descargándolo desde ftp de la Universidad del Cauca: Aplicaciones/Windows/Desarrollo/Java/j2sdk-1_e_1_01-windows-1586.exe.

15. Encienda el Switch Cisco Catalyst 2900 Series XL de 24 puertos, desconecte el *cable cruzado* del puerto No *10* del *switch 3300 XM* y conéctelo a uno de los puertos del Catalyst 2900, por ejemplo, el puerto No 10 (Por defecto todos los puertos pertenecen a la VLAN 1 o Default VLAN).

16. Ejecute el *Internet Explorer* en el PC A y en el campo de localización introduzca la dirección **IP asignada al switch**, por ejemplo, *172.16.41.130*. Introduzca la palabra *"cisco"* como *login* y como *password*.

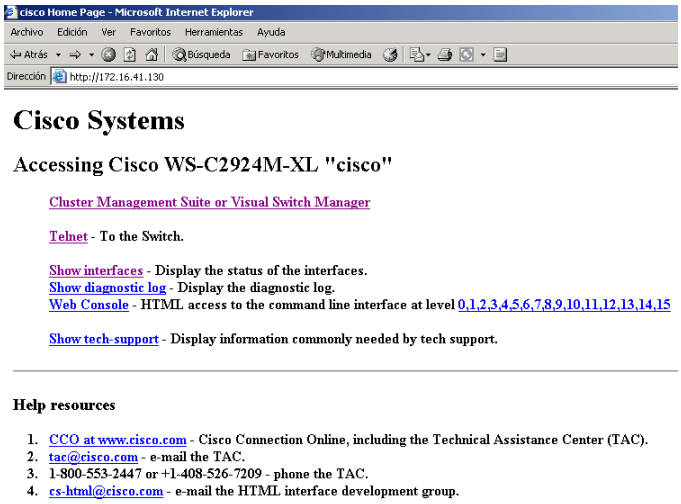


Figura 2.49. Interfaz Web Principal switch Catalyst 2900 Series XL.

17. Haga click sobre el hipervínculo *Cluster Management Suite (CMS) or Visual Switch Manager*. Esta interfaz de usuario gráfica permite configurar y monitorear un switch individual, un miembro de un cluster o un cluster entero (Utilice el mismo *login* y *password* anteriormente empleado).

18. Presione el *botón Launch Cluster Manager* en la barra de herramientas de la interfaz CMS y luego *Aceptar* en la caja de diálogo *Mensaje*.

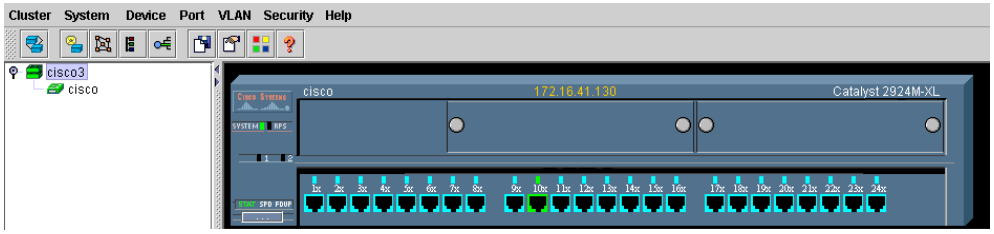


Figura 2.50. Cluster Manager para el switch Catalyst 2900 Series XL.

19. Haga click con el *botón derecho del mouse* sobre el *puerto No 1* y escoja la opción *Port Configuration....* Modifique los siguientes campos en la ventana *Port Configuration – fastEthernet 0/1*:

- *Description:* Ingenierías (VLAN 2).
- *Status*: Enable.

- *Duplex:* Auto.
- *Speed:* Auto.
- *Port Fast*: Disable.
- *802.1 p Priority:* 0.
- *Flow Control:* Ningún parámetro. Presione *OK*.

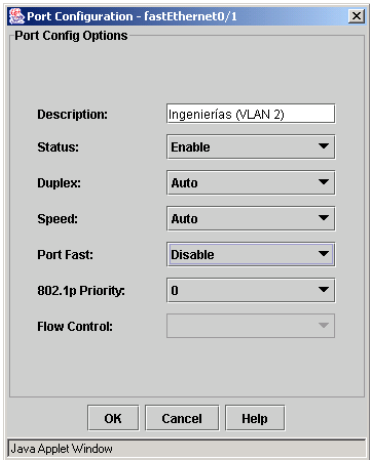


Figura 2.51. Configuración del puerto No 1 para el Catalyst 2900 Series XL.

20. Realice el anterior punto para los *puertos No 7, 12, 19* y *24* escribiendo en el campo *Description* los mensajes *Ingenierías (VLAN 2), TRONCAL DE SALIDA, Servidores (VLAN 3)* y *Servidores (VLAN 3)* respectivamente.

21. Nuevamente haga click con el *botón derecho del mouse* sobre el *puerto No 1* y seleccione la opción *VLAN Membership....* Modifique los siguientes campos en la ventana *Group VLAN Assignment:*

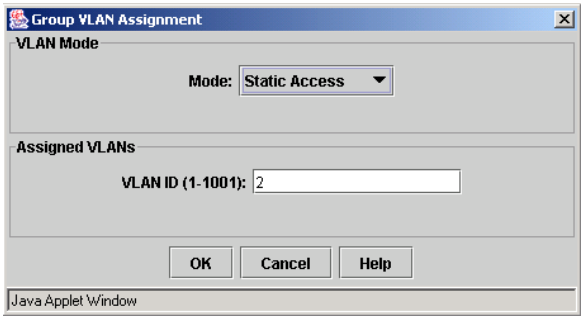


Figura 2.52. Adición del puerto No 1 del Catalyst 2900 Series XL a la VLAN Ingenierías.

- *Mode:* Static Access.
- *VLAN ID (1 -1001):* 2. Presione *OK*.

22. De igual manera adicione el *puerto No 7* a la *VLAN Ingenierías* y los *puertos No 19* y *24* a la *VLAN Servidores* escribiendo en el campo *VLAN ID (1 -1001)* el número *3*. Para el *puerto No 12* seleccione la opción **802.1 Q Trunk** del campo *Mode*.

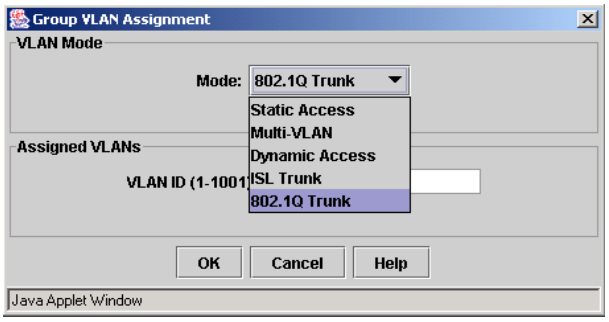


Figura 2.53. Configuración del puerto No 12 del Catalyst 2900 Series XL para soportar etiquetamiento 802.1 Q.

23. Cierre el browser y conecte los computadores restantes (PC A y PC D) desde sus tarjetas de red a los puertos No 1 y 24 del Catalyst 2900 XL empleando un par de *cables directos*. Ver Figura 2.54.

24. Encienda el Hub SuperStack II de 3 COM y realice dos conexiones utilizando el par de *cables cruzados* así: Una conexión entre el puerto No 12 del switch 3300 XM y un puerto cualquiera del hub y otra de la misma manera pero con el puerto No 12 del Catalyst 2900 XL. Conecte el Internet Advisor en **Modo Nodo** a otro puerto del Hub.

P 6.1. Intente navegar desde los cuatro equipos. Ahora cambie el cable cruzado que se encuentra en el puerto No 10 del switch Catalyst 2900 XL al puerto No 7 y al puerto no 19 e intente navegar. ¿Qué sucede en los tres casos y porqué?

P 6.2. Desconecte el cable cruzado del puerto No 19 del Catalyst y copie archivos compartidos desde los PCs posibles en ambos sentidos. ¿Qué sucede y porqué?

P 6.3. Realice las pruebas de las dos preguntas anteriores pero empleando los puertos No 7 (VLAN Ingenierías) , 10 (Default VLAN) y 19 (VLAN Servidores) en el switch 3300 XM. ¿Qué sucede y porqué?

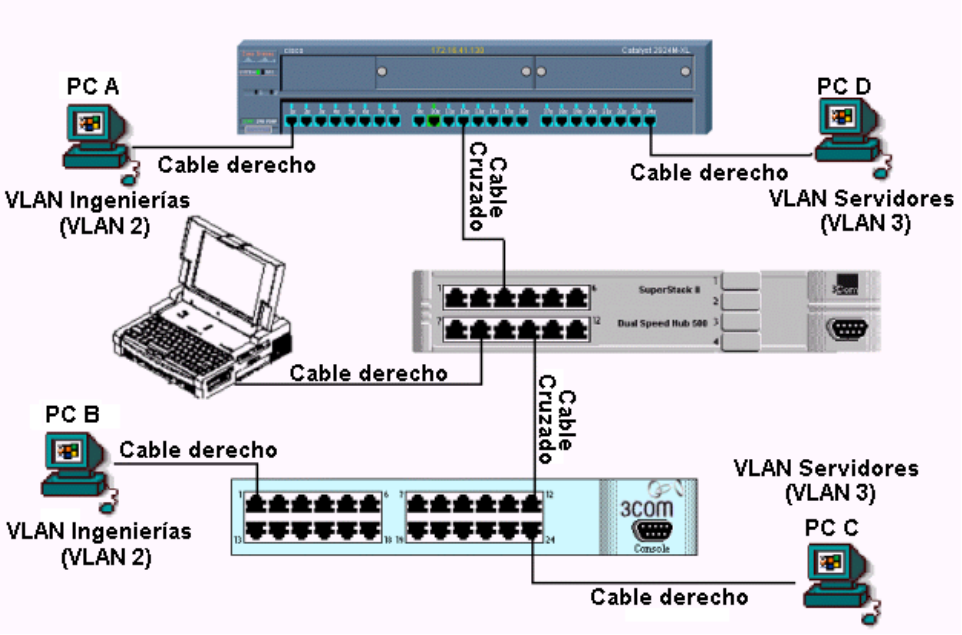


Figura 2.54. Montaje para análisis de tráfico VLAN.

25. Desconecte el cable cruzado del puerto No 19 del switch 3300 XM. En el Internet Advisor cierre todas las medidas, elimine los filtros si existen y especifique los parámetros de la ventana de configuración principal para realizar un *monitoreo autonegociado* y en *modo continuo*.

26. Abra las medidas *Estadísticas VLAN* y *Decodificador* y la medida *Protocol Stats IP.msx* mediante la opción *Open Measurement* del menú *File*. Inicie las medidas.

27. Utilizando el entorno de red copie archivos entre los computadores que pertenecen a las VLANs durante dos minutos. Detenga las medidas y responda las siguientes preguntas:

P 6.4. ¿Cuál es la utilización promedio en bits por segundo para la VLAN 2 (Ingenierías) y VLAN 3 (Servidores)?

P 6.5. ¿Por qué aparece tráfico no VLAN (Non-VLAN) y quien lo genera?

P 6.6. ¿Qué protocolos y puertos son utilizados cuando se transfieren archivos entre los PCs de una misma VLAN?

P 6.7. Para las tramas observadas en el *Decodificador*. ¿Cuáles son los datos de los campos que se adicionan a la trama Ethernet estándar cuando existe etiquetamiento 802.1 Q/p?

P 6.8. ¿Las tramas cuya longitud es mayor a 1518 octetos, son realmente errores?

B. Utilización de la herramienta Switch Advisor.

NOTA: Este software es un trial cuyo periodo de funcionamiento es de 45 días, por lo tanto, algunas funcionalidades (Sobre todo las de gestión remota) no están disponibles, por consiguiente la práctica se enfocará en aquellas que si lo estén.

28. Instale en el PC A o PC B el programa *Software Edition* cuyo instalador (SWEdition12.exe) se encuentra en el *CD anexo a la Monografía.* Conecte un cable cruzado entre el puerto No 10 del switch 3300 XM y un punto de red libre, y el PC con el *Software Edition* a su punto de red original.

29. Abra la herrramienta *Switch Advisor* desde la barra de herramientas principal en el *SW Edition*. En los campos *Ip Address* y *Range Ip Address* digite la dirección IP del switch, en el campo *Read Community* escriba *"public"* y para los campos restantes deje los valores que se visualizan. Inicie la búsqueda.

NOTA: En caso de tener incertidumbre acerca de la comunidad de lectura, verifíquela directamente en el switch desde la interfaz de comandos a través del menú snmp.

30. Seleccione la dirección IP del switch ubicada en la columna *Ip Address*, a continuación presione el botón *Open Device* y luego la medida *Switch Management* desde la barra de herramientas principal. Intercambie tráfico entre los equipos que conforman la *VLAN 3*.

P 6.9. Llene la siguiente tabla:

Tabla 2.18. Información proporcionada por Switch Management.

Puerto	Medio	Soporte RMON	Estado Operacional
1			
12			
24			

P 6.10. Presione la medida *MIB Statistics* y consigne los valores en la siguiente tabla.

Tabla 2.19. Información proporcionada por Estadísticas MIB.

Puerto	Octetos Entrantes	Octetos Salientes	Unicasts Entrantes	Unicasts Salientes	Errores Entrantes	Errores Salientes
1						
12						
24						

P 6.11. Interprete el significado de las columnas *In Discards* y *Out Discards*.

31. Con el botón derecho del mouse señale el *puerto No 24* bajo la columna *Alias Name* y seleccione la opción *Open MIB Statistics Screen* (Equivalente a presionar el botón *MIB Statistics for selected port* desde la barra de herramientas). Observe la utilización de entrada y salida del puerto No 24 de la VLAN 3 cuando se copian archivos entre sus miembros.

32. Active la medida *MIB Browser* y deshabilite las cajas de diálogo *Information, Navigation* y *Error Log*.

Se visualizan los grupos que conforman la MIB empezando con *[system]*. Dicho grupo contiene información del sistema y algunos de sus objetos son los siguientes:

- *sysDescr* - Descripción completa del sistema (versión, HW, OS).
- *sysObjectID* - Identificación que da el distribuidor al objeto.
- *sysUpTime* - Tiempo desde la última reinicialización.
- *sysContact* - Nombre de la persona que hace de contacto.
- *sysName* - Nombre del dispositivo.
- *sysLocation* - Ubicación del dispositivo.

- *sysServices* - Servicios que ofrece el dispositivo.

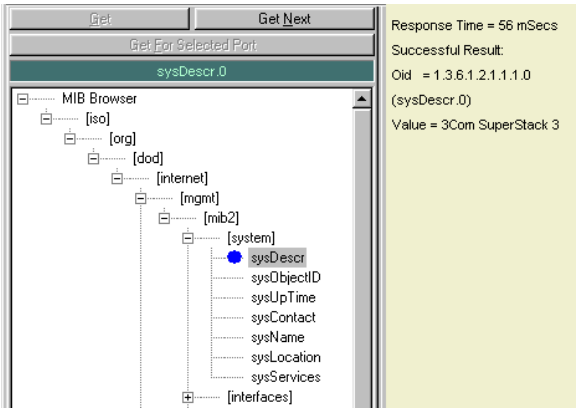


Figura 2.55. MIB Browser.

P 6.12. Obtenga los valores de los anteriores objetos empleando *Get.* Consígnelos en la siguiente tabla:

Tabla 2.20. Grupo Sistema.

Objeto	Valor
SysDescr	
SysObjectID	
SysUpTime	
SysContact	
SysName	
SysLocation	
SysServices	

P 6.13. Investigue el significado del valor de los objetos *sysServices* y *sysObjectID*.

33. Expanda el árbol *[interfaces]* y señale el *puerto No 10* haciendo click en el led respectivo de la ventana *Port Icons*. El grupo de interfaces tiene la información sobre las interfaces presentes, como pueden existir varias, el grupo contiene dos objetos de nivel superior: el *número de interfaces del objeto (ifNumber)* y una tabla con información de cada interfaz *(ifTable*). Cada entrada de la tabla (*ifEntry*) contiene información relativa a esa interfaz. Algunos de los objetos que contiene esta tabla son:

- *ifIndex* - Número de interfaz
- *ifDescr* - Descripción de la interfaz
- *ifType* - Tipo de la interfaz
- *ifMtu* - Tamaño máximo del datagrama IP
- *ifAdminisStatus* - Status de la interfaz
- *ifLastChange* - Tiempo que lleva la interfaz en el estado actual
- *ifINErrors* - Número de paquetes recibidos que contenían errores
- *ifOutDiscards* - Número de paquetes enviados y desechados

P 6.14. Para obtener los valores de los anteriores objetos se debe señalarlos y utilizar *Get for Selected Port* o *Get*. Llene la siguiente tabla:

Tabla 2.21. Grupo Interfaces.

Objeto	Valor	Interpretación
ifNumber		
IfType		
IfMtu		
ifSpeed		
ifPhysAddrers		
ifInOctects		
ifOutOctects		
ifInUCastPkts		
ifInNUCastPkts		

34. Expanda el árbol *[snmp]*. Entre los objetos que tiene se encuentran:

- *snmpInBadversions*- Número total de mensajes snmp que fueron entregados a la entidad de protocolo snmp, los cuales poseían una versión no soportada.
- *snmpInBadCommunityNames*- Número total de mensajes entregados a la entidad de protocolo snmp que utilizaban un nombre de comunidad desconocido.
- *snmpInASNParseErrs*- Número total de errores ASN.1 (Formato empleado por los oid) encontrados por la entidad de protocolo snmp durante la decodificación de los mensajes snmp recibidos.

- *snmpInTooBig*- Número total de PDUs snmp entregadas a la entidad de protocolo snmp y que tienen un valor "too Big " en el campo error_status.
- *snmpInTraps*- Número total de PDUs snmp que contienen traps aceptadas y procesadas por la entidad de protocolos snmp.

P 6.15. Llene la siguiente tabla:

Tabla 2.22. Objetos SNMP.

Objeto	Valor	Interpretación
SnmpInPkts		
SnmpInGetRequests		
SnmpInGetNexts		
SnmpInSetRequests		
SnmpOutgetResponses		
SnmpOutTraps		
snmpEnableAuthenTraps		

35. Expanda el árbol *[RMON][Statistics]* en su totalidad. Este es uno de los nueve grupos definidos por la IETF para las *estadísticas de monitoreo remoto Ethernet* y proporciona estadísticas de tráfico y errores mostrando paquetes, bytes, broadcasts, multicasts y errores sobre segmentos LAN o VLAN. Esta información es utilizada para detectar cambios en los patrones de tráfico y errores en áreas críticas de la red. Entre los objetos que posee se encuentran:

    - *etherStatsDataSource*-Representa la fuente de datos que etherStatsEntry tiene configurada para análisis. Esta fuente puede ser cualquier interfaz ethernet sobre el dispositivo.
    - *etherStatsOctets*- Número total de octetos de datos (Incluyendo aquellos en paquetes erróneos) recibidos sobre la red (Excluyendo bits de tramado pero incluyendo octetos FCS).
    - *etherStatsUndersizePkts*- Número total de paquetes recibidos menores de 64 octetos (Excluyendo bits de tramado pero incluyendo octetos FCS) bien formados.
    - *etherStatPkts64Octets*- Número total de paquetes (Incluyendo aquellos erróneos) recibidos con menos de 64 octetos de longitud (Excluyendo bits de tramado pero incluyendo bytes FCS).

P 6.16. Llene la siguiente tabla:

Tabla 2.23. Grupo Estadísticas RMON.

Objeto	Valor	Interpretación
EtherStatsDropEvents		
EtherStatsBroadcastPkts		
EtherStatsMulticastPkts		
EtherStatsCRCAlignErrors		
EtherStatsJabbers		
etherStatsPkts128to255Octects		
EtherStatsOwner		

NOTA: Las definiciones de los objetos para SNMP y el grupo Estadísticas de RMON se encuentran en las RFC 1213 y RFC 1757 respectivamente.

P 6.17. Repita el proceso anterior con el enrutador olimpo.ucauca.edu.co cuya IP es 172.16.255.190 y llene las tablas que sean posibles de acuerdo al punto B.

- **CONCLUSIONES**

2.1.7. Práctica No 7. Análisis de la Utilización del Ancho de Banda de la Red

- **OBJETIVOS:**

- Determinar que usuarios están consumiendo el mayor ancho de banda, las conexiones activas a Internet y el tráfico intercambiado entre subredes empleando el conjunto de funcionalidades que presenta la herramienta Estadísticas de Conexión.
- Utilizar el conjunto de funcionalidades que presenta la herramienta Analizador Experto.
- Utilizar el segundo conjunto de herramientas de las Pruebas Activas (Pruebas Activas Novell).
- Emplear la etiqueta Log de la ventana de configuración principal.

- **MARCO TEÓRICO**

LA UTILIZACIÓN (%): Es una medida de la cantidad de tiempo que la red está siendo usada para transmitir datos. Por lo tanto es una estadística importante que indica cuanto del ancho de banda de la red está en uso. Una alta utilización indica excesivos niveles de tráfico. El Internet Advisor despliega la utilización en el *Analizador Experto* y en *Estadísticas Vitales de Protocolo*. Ambas medidas muestran el porcentaje de utilización para el último periodo de muestreo.

TIPOS DE UTILIZACIÓN: Se presentan dos valores de utilización en *Protocol Vitals*, y sus interpretaciones dependen de la fuente actual de datos la cual es seleccionada en la ventana de configuración de la medida.

1. Pre-Filter Ethernet Utilization: Si la fuente de datos es la *red bajo prueba*, ésta es la utilización actual de la red. Este valor no es afectado por los filtros de captura. Sobre sistemas Ethernet (10Mbit) este valor siempre será exacto ya que está basado sobre contadores hardware. Sobre sistemas Fast Ethernet (100Mbit Full Duplex) donde la utilización de línea total excede 120Mbits/sec es posible que este valor no considere todas las tramas. Si ésto ocurre el indicador de estado ubicado en la parte inferior de la ventana de aplicación principal se colocará en *rojo*. Si la medida está corriendo desde el buffer de captura, este valor es el mismo que el de Post-Filter Utilization.

2. Post-Filter Utilization: Es la utilización para las tramas en el *buffer de captura.* Este es un contador software y puede ser afectado por el desempeño del procesador en el análisis del sistema. Activar pocas medidas al tiempo proporciona mayor precisión para este cálculo.

CÁLCULO DEL PORCENTAJE DE UTILIZACIÓN: Para todas las estadísticas Ethernet, la siguiente fórmula es usada para calcular el porcentaje de utilización.

Utilización (%) = (Número de bits medidos en 1 segundo / máxima velocidad de línea por sec) * 100

Para Ethernet las posibilidades de velocidad de línea son:

- 10Mbit Half Duplex (Standard Ethernet): Máxima velocidad de línea 10Mbit/sec.
- 10Mbit Full Duplex (Standart Ethernet): Máxima velocidad de línea 20Mbit/sec.
- 100Mbit Half Duplex (Opción Fast Ethernet): Máxima velocidad de línea 100Mbit/sec.
- 100Mbit Full Duplex (Opción Fast Ethernet): Máxima velocidad de línea 200Mbit/sec.

El número de bits medidos incluye el *preámbulo*, el *delimitador de inicio* y el mínimo espaciamiento entre tramas (9.6 microsegundos para Ethernet o 0.096 microsegundos para Fast Ethernet). Cualquier secuencia de bits precedida por un preámbulo válido que contiene un delimitador de trama es contabilizada como una trama y es incluida en el cálculo del porcentaje de utilización (A menos que haya sido filtrada por filtros de captura o por filtros software).

EJEMPLOS DEL CÁLCULO DE UTILIZACIÓN PARA UNA RED ETHERNET 10MBPS COMPLETAMENTE CARGADA.

1. Máximo número de tramas para una longitud de trama mínima.

La longitud de trama mínima es 64 octetos (6 para la dirección destino, 6 para la dirección fuente, 2 para el tipo o longitud, 46 de datos y 4 para FCS). A estos 64 bytes se deben adicionar los siguientes 20 octetos (7 de preámbulo, 1 delimitador de trama y tiempo para el espaciamiento de trama mínimo equivalente a 12 octetos sin importar cual sea la velocidad) con el propósito de calcular la velocidad de trama máxima.

Así, el número total de bits es 672 (64 + 20 = 84 bytes * 8 bits / octeto) y la velocidad de trama máxima para tramas de longitud mínima legal es:

Máxima velocidad de trama = 10,000,000/672 = 14,881(Tramas/sec)

En cuyo caso, la utilización es calculada como:

Utilización % = 84 * 8 (14881/10,000,000) * 100 = 100%

2. Número máximo de tramas para una longitud de trama máxima.

La longitud de trama máxima es 1518 octetos. A estos 1518 bytes se deben adicionar los siguientes 20 octetos (7 de preámbulo, 1 delimitador de trama y tiempo para el espaciamiento de trama mínimo equivalente a 12 octetos sin importar cual sea la velocidad) con el propósito de calcular la velocidad de trama máxima.

Así, el número total de bits es 12304 (1538 bytes * 8 bits / octeto) y la velocidad de trama máxima para tramas de longitud máxima legal es:

Máxima velocidad de trama = 10,000,000/12,304 = 813 (Tramas/sec)

En cuyo caso, la utilización es calculada como:

Utilización % = 1538 * 8 * (813/10,000,000) * 100 = 100%

REDES NOVELL NETWARE: Es un sistema operativo de red de computadores desarrollado por la empresa Novell que posee un conjunto de aplicaciones diseñadas para conectar, gestionar, mantener una red y sus servicios. Una red de este tipo utiliza el software NetWare para habilitar la comunicación entre dispositivos y el compartimiento de recursos. Asimismo NetWare es un conjunto de componentes software de los cuales algunos se ejecutan desde el servidor y otros desde las estaciones de trabajo. A una red NetWare se puede conectar los siguientes tipos de estaciones de trabajo DOS, Windows, OS/2, Macintosh y UNIX.

NetWare utiliza una arquitectura cliente/servidor. Los clientes solicitan servicios, tales como acceso a archivos e impresoras, a los servidores. Estas redes de datos utilizan cualquiera de los protocolos de nivel físico (1) y enlace (2) que existen, ya sean 802.3/Ethernet, Token Ring, FDDI, etc.. Hasta el lanzamiento de la versión NetWare 5.0 de Novell en 1998, todas las redes NetWare utilizaban IPX como único protocolo de nivel de red, sin embargo en la actualidad también soportan el protocolo TCP/IP. Netware de Novell es un conjunto propietario de protocolos que incluyen los siguientes:

- IPX, un protocolo de nivel 3 no orientado a conexión que no requiere acuse de recibo para cada mensaje, define la red, las direcciones de nodo y soporta broadcast. El header IPX tiene siempre 30 bytes de longitud y comienza con el valor 0xFFFF. Este header es transmitido después del frame de control de acceso al medio, pero antes del paquete de datos.

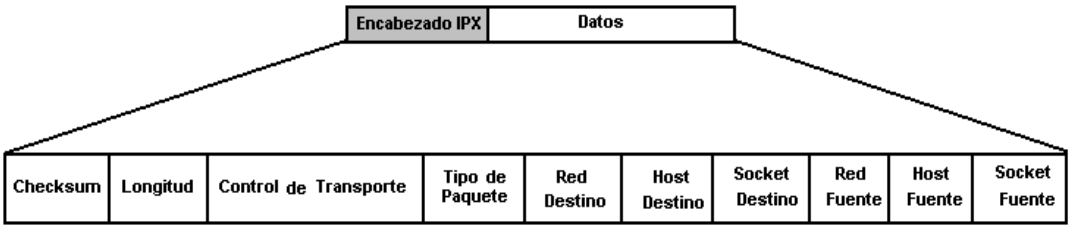


Figura 2.56. Datagrama IPX de Novell.

Donde:

Checksum: Este campo no es usado y siempre tiene el valor FFFF.

Longitud del Paquete: La longitud del paquete incluye el header y los datos, no incluye la trama Ethernet.

Control de Transporte: Este campo es usado por los routes IPX, y denota el número de routers que un paquete IPX ha atravesado. Este campo es puesto en 0 al comienzo y cuando llega a 16 se descartara el paquete.

Tipo de Paquete: 0 - unknown, 1 - RIP, 4 - SAP, 5 - sequenced packet (SPX), 17 - NCP and 20 - NetBIOS.

Red Destino: Este campo contiene la dirección de red del nodo destino que va desde 00000000 a FFFFFFFF.

Host Destino: La dirección del nodo destino es de 6 bytes, siendo FFFFFFFFFFFF broadcast.

Socket Destino: Este campo contiene el número de socket (Usados para indicar aplicaciones diferentes sobre la misma red y un nodo particular, IPX/SPX soporta un máximo de 20 sockets por nodo) del proceso de intranodo para el cual el paquete es direccionado.

Tabla 2.24. Especificación de los sockets destino.

Número de Socket	Descripción
451h	Protocolo Central de NetWare
452h	Protocolo de Anuncio de Servicio
453h	Protocolo de Información de Enrutamiento
455h	NetBIOS
456h	Diagnóstico
4000h – 6000h	Sockets Temporales*

* Usados para interacciones con servidores de archivos y otras comunicaciones de red.

Red Fuente: El número de red es la dirección de red en donde se encuentra el nodo fuente.

Host Fuente: Es la dirección del nodo fuente y FFFFFFFFFFFF no está permitido.

Socket Fuente: Este campo posee el número de socket del proceso que está transmitiendo el paquete.

- El protocolo de publicación de servicio (SAP) que permite publicar servicios de red.
- El protocolo central de NetWare (NCP) que permite proporcionar conexiones y aplicaciones cliente a servidor.
- Servicio de Intercambio de mensaje secuenciado (SPX), es un protocolo orientado a conexión que asegura la entrega correcta de los datos, controla la integridad de los paquetes y los ACK de los paquetes recibidos. Cuando un NACK es recibido el paquete se retransmite hasta un número máximo de veces, en cuyo caso se asume una falla en la red y la conexión es terminada.
- El protocolo de información de enrutamiento de Novell (RIP), que es diferente del RIP de IP, facilita el intercambio de información de enrutamiento.

Así la estructura de protocolos de Novell Netware se puede representar de la forma siguiente:

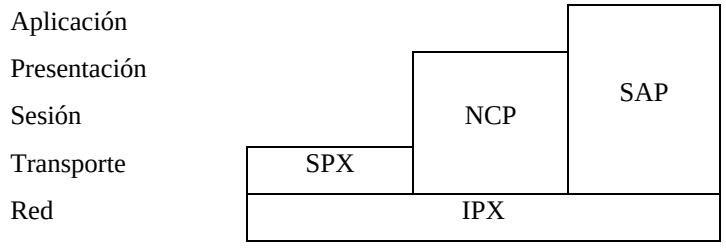


Figura 2.57. Novell vs OSI.

Direccionamiento: Los nodos son identificados por un número de 6 bytes (Node ID) y un identificador de red de 4 bytes (Network ID). El primero es asignado por los niveles bajos, por ejemplo, la dirección MAC de las tarjetas de red Ethernet. El ID de red es proporcionado por un servidor Novell a una estación de trabajo (Configurado en el servidor de archivos por el administrador) y es utilizado por los enrutadores para el envío de paquetes hacia la red correcta. El Node-ID de un servidor es usualmente 00-00-00-00-00-01 mientras el Network ID va desde 00000001 hasta FFFFFFFE (4 bytes).

ETIQUETA LOG DE LA VENTANA DE CONFIGURACIÓN PRINCIPAL: Tiene la habilidad de almacenar resultados de medidas a un archivo sobre el disco duro. Su ventaja sobre File | Save (Data) es que éste se encuentra limitado a almacenar el contenido del buffer de captura y sobre una red con alta utilización, el buffer puede ser llenado y sobrescrito varias veces durante una medición prolongada pudiéndose guardar únicamente los datos presentes en el buffer de captura, mientras que la función **Log** puede almacenar datos hasta un tamaño máximo correspondiente a la mitad del espacio disponible en el disco duro. También se puede cambiar el periodo y el intervalo de almacenamiento al

deseado controlando la cantidad de espacio de memoria utilizada y después que una medida es almacenada, se puede emplear el Internet Advisor para desplegar los datos.

- **EQUIPO UTILIZADO**
  - Internet Advisor WAN HP J2300D.
  - Cable de conexión RJ-45 100Base-TX.
  - Computador con punto de red (Puerto de un Hub).
  - Punto de red para el Internet Advisor.

- **PROCEDIMIENTO**

A. Medida Estadísticas de Conexión.

1. Entre al computador de trabajo (PC A) con privilegios de administrador y cambie la configuración de red así:

   - *Dirección IP:* 200.30.71.50. Verifique que esta dirección IP no se encuentre en uso (Por ejemplo realizando un ping), de lo contrario desconecte el punto de red del equipo que la tenga siempre y cuando se encuentre dentro del Laboratorio de Telemática del Departamento de Telecomunicaciones o emplee otra dirección IP oficial.
   - *Máscara:* 255.255.255.0
   - *Puerta de Enlace:* 200.30.71.254
   - *DNS Preferido:* 200.30.71.129
   - *DNS Alternativo:* Deje el servidor que aparece

2. Ejecute el Internet Explorer y *deshabilite* las opciones que permiten navegar mediante *proxy*. Navegue para verificar que la anterior configuración quedó bien realizada.

NOTA: Si la configuración anterior no funciona, averigue una dirección IP oficial con el ISP Telecom.

3. Instale los programas *KaZaA Media Desktop* (kmd201_en.exe) y *BearShare* (BSINSTALLES.exe) en el PC A los cuales se encuentran en el *CD anexo a la Monografía* en la carpeta *Programas Consumidores de Ancho de Banda*.

4. Encienda el Internet Advisor y entre al software LAN Fast Ethernet Undercradle. Realice una conexión en **Modo Nodo** y especifique los parámetros de la *ventana de configuración principal* para realizar un monitoreo en modo *Auto Negociado* y temporizado durante *10 minutos*. Mantenga el tamaño del buffer de captura a 26 Mb. Abra desde la barra de herramientas principal las medidas *Estadísticas de Conexión* y *Analizador Experto*, igualmente desde *File / Open Measurement* las medidas *Protocol Stats Novell.msx* y *Protocol Vitals.msx*.

5. En la ventana de configuración principal seleccione la pestaña *Log*. Habilite todas las casillas *On/Off* y digite en el campo *Interval (hhh:mm:ss)* 000:00:10 y en el campo *Period (hhh:mm)* 000:10, luego, mediante el botón *Browse* seleccione la carpeta C:*My Documents/Archivos de Datos/Practica No 7* y en el campo *File Name* escriba *EstadísticasLog.dat*. Guarde el archivo.

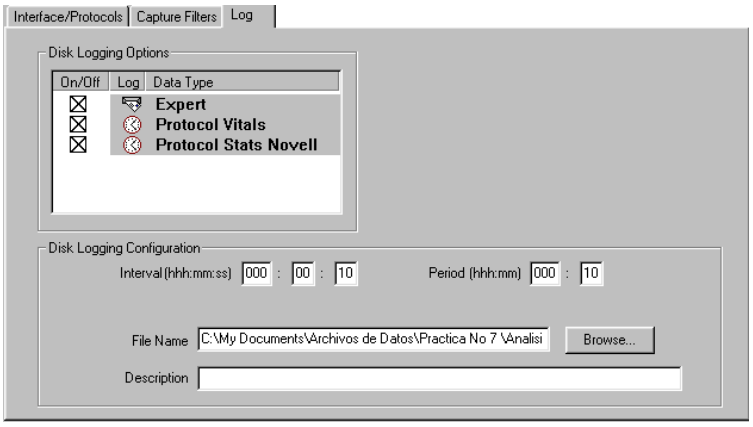


Figura 2.58. Configuración de la etiqueta Log.

6. Ejecute el programa *KaZaA*, espere a que se conecte (Debe cargar la página web principal del programa), presione el botón *Search* en la barra de herramientas principal, escriba en la caja de texto *Search for:* la palabra *"Sting"* y habilite la casilla *Audio*. Luego habilite la casilla *Artist* y presione el botón *Search Now*.

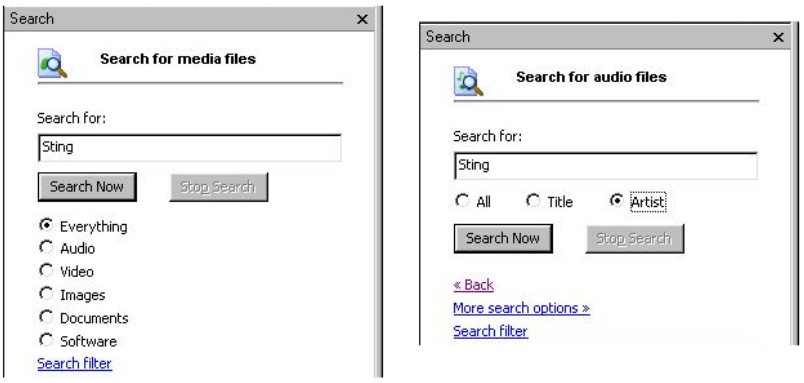


Figura 2.59. Búsqueda de archivos de audio utilizando KaZaA.

7. Ejecute el programa *BearShare*, espere a que se conecte (Debe mostrar la página de bienvenida del programa), presione el botón *Búsquedas* en la barra de herramientas principal, escriba en la caja de texto *Con todas las palabras:* la palabra "*Queen"* y seleccione de la caja de lista *Solamente estas:* la opción *Musica/MP3.* Presione el botón *Buscar Ahora*.

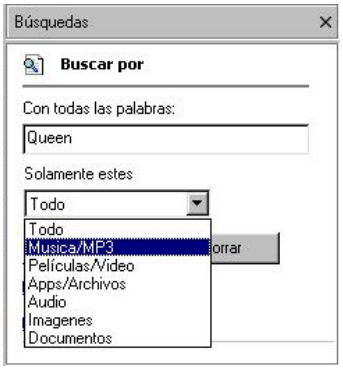


Figura 2.60. Búsqueda de archivos de audio utilizando BearShare.

NOTA: A continuación se utilizarán los programas KaZaA y BearShare para descargar archivos de audio y debido a que ellos **DEGRADAN EL DESEMPEÑO DE LA RED DE DATOS** ya que ocupan un porcentaje considerable del ancho de banda en los enlaces con los ISP Orbitel y Telecom, se recomienda **UTILIZARLOS SÓLO PARA LOS FINES DE ESTA PRÁCTICA**.

8. En el programa KaZaA seleccione los primeros 10 archivos de audio que aparecen y mediante el botón derecho del mouse escoja la opción *Download.* Presione el botón *Traffic* en la barra de

herramientas principal y verifique que efectivamente se empiezan a descargar los archivos seleccionados.

Figura 2.61. Descarga de archivos de audio utilizando KaZaA.

9. Abra el programa BearShare, en la ventana *Búsquedas* seleccione con el botón derecho del mouse la palabra "*Queen"* y escoja la opción *Parar*. Seleccione los primeros 10 archivos de audio que aparecen y mediante el botón derecho del mouse escoja la opción *Descargar.* Presione el botón *Descargas* en la barra de herramientas principal y verifique que efectivamente se empiezan a almacenar los archivos seleccionados.

Figura 2.62. Descarga de archivos de audio utilizando BearShare.

10. Inicie la captura de tráfico en el Internet Advisor y cuando termine detenga la descarga de los archivos de audio en el PC A así:

- Para KaZaA, presione el botón *Traffic*, realice un click con el botón derecho del mouse sobre el área de descarga y escoja la opción *Cancel all Downloads*. Responda afirmativamente a la caja de diálogo que aparece.

- Para BearShare, presione el botón *Descargas*, realice un click con el botón derecho del mouse sobre el área de descarga y escoja la opción *Cancelar Todo*. Responda afirmativamente a la caja de diálogo que aparece.

11. En el Advisor abra la medida *Estadísticas de Conexión*, seleccione *la columna Nodes/Conns/Prots*, despliegue las *opciones del botón derecho del mouse* y escoja *Sort by this column*.

P 7.1. Escoja cinco nodos que considere adecuados, expándalos totalmente y determine el número de conexiones activas y los protocolos usados por cada nodo, complete la tabla.

Tabla 2.25. Conexiones activas, protocolos y ancho de banda empleados por un nodo.

NODO IP	No Conexiones Activas	Protocolos Empleados	Bytes Transmitidos	Bytes Recibidos	BW Consumido

NOTA: Para calcular el ancho de banda consumido por un nodo aplique la siguiente ecuación:

BW (bps) = ((Bytes Tx + Bytes Rx) * 8) /Tiempo de captura

12. Con el botón derecho del mouse escoja *View Protocols/Nodes/Connections*, seleccione la columna de *bytes transmitidos* con el *botón derecho del mouse* y active la opción *Sort by this column.*

P 7.2. Llene la siguiente tabla para los cinco protocolos más utilizados en el segmento de red.

Tabla 2.26. Protocolos más empleados en el segmento de red.

Protocolo	Bytes -> (Tx)	% de Utilización respecto al total de bytes TX

P 7.3. ¿Cuál es la razón para que las cantidades de las estadísticas *Frames Tx* y *Frames Rx*, *Bytes Tx* y *Bytes Rx* se mantengan constantes respectivamente para cualquier protocolo en *Estadísticas de Conexión*?

P 7.4. Determine las conexiones *activas a Internet* expandiendo el árbol PROXY – NEXUS - 3128 995. Expanda los tres primeros nodos que aparecen bajo este árbol y llene la siguiente tabla.

Tabla 2.27. Conexiones Activas a Internet.

IP	Conexiones activas	Puerto Fuente	Puerto destino
	- - -	- - -	- - -
	- - -	- - -	- - -
	- - -	- - -	- - -

P 7.5. Escoja la opción *View Nodes* y llene la siguiente tabla para los cinco nodos que consumen el *mayor ancho de banda* en sentido de transmisión.

Tabla 2.28. Usuarios que consumen el mayor ancho de banda (Top Talkers) en sentido de transmisión.

IP, nombre o Dir Novell	Bytes -> (Tx)	BW_{TX} (bps)	% de Utilización$_{TX}$

NOTA: Para calcular el porcentaje de utilización consumido por un Top Talker en sentido de transmisión, aplique las siguientes ecuaciones.

$$BW_{TX} = (\text{Bytes Tx} * 8) / \text{Tiempo de captura} \quad (\text{bps})$$

$$\text{Utilización}_{TX}\ \% = (BW_{TX} * 100) / \text{Máxima velocidad de línea}$$

$$\text{Utilización}_{TX}\ \% = (BW_{TX} * 100) / 100\ 000\ 000 \quad \text{(Para segmento de red Fast Ethernet Half Duplex)}$$

P 7.6. Escoja la columna *bytes recibidos* y la opción *Sort by this column* y llene la siguiente tabla para los cinco nodos que *consumen el mayor* ancho de banda en *sentido de recepción*.

Tabla 2.29. Usuarios que consumen el mayor ancho de banda (Top Talkers) en sentido de recepción.

Nodo (Dir IP o Novell)	Bytes < - (Rx)	BW_{RX} (bps)	% de Utilización$_{RX}$

13. Escoja la opción *View Connections* y luego *Group By Subnet.* Seleccione la columna *Frames ->* y la opción *Sort by this Column.*

P 7.7. Observe todas las subredes que aparecen y para las dos primeras llene la siguiente tabla:

Tabla 2.30. Determinación de subredes y tráfico cursado entre ellas.

IP Subred	Subredes con las que posee conexiones	Frames Tx	Frames Rx
	1- 2- 3- 4-	- - - -	- - - -
	1- 2- 3- 4-	- - - -	- - - -

B. Medida Analizador Experto.

Se debe tener presente que los datos mostrados en la tabla para algunas medidas (*Frames/Sec, Bytes/Sec, Frames, Bytes* y *Utilization*) no corresponden a *valores acumulados* sino a *valores actuales* del registro seleccionado en *Rec #* (Muestra de tráfico en la red por un periodo de 10 segundos), así

para realizar un análisis global de la red o del segmento que involucren este tipo de medidas es conveniente utilizar los resultados proporcionados por la *gráfica.*

14. Abra la medida correspondiente al *Analizador Experto*. Deshabilite la tabla utilizando el botón *Show Grid* de la barra de herramientas de la medida, despliegue las *opciones proporcionadas por el botón derecho del mouse* y seleccione *Events*. De acuerdo a la gráfica realice un análisis sobre el estado del segmento, examine los picos que se presentan y realizando un *doble click* sobre éstos entre al *Comentador*; determine los *nodos*, las *conexiones* y los *eventos involucrados*.

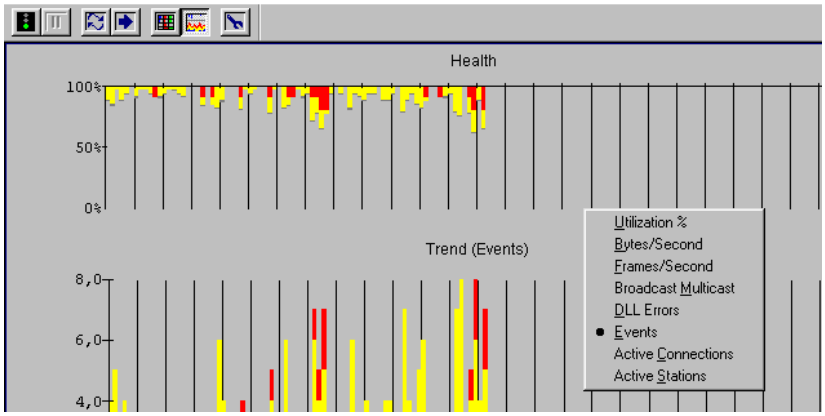


Figura 2.63. Área Gráfica de la medida Analizador Experto.

15. Regrese al *Analizador Experto* y seleccione la opción *Utilization %*. Realice un análisis teniendo en cuenta los protocolos utilizados, los niveles de éstos y analice si los resultados corresponden con lo esperado.

P 7.8. Seleccione la opción *Broadcast Multicast* y describa el comportamiento de cada tipo de tráfico.

P 7.9. Haga click con el botón derecho del mouse en cualquier punto específico de la anterior gráfica y determine el número de tramas *Broadcast, Multicast* y *Unicast* para tres muestras espaciadas cada 3 minutos. Consigne los datos en la siguiente tabla:

Tabla 2.31. Estadísticas de tramas Multicast, Broadcast y Unicast.

Muestra	Multicast	Broadcast	Unicast
1			
2			
3			

P 7.10. Seleccione la opción *DLL Errors* (Data Link Layer) y determine los tipos de errores que se presentaron en la medida.

16. Presione los botones *Show Grid* y *Rec #* de la barra de herramientas de la medida, escriba el último registro válido y presione *OK*. Este último paso tiene la finalidad de que la tabla de datos tenga en cuenta el acumulado de las muestras durante el proceso de captura del archivo. Sobre la fila *Totals* y bajo la columna *Alerts* realice un doble click para entrar al *Comentador* y expanda el árbol *Display All Events***.**

P 7.11. Realice el proceso anterior para las columnas *Warnings* y *Normals.* Anote los eventos que aparecen y haga una breve descripción sobre el significado de cada uno de ellos.

P 7.12. Realice un doble click sobre la última celda de la columna *Stations* y anote las IP de los enrutadores que aparecen. Determine los eventos asociados con éstos y sus causas (Columnas *Alerts*, *Warnings* y *Normals*).

P 7.13. Desde el menú Windows seleccione la medida *Protocol Stats Novell* y determine el porcentaje de tramas y de bytes con respecto al total de ellas para cada protocolo y empleando la medida *Estadísticas Vitales de Protocolo* anote el porcentaje de utilización promedio del medio de transmisión para el stack Novell. Llene la Tabla 2.32.

P 7.14. Consulte la funcionalidad de los protocolos IPX SMB y SERVICE ADV.

P 7.15. ¿Por qué la utilización promedio de Novell para el segmento de red es tan baja?

Tabla 2.32. Utilización del stack Novell en el segmento de red.

STACK NOVELL / PROTOCOLOS	TRAMAS (%)	BYTES (%)	Utilización promedio del medio (%)
IPX SMB			
Netbios name			
SERVICE ADV			
NETBIOS			
ROUTING			
OTROS			

C. Pruebas Activas Novell.

17. *Cierre* todas las medidas, vaya a *Active Tests* y seleccione *Novell View Nodes*, escriba en el campo *Timeout* (ms) el número 25000 e inicie la medida. Espere a que termine la medida.

18. Expanda algunos nodos cuyo número de componentes sea *uno, dos* y *tres*. Empleando el *botón derecho del mouse* seleccione un nodo que tenga encapsulación *802.3/802.2/IPX* y utilizando la opción *Drill into Decode / From Address* entre al *Decodificador*. Ejecute el mismo procedimiento para un nodo con encapsulación *802.3/802.2/SNAP/IPX*. Responda las siguientes preguntas:

P 7.16. Consulte porque el campo *Checksum* para el header IPX en ambos tipos de encapsulaciones no es utilizado y siempre posee el valor de *FFFF*.

P 7.17. A nivel de encabezado MAC ¿Cuál es la diferencia entre una trama de red capturada normalmente (TCP/IP) y este par de encapsulaciones?. ¿A qué se debe esta divergencia?

P 7.18. ¿Cuál es la composición y tamaño en bits de una dirección Novell?

19. Señale un nodo cualquiera de la lista desplegada en la prueba activa *Novell View Nodes* y utilizando las opciones desplegadas con el *botón derecho del mouse* escoja la opción *Novell Node Ping* (Esta operación es *equivalente* a escoger la opción con el mismo nombre desde la medida *Active Tests*). Digite en el campo *Number of Requests* el número 3 e inicie la medida.

20. Entre al *Decodificador* desde cualquiera de las tres respuestas desplegadas usando la opción *Drill into Decode/To or Fromm Address* y detalle las tramas en ambos sentidos.

P 7.19. Determine los *tipos de paquetes* intercambiados cuando se hace una *prueba de este tipo* conforme a la información visualizada en el *Decodificador*.

21. Cierre todas las medidas utilizadas hasta el momento y desde *Active Tests* seleccione la opción *Novell Nearest Server*, en el campo *Timeout* (ms) escriba el número 10000 y escoja la opción *All Servers* (FFFF) del campo *Server Type*. Corra la medida.

P 7.20. ¿Cómo es la dirección MAC y cuál es la diferencia con las otras MACs de Novell?

22. Vaya al *Decodificador,* haga un clareo del filtro de despliegue mediante la opción *Reset* y cree un *filtro de despliegue para protocolo Novell* teniendo en cuenta todas las encapsulaciones posibles para este stack. Observe la estructura del primer paquete que tiene como *origen* el Internet Advisor y responda las siguientes preguntas:

P 7.21. ¿Qué tipo de encapsulación tiene este paquete?

P 7.22. De acuerdo al campo Socket Destino. ¿Qué tipo de protocolo se está utilizando dentro del campo de datos del paquete IPX y que función desempeña?

Ahora observe la estructura del primer paquete que tiene como *destino* el Internet Advisor y responda las siguientes preguntas:

P 7.23. ¿Qué tipo de encapsulación tiene este paquete?. ¿Qué tipo de paquete se está enviando desde el Servidor NetWare de acuerdo a los datos embebidos en el campo de datos del datagrama IPX?. ¿Qué *tipo de servicio* está prestando este servidor?. ¿Cuál es el nombre del servidor, su dirección de red e identificador de nodo y el número de enrutadores intermedios que el paquete ha atravesado para llegar a su destino? y ¿Qué función realiza el socket que aparece en el campo SAP: Socket?

23. Desde *Active Tests* escoja la opción *Novell Server List* y digite en el campo *Timeout* (ms) el número 10000, el campo *Server Type* seleccione la opción *All Servers (FFFF)* y active la medida. Para los servidores encontrados, visualice las *opciones desplegadas con el botón derecho del mouse* y seleccione *Drill into Decode/ From Address* para entrar al *Decodificador*.

P 7.24. ¿Qué indica el campo *SAP: Packet Type* en el encabezado *SAP*?

24. Cierre todas las medidas a excepción de *Novell Server List*, señale el servidor cuyo nombre es NETWARE y utilizando las *opciones desplegadas con el botón derecho del mouse* escoja la opción *Novell Server Ping* (Esta operación es equivalente a escoger la opción con el mismo nombre desde la herramienta *Active Tests*). Inicie la prueba activa.

P 7.25. Consulte:

- El número máximo de sockets soportados por un nodo cuando maneja IPX/SPX.
- ¿El RIP utilizado en Novell es igual al empleado en TCP/IP, explique?.

- Realizar una comparación en cuanto a formato de un Datagrama IP vs IPX y segmento TCP vs SPX (Indicar cuales son sus diferencias y semejanzas).

- **CONCLUSIONES**

2.2. ENTORNO WAN

2.2.1. Práctica No 8. Análisis de Desempeño de la Red de Datos Universidad del Cauca

- **OBJETIVOS:**

- Realizar el análisis de desempeño en algunos puntos claves de la Red de Datos de la Universidad del Cauca considerando los enlaces WAN para el par de proveedores de acceso a Internet, el enlace backbone ingenierías, los servidores de correo electrónico (Atenea y Afrodita), el servidor web interno (Acuario 1), el servidor DNS Hércules, el servidor FTP (Odín), los proxys Proxydom, Proxysis, Proxyres de Orbitel y el Proxying de Telecom.
- Utilizar el análisis de desempeño para ver la realidad y la situación actual de la red en los puntos examinados.
- Enfocar el análisis en medidas claves como: Porcentaje de utilización, colisiones locales y remotas, colisiones tardías locales y remotas, broadcast, multicast, porcentaje de utilización por protocolos y porcentaje de utilización por protocolos del stack TCP/IP entre otras.

- **MARCO TEÓRICO**

SWITCH ACCELAR 1200 BayNetworks: Este equipo es un switch de nivel 3 de alta densidad diseñado para trabajar en backbones, centros de datos y aplicaciones en estaciones de trabajo de alta velocidad. El chasis del Accelar 1200 posee 8 slots, 6 de los cuales pueden soportar módulos de I/O (Entrada y Salida) y el par restante está reservado para módulos SSF (Silicon Switch Fabric) cuya funcionalidad consiste en la operación del chasis, uno solo de estos módulos es necesario y los dos pueden trabajar en una configuración de redundancia hot standby para diseño de redes de alta confiabilidad. El Accelar 1200 soporta dos fuentes de alimentación redundantes y completamente cargado tiene una de las siguientes densidades de puertos máxima:

- 96 puertos 10 BASE-T/100 BASE-TX cuando se tiene en los 6 slots la tarjeta XLR1216TX.
- 48 puertos 100 BASE-FX cuando se tiene en los 6 slots la tarjeta XLR1208FX.
- 12 puertos 1000 BASE-SX o 1000 BASE-LX cuando se tiene en los 6 slots la tarjeta XLR1202SX.

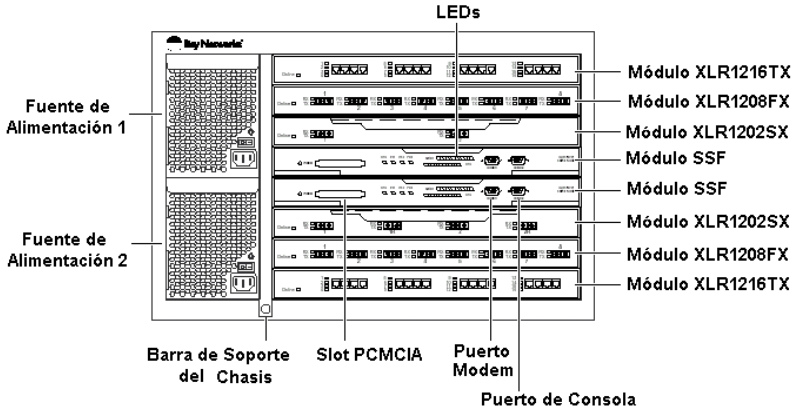


Figura 2.64. Vista Frontal del Accelar 1200.

La siguiente tabla ilustra la gama de módulos soportados por el equipo.

Tabla 2.33. Módulos Accelar 1200.

Referencia	Descripción
XLR1297SF	Módulo Silicon Switch Fabric (SSF)
XLR1216TX	Módulo de 16 puertos 10/100BASE-TX
XLR1208FX	Módulo de 8 puertos 100BASE-FX
XLR1201SX	Módulo de 1 puerto 1000BASE-SX
XLR1202SX	Módulo de 2 puertos 1000BASE-SX
XLR1202SR	Módulo de 2 puertos 1000BASE-SX con LinkSafe
XLR1201LX	Módulo de 1 puerto 1000BASE-LX
XLR1202LX	Módulo de 2 puertos 1000BASE-LX
XLR1202LR	Módulo de 2 puertos 1000BASE-LX con LinkSafe

El Switch puede ser configurado y gestionado mediante tres métodos:

- *Interfaz Web:* El Switch posee un conjunto interno de páginas Web que permiten administrarlo utilizando un *browser Web*.
- *Interfaz Línea de Comandos:* Se utiliza conectando un cable Null MODEM entre la estación de gestión y el puerto de consola del Switch empleando la herramienta *Hyper Terminal* o remotamente ejecutando un *telnet* a través de uno de sus *puertos*.
- *Gestión SNMP:* Se puede administrar el Switch usando cualquier *gestor de red* que corra el Protocolo de Gestión de Red Simple (SNMP) como el software *Accelar Device Manager*.

ACCELAR DEVICE MANAGER: Es una interfaz de usuario gráfica basada en SNMP usada para gestionar un dispositivo único. Otras herramientas de gestión que son parte del software de gestión Accelar tales como Accelar VLAN Manager, Accelar Configuration Page y la Interfaz de Línea de Comandos (CLI) permiten gestionar algunos aspectos del equipo, sin embargo, el Accelar Device Manager proporciona todas las opciones encontradas en las anteriores herramientas excepto la habilidad de gestionar VLAN´s a través de múltiples equipos.

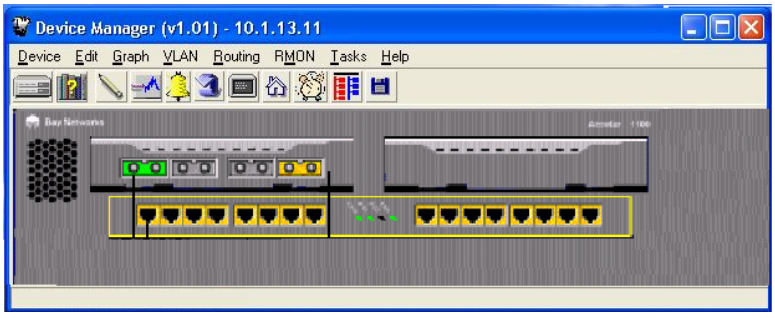


Figura 2.65. Ventana Device Manager del Accelar 1100.

La ventana del *Accelar Device Manager* contiene tres herramientas principales para el acceso a las opciones de gestión que son:

- **Barra de Menú**

Tabla 2.34. Descripción de la Barra Menú para el Accelar Device Manager.

Campo	Descripción
Device	Abre un dispositivo, permitiendo la edición de sus parámetros para la gestión del chasis y el sistema.
Edit	Mostrar y editar parámetros para la tarjeta, módulo de I/O y puerto seleccionados como también aquellos relacionados con la seguridad y el diagnóstico.
Graph	Ver las estadísticas del switch en modo gráfico.
VLAN	Configurar y editar VLANS, incluyendo spanning tree group (STG) y multi-link trunking (MLT).
Routing	Configurar y editar IP (DHCP, DVMRP, IGMP, IP, Multicast, OSPF, RIP, UDP, Forwarding, VRRP, Filtros IP E IP Policy) e IPX (IPX, RIP y SAP).
RMON	Configurar alarmas y observar eventos así como el control de los significados y el modo de notificación de éstos.
Tasks	Habilitar/Deshabilitar: La capacidad Spanning Tree FastStart sobre el puerto seleccionado, la historia y las estadísticas RMON sobre todos los puertos.
Help	Presentar la ayuda en línea.

- **Barra de Herramientas:** Contiene íconos que proveen accesos directos para tareas comunes como se describe en la siguiente figura.

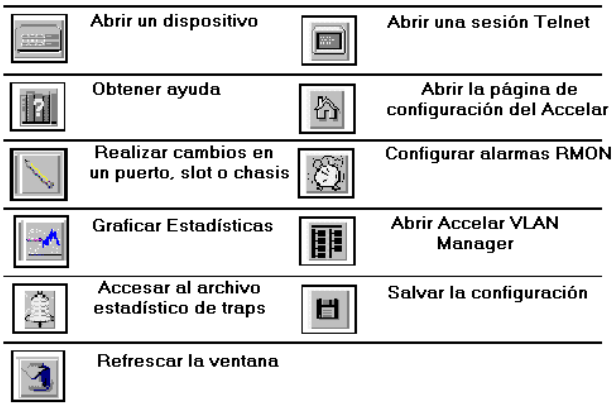


Figura 2.66. Descripción Barra de Herramientas del Accelar Device Manager.

- **Representación Gráfica del Switch:** Presenta el estado operacional actual de los puertos y slots del equipo, además se pueden ejecutar tareas de administración sobre objetos específicos (El chasis, uno o más puertos y uno o más módulos). Las siguientes dos tablas muestran la codificación por colores tanto para módulos como para puertos.

Tabla 2.35. Codificación por colores para el estado de los módulos.

Color	Descripción
Rojo	El módulo en el slot está presente pero no se encuentra operando.
Verde	El módulo en el slot está arriba y operando.

Tabla 2.36. Codificación por colores para el estado de los puertos.

Color	Descripción
Azul Claro	El puerto está en standby.
Azul Obscuro	El puerto está siendo probado.
Rojo	El puerto ha fallado o ha sido manualmente deshabilitado y no se encuentra operando.
Verde	El puerto está arriba y operando.
Naranja	El puerto no tiene enlace.

PORT MIRRORING: Empleando esta funcionalidad se especifica un *puerto destino* sobre el cual se desea observar el tráfico reflejado y *un par de puertos fuentes* desde los cuales el tráfico es reflejado. Los paquetes entrantes y salientes en los puertos especificados son transmitidos normalmente y una *copia* de ellos es enviada al *puerto espejo*. Esta operación se caracteriza por ser *no intrusiva*, es decir, no afecta el curso normal de tráfico en el switch para los puertos involucrados.

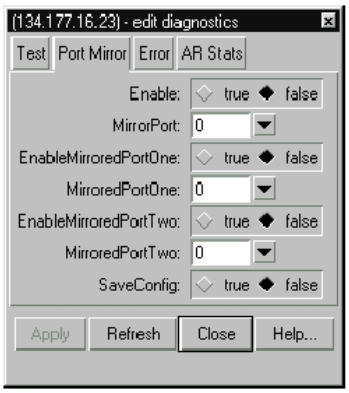


Figura 2.67. Ventana Port Mirror del Accelar Device Manager.

- *Enable:* Usado para indicar si la característica de *puerto espejo* está activa.
- *MirrorPort:* El puerto al cual el tráfico reflejado es enviado, *puerto espejo*.
- *EnableMirroredPortOne:* Empleado para indicar si el puerto especificado en MirroredPortOne debería ser reflejado.
- *MirroredPortOne:* El primer puerto a ser reflejado, es decir, el tráfico relacionado con éste será trasmitido normalmente a su destino y una *copia* se enviará al *puerto espejo*.
- *EnableMirroredPortTwo:* Empleado para indicar si el puerto especificado en MirroredPortTwo debería ser reflejado.
- *MirroredPortTwo:* El segundo puerto a ser reflejado, es decir, el tráfico relacionado con éste será trasmitido normalmente a su destino y una *copia* se enviará al *puerto espejo*.
- *SaveConfig:* Controla si la configuración del *puerto espejo* debería ser salvada a la NVRAM (Non Volatile Random Access Memory). Para hacer efectiva la configuración es necesario fijar *SaveConfig* a verdadero (Presionar el botón *Apply*) y salvar la configuración del switch presionando el botón *Save Configuration* de la barra de herramientas en el *Accelar Device Manager*.

- **EQUIPO UTILIZADO**
  - Internet Advisor WAN HP J2300D
  - Cable largo de conexión RJ-45 100Base-TX
  - Accelar 1200 Routing Switch
  - Switch 3COM 3300XM
  - Estación de trabajo con sistema operativo Windows 95/98/NT/2000/XP (Ubicada preferiblemente en la Red de Datos)

- **PROCEDIMIENTO**

A. Captura de tráfico para el enlace WAN con el proveedor de acceso a Internet Telecom.

La configuración actual de este enlace se presenta a continuación:

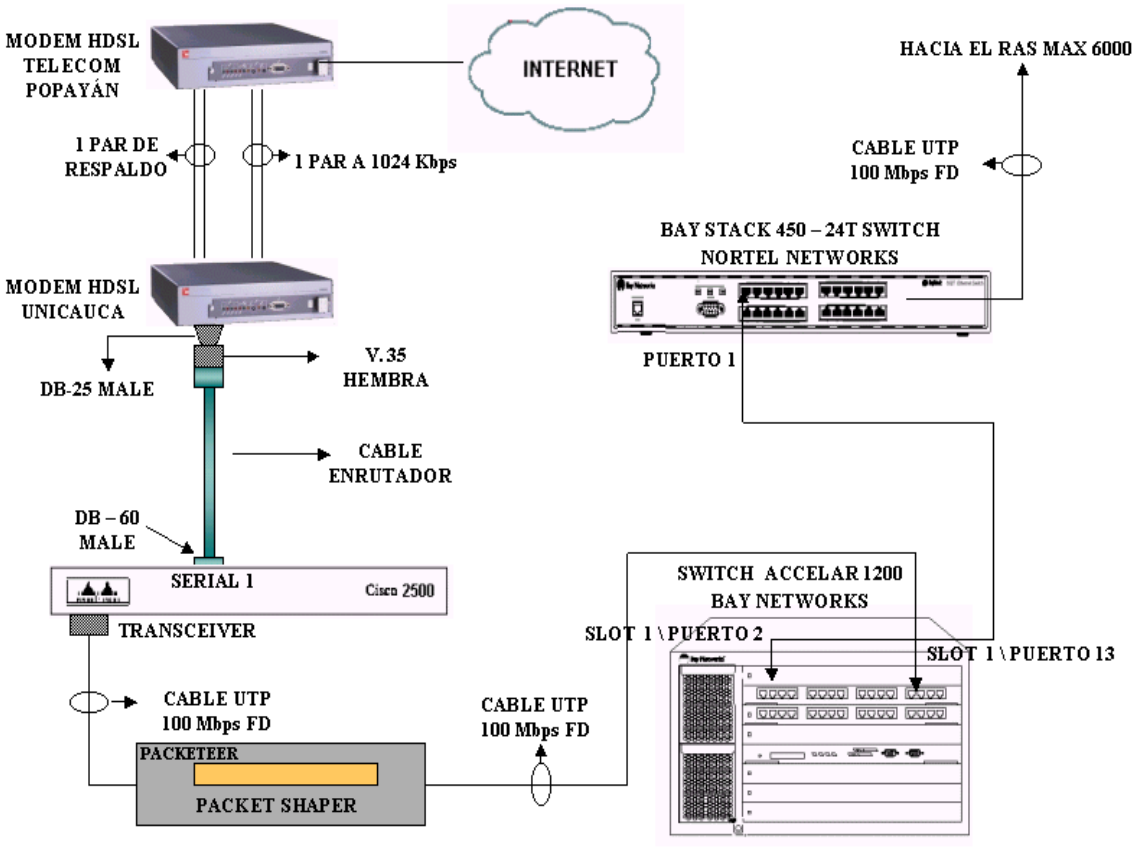


Figura 2.68. Enlace WAN Telecom.

En el centro de cableado No 5 (CC5) localizado en el IPET se encuentra un modem HDSL Pair Gain (UTU – 804 G.703 Nx64K) conectado con su homólogo en Telecom por medio de *dos pares de cobre*, de los cuales uno es de respaldo y el otro trabaja a una velocidad de 1024 Kbps. El modem HDSL de la Universidad a través de su conector DB-25 hembra se une a un conversor (DB-25 macho / V.35 hembra) y luego se conecta al puerto serial 1 del enrutador Cisco 2500 por medio de un cable propio de este equipo. Este enrutador se conecta a un Packet Shaper (Cuya finalidad consiste en filtrar determinado tipo de paquetes) y éste a su vez se une al puerto 13 del módulo XLR1216TX del Accelar 1200 cuya velocidad de línea es 100 Mbps FD. Este switch se conecta a un BayStack 450 – 24T Switch de 24 puertos, el cual se enlaza a una RAS MAX 6000 (Proporciona el acceso externo a Internet vía telefónica) a través de un cable UTP a 100 Mbps FD.

1. Instale en la estación de trabajo el software *Accelar Device Manager* que se encuentra en el CD etiquetado como *Accelar 1000 Series Software 1.0* (Windows 95/NT, Solaris, and HP-UX) que viene con el equipo o en los CD´s anexados a la monografía.

2. Abra la ventana de gestión del dispositivo seleccionando *Accelar Device Manager* y en seguida escoja la opción *Open* del menú *Device.*

Figura 2.69. Entrando al Accelar 1200 Red de Datos.

3. Escriba en el campo *Device Name* la dirección *IP 10.1.13.11* (Dirección de red del switch), en *Read Community* y *Write Community* consigne las comunidades (**Deben ser preguntadas al ingeniero encargado de dicho equipo**) que permitan el acceso a todos los privilegios de lectura-escritura y la habilidad para cambiar las configuraciones de seguridad. Cuando se abre el dispositivo se visualiza la siguiente ventana.

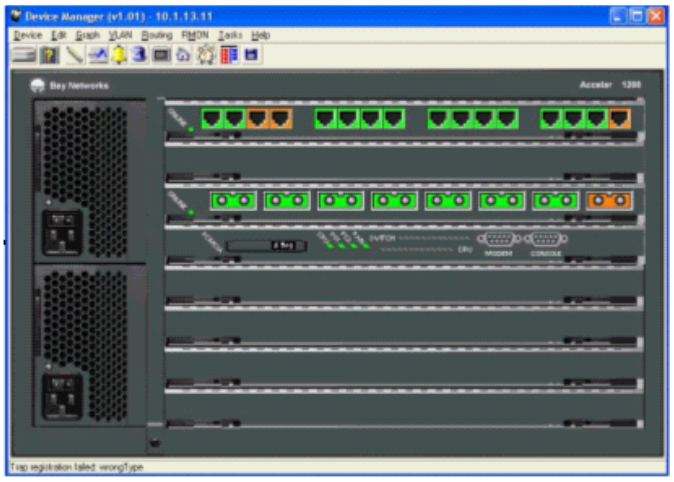


Figura 2.70. Representación gráfica del Accelar 1200 Red de Datos.

4. Conecte el cable largo de conexión RJ-45 100Base-TX a uno de los puertos **libres** y en **buen estado** del Accelar (Ejem: Puerto No 6) y el otro extremo al puerto *"To Hub/Switch"* del Internet Advisor.

5. Encienda el Internet Advisor, entre al software LAN Fast Ethernet Undercradle y en la ventana de configuración principal seleccione la pestaña *Interface/Protocols*. Fije los siguientes valores:

   - *Media Connection:* TX Auto Negotiate
   - *Monitor Type:* Timed
   - *Monitor Period (hhh:mm):* 001:00
   - *Buffer Size:* 26.00 MB

6. Abra cada una de las medidas en la barra de herramientas del Advisor con excepción de *Estadísticas Vitales de Línea*, *Pruebas Activas*, *Estadísticas VLAN* y el *Decodificador*. Desde el menú *File/ Open Measurement* abra las medidas *Protocol Stats IP.msx*, *Protocol Stats Novell.msx y Protocol Stats Stk.msx*.

7. Seleccione la pestaña *Log* de la ventana de configuración principal, habilite las casillas *On/Off* para cada una de las medidas que aparecen bajo la columna *Data Type*, escriba en el campo *Interval (hhh:mm:ss)* 000:00:30 y en el campo *Period (hhh:mm)* 001:00. En *File Name* escoja mediante el botón *Browse* la siguiente ruta C:\My Documents\Archivos de Datos\Practica No 8\ y

proporcione un nombre descriptivo para el archivo (Ejem: Router Telecom). En *Description* consigne la fecha y hora de la medición.

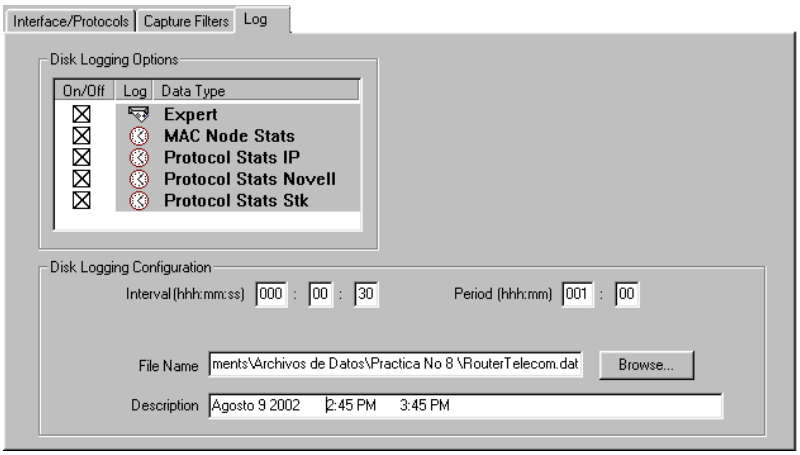


Figura 2.71. Configuración pestaña Log para el enlace WAN con Telecom.

8. Seleccione el menú *Edit* del software Accelar Device Manager y escoja la opción *Diagnostics*. En la ventana *(10.1.13.11) – edit diagnostics*, seleccione la pestaña *Port Mirror* y realice la siguiente configuración:

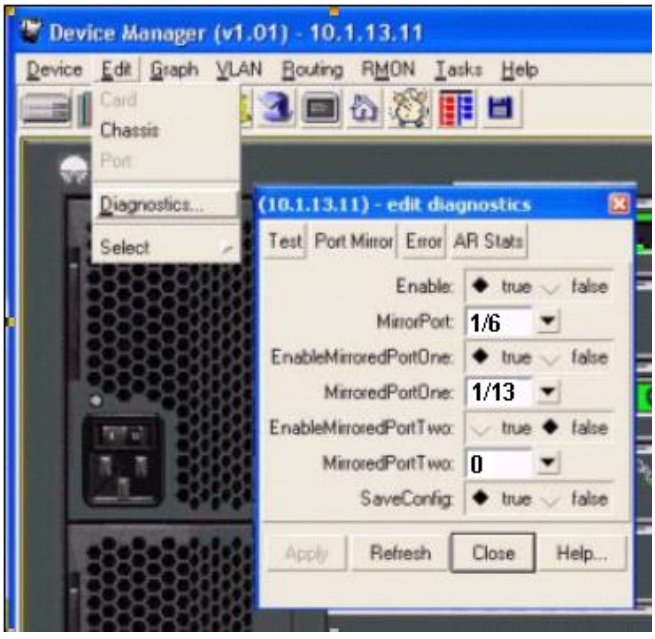


Figura 2.72. Configuración puerto espejo para el enlace WAN con Telecom.

- *Enable*: true
- *MirrorPort:* 1/6 (Slot 1/ Puerto 6)- Puerto Espejo
- *EnableMirroredPortOne*: true
- *MirroredPortOne*: 1/13 (Slot 1/ Puerto 13) – Enlace Telecom
- *EnableMirroredPortTwo:* false
- *MirroredPortTwo:* 0
- *SaveConfig*: true

Presione *Apply* y luego *Save Configuration* en la barra de herramientas del Accelar Device Manager para hacer efectivos los cambios. Inicie la captura de tráfico en el Advisor.

9. Una vez terminada la captura de tráfico, seleccione la pestaña *Capture Filters* de la ventana de configuración principal y adicione un filtro para almacenar las tramas que concuerden con los siguientes protocolos de enrutamiento: RIP, IGRP, IGMP y OSPF.

10. Abra el *Decodificador* y capture tráfico por *15* minutos. Posteriormente guarde este archivo en la carpeta C:\My Documents\Archivos de Datos\Practica No 8 con un nombre dado (Ejem: Decode Router Telecom).

B. Captura de tráfico para el enlace WAN con el proveedor de acceso a Internet Orbitel.

Los equipos de datos al igual que el enlace de Telecom se encuentran ubicados en el CC5 y la velocidad de línea soportada por el par de cobre activo entre los módems HDSL es 1536 Kbps. El enrutador Cisco 3600 se encuentra conectado al Accelar 1200 en el puerto 14 del módulo XLR1216TX, Ver Figura 2.73.

11. Una vez terminada la captura de tráfico con el enlace de Telecom, elimine el filtro anteriormente creado, vaya a la pestaña *Log* en la ventana de configuración principal del Advisor y rehabilite todas las casillas de verificación *On/Off*, luego cambie el nombre del archivo, fecha y periodo de medición.

NOTA: Este archivo al igual que todos los capturados en esta práctica deben ser almacenados en la carpeta C:\My Documents\Archivos de Datos\Practica No 8.

12. Ejecute los pasos 8, 9 y 10. Para el paso 8 cambie el campo *MirroredPortOne* al valor 1/14 (Slot 1/ Puerto 14).

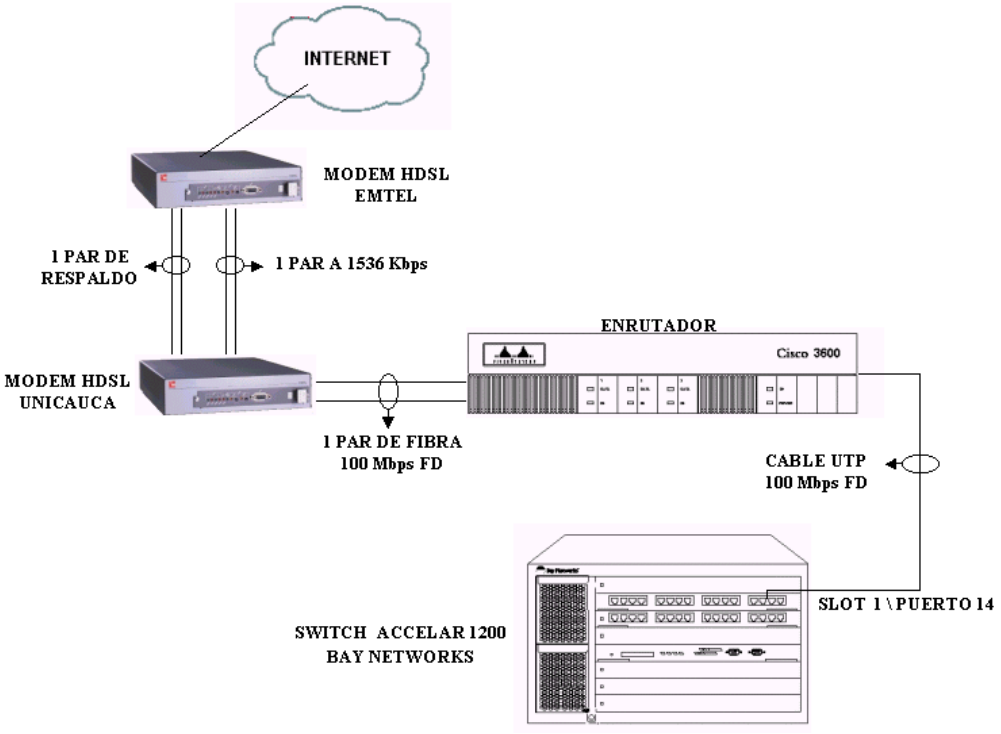


Figura 2.73. Enlace WAN Orbitel.

C. Captura de tráfico para el servidor de correo electrónico Atenea.

13. Terminada la captura de los datos elimine el filtro, seleccione la pestaña *Interface/Protocols* de la ventana de configuración principal del Advisor y digite en el campo *Monitor Period* (hhh:mm) el valor 000:30.

14. Seleccione la pestaña *Log* de la ventana de configuración principal, habilite las casillas *On/Off* para cada una de las medidas que aparecen bajo la columna *Data Type*, escriba en el campo *Interval (hhh:mm:ss)* 000:00:30 y en el campo *Period (hhh:mm)* 000:30. En File *Name* proporcione la ruta y el nombre para el archivo (Ejem: Atenea 2) y en *Description* consigne la fecha y hora de la medición.

15. Ejecute el paso 8 cambiando el campo *MirroredPortOne* al valor 1/12 (Slot 1/ Puerto 12).

NOTA: El servidor e-mail Atenea tiene una tarjeta de red con dos interfaces, una para la Intranet (Atenea 2) y la sobrante para el acceso externo (Atenea 1).

16. Finalizada la captura de los datos del servidor Atenea, repita el mismo procedimiento para los siguientes puertos del switch Accelar 1200:

- Puerto 9/Slot 1 (Servidor web interno)
- Puerto 8 /Slot 1 (DNS Hércules)
- Puerto 11/Slot 1 (Proxydom Orbitel)
- Puerto 7/Slot 3 (Enlace Backbone Ingenierías)

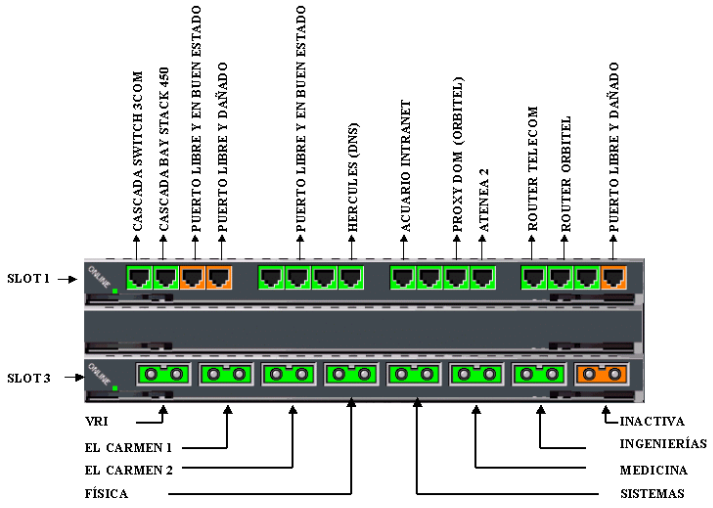


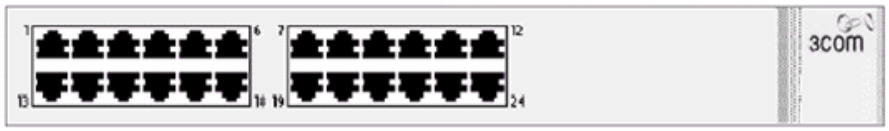
Figura 2.74. Distribución y asignación de puertos Accelar 1200 Red de Datos.

17. Cuando se hayan tomado todas las medidas con el Accelar 1200, seleccione el menú *Edit* de la barra principal del Accelar Device Manager, escoja la opción *Diagnostics* y luego seleccione la pestaña *Port Mirror*. Realice la siguiente configuración:

- *Enable*: false
- *MirrorPort:* 1/6 (Slot 1/ Puerto 6)- Puerto Espejo
- *EnableMirroredPortOne*: false

- *MirroredPortOne*: 3/7 (Slot 3/ Puerto 7)
- *EnableMirroredPortTwo:* false
- *MirroredPortTwo:* 0
- *SaveConfig*: true. Presione *Apply*, luego *Save Configuration* en la barra de herramientas del Accelar Device Manager y cierre el software.

D. Captura de tráfico en el switch 3COM 3300XM Red de Datos.



Puerto (Puerto Monitor)	Servidores Conectados
4	Odín (ftp)
9	Proxying (Orbitel)
10	Afrodita (E-mail y DNS Externo)
11	Proxyres (Telecom)
12	Proxysis (Telecom)

Figura 2.75. Distribución y asignación de puertos switch 3COM 3300XM Red de Datos.

18. Desconecte el extremo del cable RJ-45 100Base-TX unido al puerto 6 del módulo XLR 1216TX en el Accelar 1200 y conéctelo a uno de los puertos libres del switch 3300XM (Ejm: Puerto 5).

19. Desde la estación de trabajo ejecute el Internet Explorer y consigne en el campo de localización del browser la dirección IP del equipo, así: *http://10.1.13.204/* con la finalidad de gestionar el switch vía web.

20. Consigne el *login* y *password* necesarios para obtener privilegios de administrador (**Deben ser preguntados al Ingeniero responsable de dicho equipo**). Presione el ícono *Configuration* y luego el vínculo *Roving Analysis Port*.

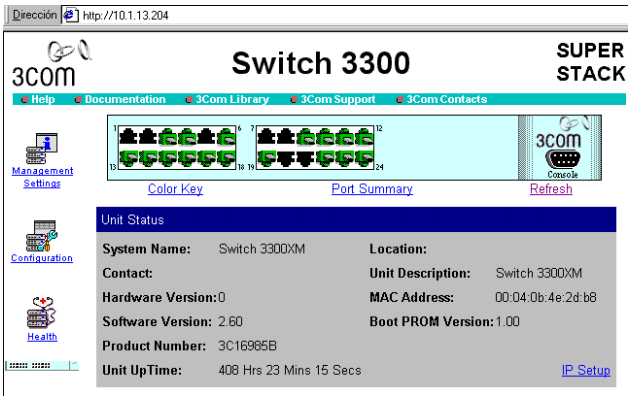


Figura 2.76. Interfaz de gestión web switch 3COM 3300XM Red de Datos.

21. En la caja de lista *Roving Analysis State* seleccione la opción *Enabled*, luego *Unit 1 Port 5* del área *Analysis Port* (Puerto al cual se conecta el Internet Advisor) y *Unit 1 Port 4* del área *Monitor Port* (Puerto a monitorear). Presione *Apply* para hacer efectivos los cambios.

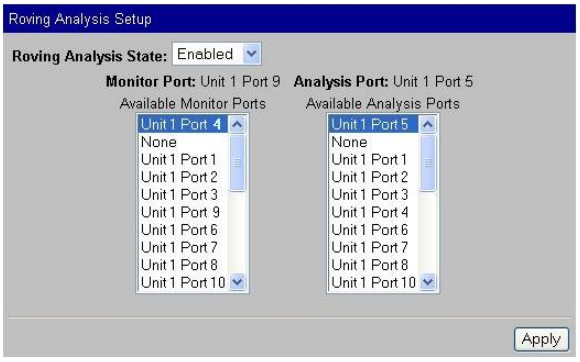


Figura 2.77. Configuración del puerto espejo para Odín.

22. En el Advisor seleccione la pestaña *Log* de la ventana de configuración principal y habilite las casillas *On/Off* para cada una de las medidas que aparecen bajo la columna *Data Type*. En *File Name* proporcione la ruta y el nombre para el archivo (Ejem: Odín) y en *Description* consigne la fecha y hora de la medición. Inicie las medidas en el Advisor.

23. Repita los pasos 21 y 22 para *Proxying* (Orbitel), *Proxyres/Proxysis* (Telecom) y A*frodita*.

24. Al terminar las medidas con el switch 3COM 3300XM, *deshabilite* la funcionalidad *Roving Analysis Port* restableciendo la *configuración original*, así:

- *Roving Analysis State:* Disabled
- *Monitor Port:* None
- *Analysis Port:* None. Presione *Apply* y cierre el browser.

E. Análisis de los proveedores de acceso a Internet.

P 8.1. Conforme a los datos capturados para ambos enlaces, consigne los valores en la siguiente tabla:

Tabla 2.37. Estadísticas Accesos WAN Orbitel y Telecom.

NOMBRE DE LA ESTADÍSTICA	AVERAGE		PEAK		*THRESHOLD EXCEEDED	
	Telecom	Orbitel	Telecom	Orbitel	Telecom	Orbitel
Utilización (% de la Capacidad).						
Colisiones Locales y Remotas (% de Tramas).						
Colisiones Tardías Locales y Remotas (% de Tramas).						
Broadcast (% de Tramas).						
Multicast (% de Tramas).						

***** Es el número de veces que se ha sobrepasado el nivel umbral para la estadística señalada.

Responda las siguientes preguntas:

P 8.2. ¿La utilización promedio para los enlaces de acuerdo a la *tecnología empleada* está dentro del límite recomendado?

P 8.3. Un alto porcentaje de colisiones. ¿Qué problemas representan para el enlace?

P 8.4. Analice los niveles de tráfico Multicast y Broadcast para los enlaces y determine si dichos valores se encuentran dentro del rango especificado de acuerdo a la tecnología empleada.

P 8.5. Determine el porcentaje de tramas y de bytes con respecto al total de ellas para cada stack de protocolos, el porcentaje de los protocolos IP y la utilización promedio del medio para los stacks indicados en la siguiente tabla.

Tabla 2.38. Tendencias de los protocolos para los Accesos WAN Orbitel y Telecom.

Stack / Protocolos	Utilización (%)		Tramas (%)		Bytes (%)	
	Telecom	Orbitel	Telecom	Orbitel	Telecom	Orbitel
IP						
WWW						
ICMP						
FTP 20, 21						
ARP / RARP						
SMTP 25						
DNS 53						
NetBIOS 137 – 139						
POP3 110						
RIP						
Igmp						
Puerto TCP/UDP 22						
RPC						
SNMP 161,162						
BOOTP						
Telnet 23						
Proxy Nexus 3128						
Novell						
NetBEUI						
Otros						

P 8.6. De acuerdo a la información de la tabla, ¿Qué servicios o aplicaciones que presta actualmente la Red de Datos de la Universidad del Cauca son los más utilizados?

P 8.7. ¿Los protocolos encontrados y el nivel de utilización corresponden con los esperados teniendo en cuenta la naturaleza de la Red y los servicios que ésta presta?

P 8.8. Realice una comparación entre los dos enlaces a nivel de utilización y servicios.

P 8.9. Haciendo uso de la medida *Estadísticas de Conexión* determine los cinco nodos que generan la mayor cantidad de tráfico y retransmisiones tanto en transmisión como recepción.

P 8.10. Agrupe las conexiones por *subredes* y ubique las siguientes: 172.16.0.0 (Intranet), 200.30.71.0 (Orbitel) y 200.21.83.0 (Telecom). Para cada una de éstas determine las *tres subredes* con las que se cursa la mayor cantidad de tráfico.

25. Abra el archivo *Decodificador* para ambos enlaces y responda las siguientes preguntas:

P 8.11. ¿Qué tipos de protocolos de enrutamiento se observaron y que versiones tienen?

P 8.12. ¿Qué protocolo de transporte utiliza RIP y cual es el número de puerto?

P 8.13. ¿Cuáles son las direcciones de multidifusión que se observan para IGMP?

P 8.14. Determine para RIP:

- Número de saltos de cada ruta o enlace.
- El tiempo entre cada actualización de las tablas de ruta. ¿Concuerda con el valor teórico?

F. Análisis para DNS, WEB, FTP, E-MAIL y PROXYS.

Conforme a los archivos capturados para el conjunto de EQUIPOS responda las siguientes preguntas.

P 8.15. Realice un diagrama de columnas cuyos ejes sean *Utilización Promedio* vs *Proxy* y analice los resultados para el periodo de medida.

P 8.16. Ejecute el paso anterior para los servidores DNS, WEB, FTP y E-MAIL.

P 8.17. Compare el tráfico Unicast, Multicast y Broadcast para el conjunto de equipos.

P 8.18. Determine aproximadamente el promedio de conexiones y estaciones activas para el conjunto de equipos. ¿Cuál aplicación o servicio presenta más retransmisiones?

P 8.20. Analice con profundidad los protocolos observados a nivel de IP y determine si su nivel de utilización reflejan el tipo de servicio para el cual cada uno de estos equipos está configurado.

- **CONCLUSIONES**

2.3. ENTORNO ACCESO TELEFÓNICO REMOTO

2.3.1. Práctica No 9. Análisis del Acceso Primario RDSI Red de Datos Universidad del Cauca

- **OBJETIVOS:**

- Utilizar el módulo PRI J2296B E1/ISDN SIM para el monitoreo del acceso remoto a la Red de Datos de la Universidad del Cauca.
- Emplear la herramienta software WAN ISDN D-Channel Analysis en modo de monitoreo.
- Comparar los resultados obtenidos con la teoría acerca de RDSI en los niveles de enlace y red.
- Reconocer los componentes, fases de operación y formato de trama del protocolo Punto a Punto.

- **MARCO TEÓRICO**

RDSI: Según la definición acogida por UIT (Norma I.110) una Red Digital de Servicios Integrados es una red que ha evolucionado en general a partir de la Red Digital Integrada (RDI) para telefonía y que proporciona una conectividad digital de extremo a extremo para apoyar una amplia gama de servicios vocales y no vocales, a los cuales los usuarios tiene acceso mediante un conjunto limitado de interfaces polivalentes normalizadas usuario-red.

GRUPOS FUNCIONALES Y PUNTOS DE REFERENCIA: Los grupos funcionales son conjuntos operacionales con funciones residentes en uno o más equipos de la RDSI. Para evitar cualquier confusión entre éstos y el equipo físico, la UIT emplea la expresión puntos de referencia para designar los límites entre los grupos, es decir, son puntos teóricos que pueden corresponder o no a interfaces físicas existentes.

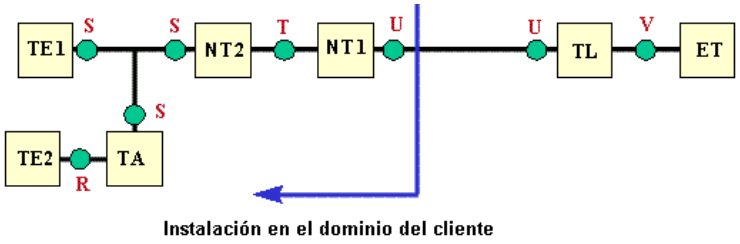


Figura 2.78. Configuración de referencia para RDSI.

Los grupos funcionales son:

- *TE2 (Equipos Terminales Clase 2):* Son aquellos periféricos que utilizan las actuales interfaces y protocolos no-RDSI. Precisan de un adaptador de terminal para poder acceder a la red. Por ejemplo, un teléfono analógico tradicional.
- *TE1 (Equipos Terminales Clase 1):* Son periféricos que integran de forma nativa los protocolos RDSI y pueden conectarse directamente a la interfaz S y T. Por ejemplo, un teléfono digital o una tarjeta adaptadora para PC.
- *TA (Adaptador de Terminal):* Permite la conexión de los ET2 a la RDSI actuando como conversor de protocolos V.24 o X.21 en la señalización RDSI.
- *NT2 (Terminador de Red Clase 2):* Equipo de usuario que realiza las funciones de tratamiento y multiplexación de los protocolos de nivel 2 y 3, conmutación, concentración, y mantenimiento. Por ejemplo, una centralita PBX.
- *NT1 (Terminador de Red Clase 1):* Localizado en casa del abonado y es el responsable de ejecutar funciones de bajo nivel como terminación, mantenimiento y control de la línea de transmisión digital, temporización, transferencia de alimentación de potencia y multiplexación de nivel 1. Presenta el final de la conexión física que monitorea el acceso a la red.
- *LT (Terminador de línea):* Hace referencia a los equipos del proveedor que suministran al usuario una línea a través de una interfaz U.
- *ET (Terminador de conmutación):* El bloque engloba los elementos que efectúan la conexión del equipo del proveedor a la red telefónica.

Los puntos de referencia son:

- *R:* Permite la conexión de dispositivos no RDSI (Interfaz telefónico actual). Puede ser un interface RS-232 (o V24) o un interface digital X.21
- *S:* Subscriber es el punto de acceso universal a la red para los terminales con RDSI nativo. Puede coincidir o incluir al punto T.
- *T:* Interfaz entre NT1 y NT2. Separa el bucle de abonado de la instalación propia del usuario.
- *U:* Se puede considerar actualmente como el límite entre las instalaciones del usuario y la administración RDSI.
- *V:* Interfaz dentro de la central. Pertenece a la implementación propia de la compañía operadora.

CANALES DE TRANSMISIÓN: La RDSI dispone de distintos tipos de canales para el envío de información de voz, datos y control.

Tabla 2.39. Tipos de Canal RDSI.

Tipo	Función	Velocidad
B	Servicios básicos	64 Kbps.
D	Señalización	16 Kbps. (BRI) 64 Kbps. (PRI)
H_0	6 canales B	384 Kbps. (PRI)
H_1	todos los canales H0 H_{10} (23B) H_{11} (24B) H_{12} (30B)	 1472Kbps 1.536 Kbps. (PRI) 1.920 Kbps. (PRI)
H_2	RDSI de banda ancha H_{21} H_{22}	(propuesta actual) 32.768 Kbps. 43-45 Mbps.
H_4	RDSI de banda ancha	132-138,240 Mbps.

- **Canal B:** Los canales tipo B transmiten información a 64Kbps y se emplean para transportar cualquier tipo de información de los usuarios, bien sean datos de voz o datos informáticos. Estos canales no transportan información de control de la RDSI pero si de temporización. Este tipo de canales sirve además como base para cualquier otro tipo de canales de datos de mayor capacidad, que se obtienen por combinación de canales tipo B. La velocidad de 64Kbps permite enviar datos de voz con calidad telefónica. Considerando que el ancho de banda telefónico es de 4KHz, una señal de esta calidad tendrá componentes espectrales de 4KHz como máximo, y según el teorema de muestreo se requerirá enviar muestras a una frecuencia mínima de $2 \cdot 4KHz = 8KHz = 8000$ muestras por segundo, es decir, se enviará un dato de voz cada 125µseg. Si las muestras o datos de voz son de 8 bits, como es el caso de las líneas telefónicas digitales, se requerirán canales de $8 \cdot 8000$ bps = 64Kbps.

- **Canal D:** Los canales tipo D se utilizan principalmente para enviar información de control de la RDSI, como es el caso de los datos necesarios para establecer o terminar una llamada. Por ello también se conoce un canal D como "canal de señalización". Los canales D también pueden transportar datos cuando no se utilizan para control. Estos canales trabajan a 16Kbps o 64kbps según el tipo de servicio contratado.

- **Canales H:** Combinando varios canales B se obtienen canales tipo H que sólo transportan datos de usuario pero a velocidades mucho mayores. Por ello se emplean para información como audio de alta calidad o vídeo. Hay varios tipos de canales H como H0 que trabajan a 384Kbps (6 canales B), H10 que trabajan a 1472Kbps (23 canales B), canales H11 que trabajan a 1536Kbps (24 canales B) y canales H12 que trabajan a 1920Kbps (30 canales B).

MODOS DE ACCESO: Un usuario puede contratar dos accesos diferentes con el proveedor telefónico según sus necesidades.

- *Acceso básico o BRI (Basic Rate Interface):* Proporciona dos canales B y un canal D de 16Kbps multiplexados a través de la línea telefónica. De esta forma se dispone de una velocidad total de 144Kbps. Es el tipo de acceso que encaja en las necesidades de usuarios individuales.

- *Acceso primario o PRI (Primary Rate Interface):* En EE.UU. suele tener 23 canales tipo B y un canal D de 64Kbps, alcanzando una velocidad global de 1536Kbps. En Europa el PRI consiste de 30 canales B y un canal D de 64Kbps, alcanzando una velocidad global de 1984Kbps. En el segundo caso, los canales B también pueden estar agrupados como 5 canales H0 o un canal H12.

Tabla 2.40. Estructuras de los Accesos BRI y PRI.

Interfaz	Estructura	Velocidad Interfaz Física	Velocidad disponible
BRI	2B + D16	192 Kbps.	144 Kbps.
PRI	23B + D64 30B + D64	1.544 Kbps. 2.048 Kbps.	1.536 Kbps. 1.984 Kbps.

SERVICIOS RDSI: Se distinguen tres grandes grupos de servicios, a título meramente enunciativo y no limitativo:

- **Servicios Básicos o Portadores:** Proporcionan los medios básicos para permitir el tráfico de la información, sin alterar su contenido, entre dos puntos de la red y en tiempo real.

  A. *Conmutación de circuitos:* Tráfico de datos a 64 Kbps, conversación telefónica, servicio de audio a 3,1 Khz, simultaneidad de datos y voz (2 o más canales B), tráfico de datos a

384 Kbps, tráfico de datos a 1.536 Kbps o 1.920 Kbps, backup digital de líneas punto a punto.

B. *Conmutación de paquetes:* Circuitos conmutados y circuitos virtuales permanentes, señalización de usuario.

- **Teleservicios:** Utilizan los servicios portadores e implementan niveles superiores de comunicación y pueden ser ofrecidos tanto por la compañía operadora como por terceras empresas. Pertenecen a esta categoría la telefonía (Conversación a 3,1 KHz), videoconferencia, teletexto, telefax, modo mixto (Teletexto y fax grupo 4 combinados), videotexto, télex, vigilancia y seguridad remota, aplicaciones médicas (Transferencia de rayos X, telemedicina, ultrasonidos y scanners), transmisiones de radio de alta calidad de audio, trabajo desde el hogar, servicios de telefonía integrados con ordenador.

- **Servicios suplementarios:** También se denominan Servicios de Valor Agregado y modifican o amplían las características de los Accesos de Usuario en Banda Estrecha. Entre ellos se encuentran la Presentación/Restricción del iniciador de la llamada, presentación/restricción de la línea conectada, aviso de cargo, llamada en espera, grupo cerrado de usuarios, etc.

PROTOCOLO LAP D: El nivel de enlace es responsable de la transmisión de información libre de errores a través del medio físico. En RDSI este nivel emplea principalmente el protocolo LAP-D (Link Access Protocol o protocolo de acceso al enlace) para el canal D. LAP-D es un subconjunto del protocolo HDLC. Por otro lado, los protocolos para los canales B son escogidos por los usuarios. La función principal de LAP-D es transmitir los mensajes de nivel superior necesarios entre los equipos del usuario y la central telefónica para establecer una llamada. Con esta llamada se establece también un circuito o camino virtual a través de la red entre el usuario origen y el destino. El nivel de enlace proporciona los siguientes servicios al nivel superior (nivel de red):

- *Servicio orientado a conexión con transferencia de información confirmada*. La información de nivel superior se envía como tramas numeradas. Esto permite recuperar errores mediante retransmisión de tramas. Se utiliza para transmitir los mensajes relativos al establecimiento de una llamada.
- *Servicio sin conexión con transferencia de información no confirmada*. La información de nivel superior se envía como tramas no numeradas. En casos de errores en la recepción de una trama, simplemente se ignoran ésta. Se emplea para transferir mensajes relativos a la gestión del enlace.

- *Servicios de administración.* Son proporcionados a través de una serie de primitivas de servicio y cumplen diversas funciones, entre las que se destacan la gestión del mecanismo que permite identificar los equipos específicos dentro del bus S/T asociado a una conexión RDSI. Este mecanismo se basa en incorporar en el campo de dirección de una trama LAP-D dos subdirecciones: el identificador de acceso a servicio o SAPI (Service Access Point Identifier) y el identificador de extremo terminal o TEI (Terminal Endpoint Identifier). El primer valor identifica la clase de servicio con que se relaciona el terminal o equipo del usuario (voz, datos, voz y datos), y el segundo valor especifica de manera única el terminal. Además es posible especificar una dirección *broadcast* o de radiodifusión (valor TEI cuyos bits están todos a uno), para que la trama llegue a todos los equipos del usuario destino. El identificador de un terminal se puede asignar al instalar el terminal (asignación fija) o de forma automática cuando el terminal se activa (asignación dinámica). Cabe señalar que este método de direccionamiento del equipo destino sólo tiene significado local en la parte del usuario, y es totalmente transparente a la gestión que la red hace de las tramas.

TRAMA LAP-D: La trama está limitada por dos bytes de bandera que tienen el valor binario 01111110. En el resto de campos de la trama no se admite dicho valor y en cualquier dato que tenga más de cinco unos seguidos se intercalará un 0 después del quinto uno antes de ser transmitido. Este cero será suprimido en el receptor. Todo esto no es más que es el mecanismo de transparencia de HDLC.

Figura 2.79. Formato de trama LAP-D.

Tras la bandera inicial está el campo de dirección, formado por dos bytes. El campo SAPI identifica la clase de servicio con que se relaciona el terminal o equipo del usuario y el campo TEI especifica de manera única el terminal. El bit C/R (Command /Response) especifica si la trama es un comando o una respuesta. La red debe enviar órdenes con C/R a 1 y respuestas con C/R a 0. El equipo de usuario debe actuar al contrario. El bit EA0 indica si el campo de dirección contiene el byte adicional de TEI (a 0) o no (a 1). EA1 es como EA0, pero para LAP-D vale 1.

Figura 2.80. Formato del campo de dirección de la trama LAP-D.

Tabla 2.41. Asignación de valores SAPI.

VALOR SAPI	DESCRIPCIÓN
0	Procedimiento de control de llamada
1	Datos modo paquete conforme a procedimiento de la norma Q.931
2 – 15	Reservados para normalización futura
16	Comunicación de paquetes conforme a procedimiento de nivel 3 dela norma X.25
17 – 61	Reservados para normalización futura
62	Prueba y mantenimiento
63	Procedimiento de gestión de la capa 2

Tabla 2.42. Asignación de valores TEI.

VALOR TEI	DESCRIPCIÓN
0 – 63	Para un TE de asignación fija o no automática
64 – 126	Para una asignación dinámica o automática
127	Difusión

Tras el campo de dirección viene un campo de control, que identifica el tipo de trama y donde es aplicable, el número de secuencia de emisión y el número de secuencia de recepción. Este campo es igual al de control de una trama HDLC y ocupa 2 bytes. Se especifican tres tipos de formatos para este campo:

- *Tramas I*: Son tramas comando de información numeradas módulo 128, o sea, van de la 0 a la 127. Estas tramas contienen datos de la capa de red en el campo de información y exigen un acuse de recibo de la capa de enlace de datos.
- *Tramas S*: Son tramas de supervisión y se emplean para indicar al terminal remoto el número de trama I recibida y alguna acción. Pueden se tramas comando o respuesta.

- *Tramas U:* Son tramas de información no numerada y funciones de control. Con ellas se puede transferir información contenida en el campo de información sin acuse de recibo o bien desempeñarán funciones de control en cuyo caso, no contienen campo de información. Están codificadas con un solo byte.

Para las tramas de tipo I, en el campo de control se especifica el número de secuencia de emisión de trama (conocido como N(S)), con el que se numeran las tramas emitidas de 0 a 127. Por otra parte, para tramas tipo I y tipo S, también se especifica el número de secuencia de recepción (conocido como N(R)). Con este valor la entidad de nivel de enlace que transmite la trama confirma las tramas I numeradas hasta el valor indicado. El campo de control también incluye un bit conocido como bit P/F. En tramas de órdenes (Poll) este bit es fijado a 1 por el nivel de enlace para indicar al receptor que debe confirmar con una respuesta. En las tramas de respuesta (final) el bit se pone a 1 para contestar una trama de orden del tipo anterior.

El campo de información de la trama LAP-D contiene los datos de la comunicación a nivel de Red. Finalmente, la trama incorpora un campo CRC que permite al receptor un chequeo de errores. Se utiliza para este campo un código de redundancia cíclica de 16 bits.

NIVEL DE RED: Este nivel es responsable del establecimiento, mantenimiento y terminación de las conexiones para canales D y B, y además proporciona las funciones de direccionamiento. Toda la información intercambiada entre los niveles pares de red del equipo origen y destino va colocada en el campo de información de tramas de nivel de enlace siguiendo el formato de la Figura 2.81. Este nivel se especifica en las series de normas I.450/1 y Q.930-39 de la ITU.

El campo *discriminador de protocolo* identifica el protocolo del nivel de red empleado. Este puede ser el especificado por la ITU, una versión nacional u otro protocolo como el X.25. El segundo campo útil especifica la *longitud* del campo *referencia de llamada*. Este último identifica unívocamente cada llamada en la interfaz local entre usuario y red. Su valor es asignado al comienzo de una llamada por el origen y queda disponible para otra llamada cuando finaliza la llamada en curso. De esta forma, a nivel de enlace se identifica un *TE* del usuario con el valor *TEI*, pero a nivel de red, a ese TE pueden llegar diferentes llamadas identificadas por distintas referencias de llamada. El campo tipo de mensaje indica el papel del mensaje en el proceso de llamada incluyendo el establecimiento y la desconexión de la misma. Según el tipo de mensaje puede requerirse información adicional, la cual se envía en el campo elementos de información prioritario y opcional.

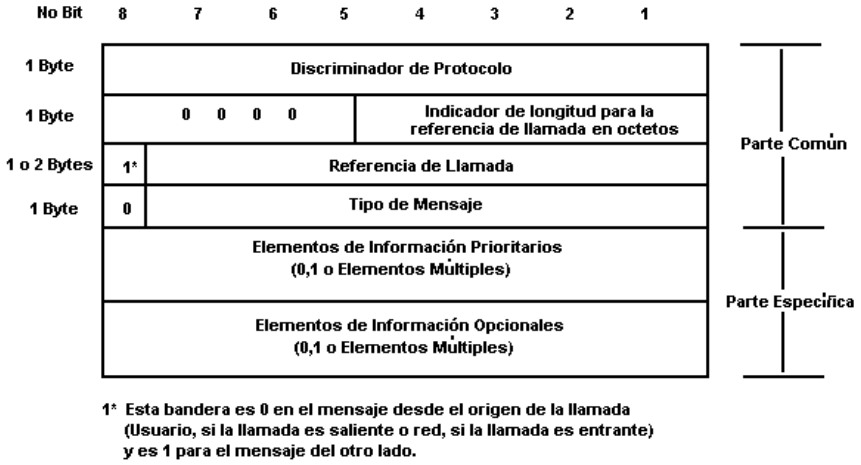


Figura 2.81. Estructura del mensaje de nivel 3 o formato campo de información trama LAP-D.

- **EQUIPO UTILIZADO**
  - Internet Advisor WAN HP J2300D
  - Cuatro cables coaxiales de 75 Ohms
  - Módulo de Interfaz J2296B E1/ISDN SIM BNC
  - Modem HDSL Pair Gain Proveedor EMTEL
  - RAS MAX 6000
  - Dos T BNC hembras
  - Cable Y- RS 232/V.24
  - Modem Externo
  - Computador Personal
  - Línea Telefónica Directa que se encuentra en la oficina 319: Grupo I+D de Nuevas Tecnologías en Telecomunicaciones.

- **PROCEDIMIENTO**

A. Captura de información.

La Red de Datos de la Universidad del Cauca para proveer el servicio de Internet a sus usuarios externos tiene contratado un acceso PRI a 2048 Kbps con la empresa EMTEL a través de un par de módems HDSL Pair Gain como los utilizados para los enlaces WAN. El módem HDSL en el CC5 se conecta a un puerto PRI WAN ISDN RJ 48 hembra del MAX 6000 como se muestra en la siguiente figura. Cuando un usuario externo desea conectarse a Internet, realiza una llamada a EMTEL el cual le

asigna un canal B de los 30 disponibles para establecer la comunicación con el MAX 6000, éste pide el *login* y el *password* para validarlo con ayuda de un *servidor de autenticación* y luego le asigna una *dirección IP al usuario externo*.

La configuración actual de esta conexión se presenta a continuación:

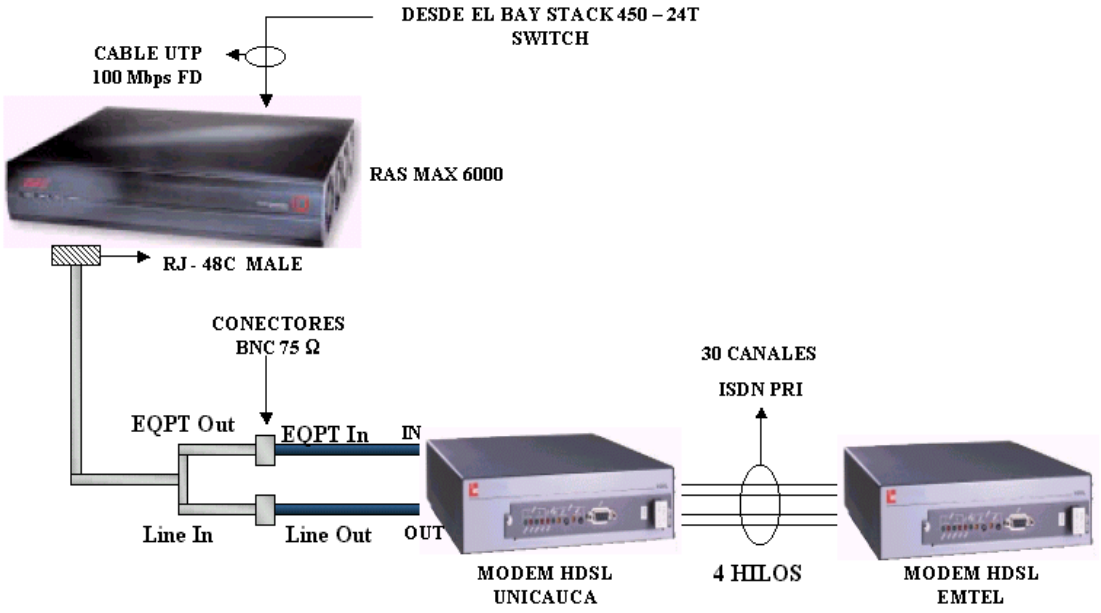


Figura 2.82. Acceso Remoto Red de Datos Universidad del Cauca.

1. Encienda el Internet Advisor y conecte *directamente* los cuatro cables coaxiales **(Como lo indican las etiquetas en los extremos)** a los conectores BNC del módulo RDSI. *Reconozca* la conexión entre el MAX 6000 y el módem HDSL, ábrala y proceda a conectar *exactamente* los cuatro extremos restantes de los cables como lo indica la siguiente figura. Procure no gastar más de 2 minutos.

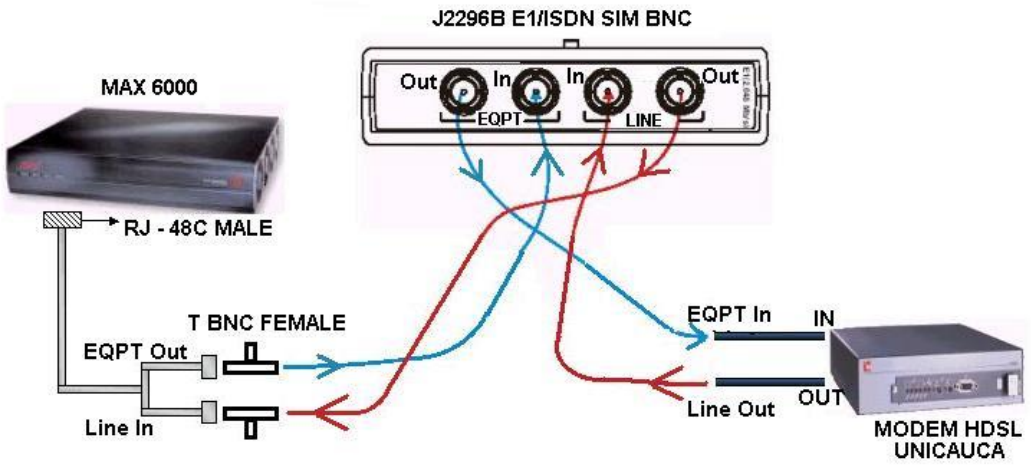


Figura 2.83. Conexión puenteada para monitoreo E1.

2. Para el módem HDSL verifique que los leds de sincronismo se encuentren en *verde* y los leds de alarma estén *apagados.* Para el MAX 6000 los leds POWER y DATA deben estar en *verde* y el led ALARM *apagado.*

A.1. Análisis de tramas de canal D:

3. Entre al software WAN para *análisis de tramas de canal D* mediante la siguiente ruta: | Start | Internet Advisor | WAN Analysis | ISDN D Channel Analysis | Etsi (E1, BRI –ST, U) | Monitor | Analysis of D Channel Frames |.

4. Abra la ventana de configuración principal desde la barra de herramientas y seleccione la pestaña *Interface/Protocols*. En la caja de lista *Interface Type* escoja la opción *E1* (Acorde con el Módulo de Interfaz) y luego presione el botón *Configuration*. En la caja de lista *Receiver Mode* seleccione la opción *Bridged* y posteriormente presione *OK*.

5. Seleccione la pestaña *Log*, habilite las casillas *On/Off* para cada una de las medidas que aparecen bajo la columna *Data Type*, escriba en el campo *Interval (hhh:mm:ss)* 000:01: 00 y en el campo *Period* (hhh:mm) 000:30. En *File Name* escoja mediante el botón *Browse* la siguiente ruta C:\My Documents\Archivos de Datos\Practica No 9\ y proporcione un nombre descriptivo para el archivo (Ejem: Análisis de tramas de canal D). En *Description* consigne la fecha y hora de la medición.

NOTA: Este archivo al igual que todos los capturados en esta práctica deben ser almacenados en la carpeta C:\My Documents\Archivos de Datos\Practica No 9.

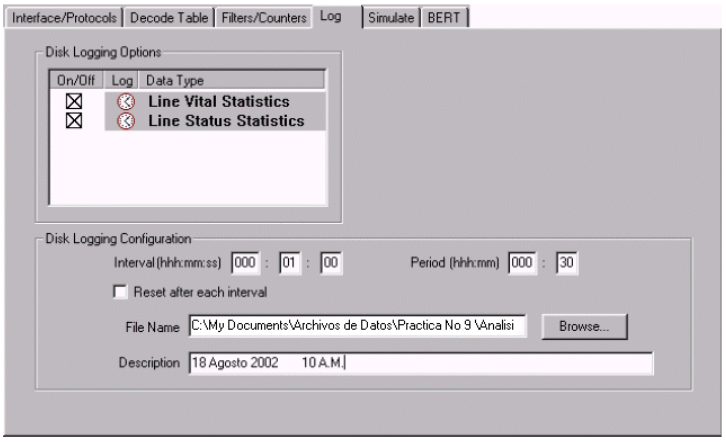


Figura 2.84. Configuración pestaña Log para la medida Análisis de Tramas de Canal D.

6. Inicie la medida. Durante los 30 minutos que dura la captura de la información verifique de forma periódica el estado del sincronismo del enlace en ambos lados (Equipo y Línea) a través de la herramienta *Estado de Línea*. Los leds software *Signal* y *Frame Sync* tanto para el equipo como para la línea *deben estar en verde*.

7. Una vez finalizada la captura de los datos, abra el menú *File* y escoja la opción *Save*. Deshabilite todas las casillas de verificación debajo de la columna *On/Off* excepto la correspondiente al *Decodificador* y guarde dicho archivo con otro nombre dentro de la misma carpeta donde almacenó el registro anterior. Cierre la aplicación.

A.2. Análisis de llamadas ISDN (Seguimiento de canal B):

8. Entre al software WAN para *análisis de llamadas ISDN* mediante la siguiente ruta: | Start | Internet Advisor | WAN Analysis | ISDN D Channel Analysis | Etsi (E1, BRI –ST, U) | Monitor | Analysis of ISDN Calls (B – Channel Tracker) |. Luego realice los pasos 5, 6, 7 y 8.

A.3. Análisis de tramas LAPD:

9. Entre al software WAN para *análisis de tramas LAP D* mediante la siguiente ruta: | Start | Internet Advisor | WAN Analysis | ISDN D Channel Analysis | Etsi (E1, BRI –ST, U) | Monitor | Analysis of LAPD Frames |. Luego realice los pasos 5, 6, 7 y 8.

A.4. Análisis de causas de desconexión Q.931:

10. Entre al software WAN para *análisis de causas de desconexión Q.931* mediante la siguiente ruta: | Start | Internet Advisor | WAN Analysis | ISDN D Channel Analysis | Etsi (E1, BRI –ST, U) | Monitor | Analysis of Q.931 Disconnect Causes |. Luego realice los pasos 5, 6, 7 y 8.

A.5. Análisis de tipos de mensajes Q.931:

11. Entre al software WAN para *análisis de tipos de mensajes Q.931* mediante la siguiente ruta: | Start | Internet Advisor | WAN Analysis | ISDN D Channel Analysis | Etsi (E1, BRI –ST, U) | Monitor | Analysis of Q.931 Message Types |. Luego realice los pasos 5, 6, 7 y 8.

B. Análisis de la información.

P 9.1. Para el acceso remoto a la Red de Datos de la Universidad del Cauca realice un diagrama en bloques similar a la Figura 2.78 donde se distingan claramente los puntos de referencia y grupos funcionales de acuerdo a la funcionalidad de cada uno de los dispositivos que intervienen en la conexión.

12. Abra el archivo almacenado correspondiente a la *medida análisis de tramas de canal D.*

P 9.2. Para los mensajes de nivel tres presentados en la medida *Estadísticas de Filtros y Contadores* que hayan tenido algún tipo de conteo, consulte su *tipo* (Establecimiento de llamada, liberación de llamada, fase de llamada, liberación y mensajes diversos), su *funcionalidad* y su *codificación* en binario.

P 9.3. ¿Por qué los mensajes de red TEI (Request, Assign, Denied, Check y Remove) no se presentaron?

13. Abra el archivo *Decodificador* correspondiente a la medida anterior.

P 9.4. Determine la estructura de nivel tres para el mensaje Establecimiento (SETUP). ¿Concuerda con el formato teórico establecido?. ¿Qué modo de conmutación se está empleando?. ¿Qué tipo de servicio portador utiliza la Universidad del Cauca?. ¿Cuál es la clase de compresión usada en las conexiones?

P 9.5. Empleando el *Decodificador*, realice un diagrama de secuencia donde se ilustre el intercambio de *mensajes a nivel de red* entre el MAX 6000 y la línea para el establecimiento y terminación de una llamada (Procedimiento de control de llamada por conmutación de circuitos). ¿Concuerda con el procedimiento teórico?

14. Abra el archivo almacenado correspondiente a la medida *análisis de llamadas ISDN*.

P 9.6. Durante la captura de los datos. ¿Cómo es el orden de asignación que realiza EMTEL para los canales B cuando se establecen las conexiones?

P 9.7. Realice una gráfica *Número de llamadas en sesión* Vs *Tiempo*, tomando muestras cada minuto y determine el promedio de llamadas establecidas durante la medida.

P 9.8. Ubique el último registro de la medida por medio del botón *Rec #*. Utilizando la estadística *Number of Call Setup Completed* realice una gráfica *Número llamadas completadas* Vs *Número de canal* para los 30 canales B. Establezca el promedio de llamadas atendidas por canal B y cuales fueron los más y menos utilizados.

P 9.9. ¿Por qué razón cuando se ocupan los canales se presenta un establecimiento de llamada de voz en lugar de una de datos?

P 9.10. ¿Cuál es el número telefónico que marca un usuario externo de la Universidad cuando desea conectarse a Internet a través de la Red de Datos de la Universidad del Cauca?

P 9.11. Observando las estadísticas *Number of Calls Attempted* y *Number of Call Setup Completed* para cada canal. ¿Cómo calificaría la disponibilidad de un canal?

15. Abra el archivo almacenado correspondiente a la medida *análisis de tramas LAP D.*

P 9.12. Para las tramas de nivel dos presentadas en la medida *Estadísticas de Filtros y Contadores* que hayan tenido algún tipo de conteo, consulte su *formato de pertenencia* (Información, supervisión y no numerada) y su *funcionalidad*, es decir, si actúan sólo como tramas comando, respuesta o de ambos tipos. Compare estos resultados con los capturados en el *Decodificador* de esta misma medida.

P 9.13. ¿Cómo es el valor del SAPI y TEI para las tramas decodificadas?

P 9.14. ¿Los mensajes de nivel tres están encapsulados dentro de un tipo especial de trama LAPD, cuál?

16. Abra el archivo almacenado correspondiente a la medida *análisis de causas de desconexión Q.931*.

P 9.15. Consulte la definición para las razones de desconexión que presenta la herramienta *filtros y contadores*.

NOTA: Los tipos de mensajes Q.931 ya fueron tenidos en cuenta en las anteriores medidas.

C. Captura de información del Protocolo Punto a Punto (PPP) sobre un acceso telefónico remoto.

17. Conecte el *módem externo* a cualquier *puerto serial* (DB-25 o DB-9) del PC, encienda el conjunto utilizando el cable *Y RS-232* e instale el software del módem en el PC.

NOTA: Si no hay disponibilidad de un puerto serial DB-25 en el PC, utilice un conversor DB-9 a DB-25.

18. En el PC vaya al ícono *Entorno de Red* y escoja *Propiedades*. Seleccione los *protocolos TCP/IP* que aparezcan y elimine cada uno de ellos. Ejecute el Internet Explorer y deshabilite las opciones que permiten navegar mediante *proxy*.

19. Conecte el *extremo sobrante* del cable *Y RS-232* a cualquiera de los puertos *RS-232/V.24* del Internet Advisor e igualmente enchufe el modem a la *línea telefónica directa* a través de un cable telefónico convencional (Conector RJ-11).

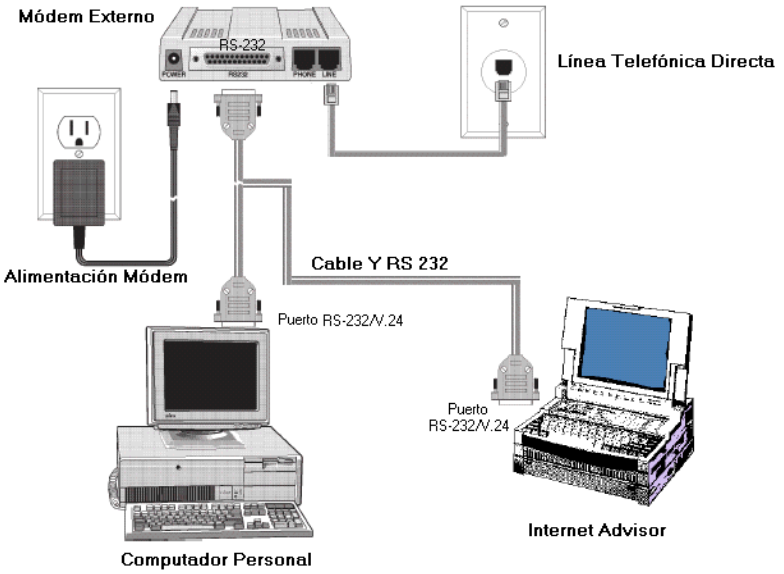


Figura 2.85. Conexión Internet Advisor para monitoreo PPP.

20. Encienda el Advisor y seleccione la prueba *Análisis de Protocolos LAN de Nivel de Red (Ethertype)* mediante la siguiente ruta: | Start | Internet Advisor | WAN Analysis | Asynchronous PPP Analysis (V Series) | Analysis of Network Layer LAN Protocols (Ethertype)|.

21. Seleccione la pestaña *Interface/Protocols*, de la caja de lista *Interface Type* escoja *RS-232/V.24* y de *Layer 2 Protocol* seleccione *RFC 1662*. Presione el botón *Configuration* y de las cajas de lista *Character Framing* y *Bits/Sec* elija las opciones *Async* y *19,200* respectivamente. Presione *OK*.

NOTA: Se seleccionó una tasa de 19200 bps ya que la velocidad de la conexión en el acceso a Internet empleando PPP depende de la capacidad del modem, la velocidad de transferencia del canal contratado y la tasa máxima de transferencia del puerto serial. Por tal razón, así el modem externo soporte hasta 56 Kbps la velocidad efectiva en la conexión estará restringida a la velocidad máxima del puerto serial.

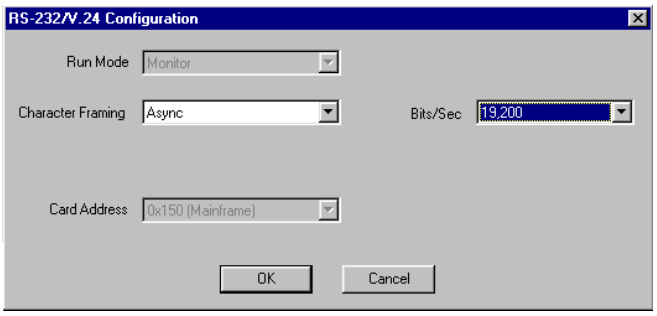


Figura 2.86. Configuración pestaña Interface/Protocols para monitoreo PPP.

22. Abra el *Decodificador* e inicie la captura de tráfico y en el PC configure una conexión con un ISP como Caucatel, EMTEL o Universidad del Cauca. Se requiere *login* y *password* con permisos de acceso telefónico.

23. Establezca la conexión a Internet, abra la página de la Universidad del Cauca y ejecute las siguientes operaciones: Leer correo y bajar un archivo pequeño del FTP. Cierre el browser y consulte nuevamente su correo con la Universidad empleando el programa SSH. Termine la conexión a Internet y detenga el *Decodificador* en el Advisor.

D. Análisis PPP.

Responda las siguientes preguntas:

P 9.16. Consulte como se define PPP, donde se utiliza y como está conformado.

P 9.17. Consulte el formato de trama para PPP de acuerdo a los documentos *RFC 1661* (The Point To Point Protocol) y *RFC 1662* (PPP in HDLC-like Framing). Describa sus diferencias, anote el tamaño en bytes para cada uno de los campos que conforman las tramas y determine los valores empleados por los campos de Dirección y Control en ambos formatos. ¿Cuál formato *aplica* en este caso de acuerdo a las tramas capturadas en el *Decodificador* y por qué?

P 9.18. Seleccione la primera trama en el *Decodificador* y determine el formato de un paquete perteneciente al *Protocolo de Control de Enlace (LCP)*. ¿Cuál es la funcionalidad de cada uno de sus campos?

P 9.19. Verifique en el *Decodificado*r que el campo *Protocol ID* de las tramas PPP se caracterizan porque *siempre* el bit menos significativo del byte menos significativo es 0 y el bit menos significativo del byte más significativo es 1. Consulte que ocurre si ésto no sucede.

P 9.20. ¿Cuáles son las tres *clases* de paquetes LCP que PPP maneja y que *tipos* se presentaron en la comunicación PC -ISP?

P 9.21. En el proceso de configuración, mantenimiento y terminación del enlace punto a punto, PPP pasa a través de diversas fases de operación, las cuales se pueden resumir en el siguiente esquema:

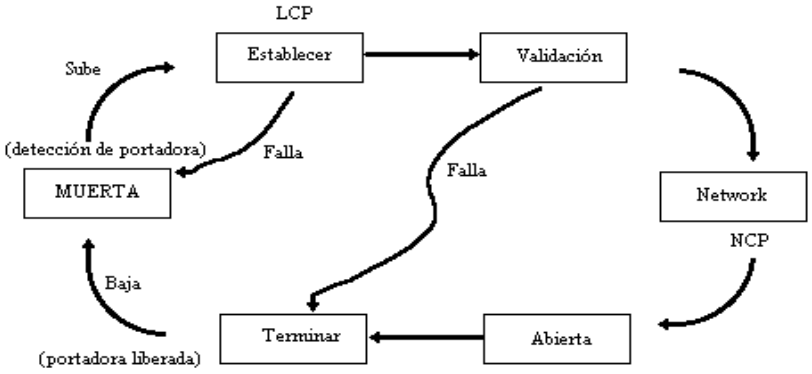


Figura 2.87. Fases de Operación PPP.

Describa cada una de ellas y de acuerdo a las tramas capturadas en el *Decodificador* realice un diagrama de secuencia entre el PC e ISP donde se ilustre el intercambio de paquetes *LCP* y *NCP* (Network Control Protocol) para cada una de las fases de operación.

P 9.22. Ubique la primera trama en el *Decodificador* cuyo campo *Protocol ID* sea igual a *0XC023*. ¿Qué *protocolo de validación o autenticación* se utilizó en la conexión de enlace de datos y durante que fase de operación PPP debe ocurrir esta situación?. Observe como el *login* y *password* de la cuenta se obtienen de **forma directa**.

P 9.23. ¿Cuál es la función del *número mágico* que se presenta en el campo *Magic Number* dentro de *Configuration Options* para algunas tramas PPP dentro del *Decodificador*?

P 9.24. Una vez se ha llegado a la fase de red. ¿Por qué razón se *comprimen* los *campos de Control y Dirección* de la trama PPP y cuales son sus consecuencias?

P 9.25. ¿Cuál es la dirección IP asignada por el ISP al PC y que protocolos de red (IP, IPX, AppleTalk, etc) se presentaron?

- **CONCLUSIONES**

3. CONCLUSIONES Y RECOMENDACIONES

3.1 CONCLUSIONES

- De acuerdo al trabajo realizado con el Internet Advisor se observó que su *alcance* va más allá de la *detección* y *resolución* efectiva de problemas en redes LAN y WAN, ya que permite efectuar acciones como la *captura* de *logins* y *passwords* en aplicaciones como Telnet y FTP, y protocolos como PPP, ICMP Versión 1 y POP3 violando uno de los factores más importantes: *"La confidencialidad".*

- Debido a las capacidades y funcionalidades del Internet Advisor, éste puede ser empleado de forma periódica para monitorear la Red de Datos de la Universidad del Cauca sin causar ningún traumatismo, con el objetivo de observar la evolución de la misma en aspectos como utilización del ancho de banda, protocolos empleados y errores a nivel físico. Igualmente la capacidad de generación de tráfico permite probar los límites de desempeño de los equipos que conforman la red y detectar problemas antes de que ellos puedan ocurrir.

- En base a las prácticas realizadas se determinó que la configuración personalizada de los parámetros medio de transmisión y velocidad de línea en la pestaña "Interface/Protocols" provoca el funcionamiento incorrecto de los filtros de captura creados, así, es necesario realizar una configuración autonegociada si se desea lo contrario. Además los triggers "*Start Capture"* , "*Center in Capture"* y "*Halt Capture"* ubicados en la pestaña "*General"* de la ventana "*Properties of Filters/Counters"* funcionan de forma inadecuada.

- Gracias al Módulo de Interfaz J2296B E1/ISDN SIM BNC se pudo monitorear de forma exitosa el Acceso Telefónico Remoto de la Red de Datos de la Universidad del Cauca, comprobando la teoría relacionada de los protocolos LAP-D y Q.931 en ISDN. También la utilización de uno de los puertos Serie V y la prueba "Asynchronous PPP Analysis (V Series)" del Internet Advisor permitieron reconocer los componentes, las fases de operación y la estructura de trama del protocolo PPP.

- Las pruebas BERT proporcionadas por el Internet Advisor requieren la generación e introducción de un patrón de bits en el medio de transmisión a probar, razón por la cual se debe realizar una conexión y configuración en Modo Terminado. Dentro de la infraestructura actual de la Red de Datos de la Universidad del Cauca esta prueba puede ejecutarse en el Acceso Telefónico Remoto gracias a que los modems HDSL en ambos extremos de la conexión soportan esta capacidad. Sin embargo esta prueba no se ejecutó ya que se requiere la desconexión temporal del RAS y por ende dejar fuera de servicio a los usuarios que acceden a Internet a través de la Universidad.

3.2. RECOMENDACIONES

- La dificultad en la adquisición de otros equipos Internet Advisor debido a su elevado costo hace que la disponibilidad de trabajar simultáneamente con éste sea limitada constituyendo un inconveniente o problema para los grupos de estudiantes que deseen realizar las prácticas de laboratorio. Por tal razón se recomienda adquirir la licencia del programa Advisor SW Edition (J1955A) el cual posee las mismas medidas para análisis LAN que el Internet Advisor y puede ser instalado en un computador personal convencional. Hay que anotar que este software opera de forma satisfactoria ante niveles de tráfico bajos y medios pero es ineficiente en presencia de niveles de tráfico muy altos al estar limitado por la tarjeta de red del computador por lo que se recomienda su utilización para fines académicos.

- Dada la evolución y alta utilización de aplicaciones como voz y video sobre redes IP que exigen trasporte en tiempo real, es necesario disponer de herramientas que permitan realizar un monitoreo y análisis de ellas sobre la red. Además es importante que la Facultad se involucre con el estudio e implementación de este tipo de aplicaciones, razón por la cual se considera conveniente adquirir la herramienta software complementaria para el Internet Advisor denominada Advisor with IP Telephony Analyzer & XoIP Commentator (J4618C).

- A nivel de proyección de prácticas de laboratorio se sugiere simular un enlace WAN utilizando PCs, Hubs, Switches y en especial un par de Enrutadores con el fin de realizar un análisis de los protocolos de enrutamiento EGP e IGP, el protocolo PPP y correr pruebas BERT empleando el Internet Advisor. Además para representar un esquema más real en una

red de telecomunicaciones sería conveniente utilizar ya sea un par de modems o un enlace vía radio en la interconexión entre los enrutadores.

DESCRIPCIÓN DE ANEXOS

ANEXO A. INTERNET ADVISOR WAN HP J2300D: En este anexo se profundizan los temas tratados en el capítulo uno y se tratan otros como el software WAN "ISDN D-CHANEL ANALYSIS" con todas sus medidas, las cuales están relacionadas directamente con los dos Módulos de Interfaz del Analizador de Protocolos, y el software complementario que puede agregarse al equipo y no necesita hardware adicional para operar como el "Switch Advisor RMON", "Advisor with IP Telephony Analizer & XoIP Commentator", "Agilent Internet Reporter", "Sybase Commentator" y "Oracle Commentator".

GLOSARIO

DS3: Opera a 45 Mbps sobre cable coaxial.

E1: Sistema de transmisión digital a 2.048 Mbps utilizado en Europa.

E3: 34.368 Mbps sobre cable coaxial.

J2: 6 Mbps sobre cable coaxial (Usado para el Japón).

T1: Sistema de transmisión digital a 1.544 Mbps utilizado en Japón y U.S.A.

10BASE-T: Estándar IEEE 802.3, que especifica Ethernet sobre UTP.

100BASE-TX: Estándar IEEE 802.3u, que especifica Ethernet sobre UTP Categoría 5 y cableado Tipo 1 a 100 Mbps.

A

APPLETALK: protocolos de red desarrollados y comercializados por la corporación de computadores Apple utilizados para conectar ordenadores Macintosh en redes locales.

ARP (Protocolo de Resolución de Direcciones – Address Resolution Protocol): protocolo del conjunto TCP/IP que permite la resolución de direcciones IP a direcciones MAC para paquetes IP.

ASOCIACIÓN INTERNACIONAL DE TARJETAS DE MEMORIA PARA COMPUTADORAS PERSONALES (Personal Computer Memory Card International Association – PCMCIA): asociación comercial internacional que ha desarrollado estándares para dispositivos, como modems y unidades externas de disco duro, que se pueden conectar con facilidad a las computadoras tipo notebook o laptop.

B

BANYAN-VINES: sistema operativo de red desarrollado y comercializado por la empresa Banyan Systems.

BASE DE DATOS DE INFORMACIÓN PARA ADMINISTRACIÓN (Management Information Base – MIB): conjunto de objetos que representan los distintos tipos de información sobre un dispositivo.

BASELINE: medida y registro del estado de operación de la red sobre un periodo de tiempo, que sirve de base para operación y control.

BENCHMARKING: evaluación comparativa.

BRIDGE: equipo que trabaja a nivel dos del modelo OSI y se encarga de monitorear todo el tráfico de las subredes que él enlaza. Con base en las direcciones MAC fuente y destino, puede decidir cual subred envía el paquete y hacia cual va dirigida.

BROADCAST: un paquete entregado a todas las estaciones de trabajo en una red. Existe en los niveles dos y tres.

BUFFER: memoria intermedia que se utiliza como memoria de datos temporal durante una sesión de trabajo.

C

CANAL VIRTUAL (Virtual Channel - VC): conexión establecida entre usuarios de extremo en la cual los paquetes son enviados por el mismo trayecto y el ancho de banda no es asignado permanentemente hasta que es utilizado.

CDPD (Cellular Digital Packet Data): es una especificación para soportar acceso inalámbrico a Internet y otras redes públicas de conmutación de paquetes.

CIRCUITO VIRTUAL (Virtual Circuit – VC): conexión lógica entre dos usuarios pasando a través de diversos nodos en la red. Múltiples circuitos virtuales pueden emplear un único medio físico, así como un único camino virtual puede hacer uso de distintos caminos físicos para llegar a su destino.

CONTROL DE ENLACE LÓGICO (Logical Link Control - LLC): parte de la cabecera LLC/SNAP del IEEE usada para identificar el tipo de un paquete. La cabecera completa es de 8 octetos, de los cuales LLC ocupa los primeros tres.

D

DECNET: es un protocolo de red propio de Digital Equipment Corporation (DEC) que se utiliza para las conexiones en red de los ordenadores y equipos de esta marca al igual que sus compatibles. Uno de sus componentes, LAT (*Local Area Transport*, transporte de área local), se utiliza para conectar

periféricos por medio de la red y tiene una serie de características de gran utilidad como la asignación de nombres de servicio a periféricos o los servicios dedicados.

E

EMULACIÓN LAN (LAN Emulation - LANE): un conjunto de protocolos desarrollados por el ATM Forum que permite a los protocolos de las LAN heredadas, como Ethernet y Token Ring, y a los protocolos de nivel superior y a las aplicaciones que dependen de los protocolos LAN, trabajar transparentemente a través de una red ATM. LANE convierte formatos de trama, emula las funciones de broadcast, y automáticamente establece conexiones ATM.

ETHERNET: el protocolo de nivel dos más utilizado en las LAN. Ethernet es un estándar CSMA/CD a 10 Mbps originalmente desarrollado por Xerox para correr sobre cableado coaxial grueso. Ha evolucionado y ahora corre principalmente sobre cableado de par trenzado.

F

FAST ETHERNET: versión de Ethernet que trabaja a 100 Mbps.

FRAME RELAY: protocolo de nivel dos que emplea conmutación de paquetes para la entrega confiable de los mismos sobre circuitos virtuales mediante una forma de encapsulamiento HDLC entre dispositivos conectados.

FULL-DUPLEX: transmisión bidireccional simultánea de información sobre un medio común.

G

GIGABIT ETHERNET: una variación de Ethernet tradicional que opera sobre cable de fibra óptica multimodo, monomodo o par trenzado no apantallado a 1.000 Mbps.

GPRS (General Packet Radio Service): es un servicio que permite enviar paquetes de datos a través de las redes GSM.

GRUPO DE EXPERTOS DE IMAGEN EN MOVIMIENTO (Motion Pictures Expert Group - MPEG): formato gráfico de almacenamiento de video que utiliza como el JPEG compresión con pérdidas alcanzando radios muy altos de compresión.

H

HALF-DUPLEX: transmisión bidireccional de información sobre un medio común, pero donde la información puede solamente viajar en una dirección en un momento determinado.

HOST (Anfitrión): computadora que realiza funciones centralizadas en redes de telecomunicaciones y computadoras, como poner al alcance de los demás PC's los programas y los archivos de datos disponibles.

I

IDENTIFICADOR DE EXTREMO TERMINAL (Terminal Endpoint Identifier - TEI): especifica de manera única el terminal o equipo de usuario en ISDN.

IDENTIFICADOR DE PUNTO DE ACCESO AL SERVICIO (Service Access Point Identifier – SAP): en ISDN identifica la clase de servicio con que se relaciona el terminal o equipo del usuario (voz, datos, voz y datos).

INSTITUTO AMERICANO NACIONAL DE ESTÁNDARES (American National Standards Institute - ANSI): organismo norteamericano cuyas decisiones y normas de estandarización tienen un importante peso sobre la industria informática mundial.

INTERFAZ DE DATOS DISTRIBUIDA PARA FIBRA (Fiber Distributed Data Interface – FDDI): una red de área local basada en un backbone de dos anillos en fibra óptica a 100 Mbps. Uno de los anillos se diseña normalmente como anillo primario; el otro es el anillo secundario.

INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS (Institute of Electrical and Electronic Engineers - IEEE): un cuerpo de estandarización responsable de desarrollar muchos estándares usados en las redes de área local, incluyendo la serie 802.x.

INTERFAZ DE SISTEMA PARA COMPUTADOR PEQUEÑO (Small Computer System Interface - SCSI): interfaz equivalente a un bus de expansión completo en el que se puede conectar dispositivos como unidades de disco duro, unidades de CD – ROM, digitalizadores e impresoras láser.

INTERFAZ DE TASA BÁSICA (Basic Rate Interface - BRI): acceso básico ISDN que proporciona dos canales B (64 Kbps) y un canal D (16 Kbps) multiplexados a través de una línea telefónica.

INTERFAZ DE TASA PRIMARIA (Primary Rate Interface - PRI): acceso primario ISDN que proporciona 30 canales B y un canal D de 64 Kbps en Europa. En EE.UU. suele tener 23 canales tipo B y un canal D de 64Kbps.

INTERFAZ DE USUARIO MEJORADA NETBIOS (NetBIOS Extended User Interface - NetBEUI): es la implementación de Microsoft del estándar NetBIOS.

INTERFAZ ENTRE NODOS DE LA RED (Network Node Interface – NNI): define la conexión interna entre nodos ATM en una red.

INTERFAZ USUARIO RED (User Network Interface – UNI): define la conexión entre el switch ATM y los usuarios.

IPX/SPX (Internet Packet eXchange/Sequenced Packet eXchange): es el conjunto de protocolos de bajo nivel utilizados por el sistema operativo de red Netware de Novell. SPX actúa sobre IPX para asegurar la entrega de los datos.

ISL (Inter-Switch Link Protocol): (1) Protocolo propietario de Cisco para interconectar múltiples switches y mantener información VLAN conforme el tráfico cursa entre switches. Opera en un ambiente punto a punto y soporta hasta 1000 VLAN's. (2) ISL and 802.1q son dos tipos de encapsulaciones usadas para transportar información de VLAN's sobre un enlace troncal.

J

JITTER: desplazamiento de una señal de transmisión en el tiempo o en la fase. Puede introducir errores y pérdida de sincronización en las comunicaciones sincrónicas de alta velocidad.

L

LEY μ: sistema de codificación usado en América del Norte y Japón para la transferencia de voz, sistemas de respuesta de voz interactiva, dispositivos de conmutación privados y radio por Internet.

LEY A: sistema de codificación similar a la Ley μ utilizado en Europa y el resto del mundo.

M

MEGACO: el protocolo H.248 o Megaco permite la conmutación de llamadas de voz, fax y multimedia entre la red PSTN y las redes IP de siguiente generación. Este protocolo, que tiene su origen en el protocolo MGCP, proporciona un control centralizado de las comunicaciones y servicios multimedia a través de redes basadas en IP.

MULTICAST: una forma de broadcast en la cual un paquete es entregado a un grupo definido de destinatarios. Una dirección de destino multicast específica es usada.

N

NETWARE: nombre de un sistema de red desarrollado y comercializado por Novell Incorporated.

NETWORK (Red): (1) Grupo de nodos interconectados. (2) Serie de puntos, nodos o estaciones conectados por canales de comunicación. (3) El conjunto de equipos por medio del cual se establecen las conexiones entre las estaciones de datos.

NIVEL DE CONTROL DE ACCESO AL MEDIO (Medium Access Control - MAC): un subnivel dentro del nivel 2 que se asocia a un tipo de LAN específico como Ethernet o Token Ring.

NODO: es el punto en donde se producen dos o más conexiones en una red de comunicaciones. No se trata de un elemento estrictamente físico, sino de una unidad funcional que exige hardware y software. Un nodo puede incluir controladores de comunicaciones, clusters, servidores, repetidores, etc.

NOVELL: es una de las firmas de origen norteamericano más importantes en el ámbito de las redes de área local en todo el mundo y su producto estrella es Netware.

NÚMERO DE CANAL LÓGICO (Logical Channel Number - LCN): número único dado a cada circuito virtual en una llamada. Un LCN es adicionado a cada paquete durante la llamada y diferencia los paquetes de aquellos generados por otros usuarios en otras llamadas.

O

ORACLE: empresa especializada en la fabricación de programas de bases de datos en ordenadores.

OSPF (Open Shortest Path First): protocolo de enrutamiento enlace-estado no propietario utilizado por los enrutadores IP para determinar el camino óptimo a lo largo del cual transportar un paquete.

P

PACKET (Paquete): bloque de información transmitida en una red. Un paquete contiene la dirección de la fuente, del destino, la información para verificación de errores y la información del mensaje.

PING (Packet Internet Groper): es una herramienta de diagnóstico para verificar la conectividad entre dos computadores en una red. Envía paquetes ICMP con Respuesta de Eco a una dirección IP remota, observa las respuestas ICMP e indica el tiempo exacto que tardan los paquetes en ir y volver desde la máquina origen hasta la máquina destino.

PROTOCOLO DE ACCESO AL ENLACE PARA EL CANAL D (Link Access Protocol Channel D – LAP D): protocolo de nivel dos en ISDN cuya función principal es transmitir los

mensajes de nivel superior necesarios entre los equipos del usuario y la central telefónica para establecer una llamada.

PROTOCOLO DE CONTROL DE ENLACE (Link Control Protocol – LCP): usado por PPP para acordar automáticamente las opciones del formato de encapsulación, los límites de manipulación de tamaño de paquete, detectar un enlace con ciclos, otros errores comunes por mala configuración y terminar el enlace.

PROTOCOLO DE CONTROL DE RED (Network Control Protocol - NCP): en PPP se emplea para el establecimiento y la configuración de los diferentes protocolos de nivel de red como IP, IPX o AppleTalk.

PROTOCOLO DE DATAGRAMAS DE USUARIO (User Datagram Protocol – UDP): complemento de TCP que ofrece un servicio de datagramas sin conexión que no garantiza la entrega o la secuencia correcta de los paquetes enviados.

PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (Routing Information Protocol – RIP): protocolo IGP basado en el algoritmo Vector – Distancia diseñado para permitir el intercambio de información entre dispositivos que participan en el enrutamiento de una red IP.

PROTOCOLO DE MENSAJES DE CONTROL EN INTERNET (Internet Control Message Protocol - ICMP): protocolo empleado para reportar problemas mediante el envío de datagramas IP dentro de una red de la misma clase.

PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS (File Transfer Protocol – Ftp): protocolo empleado para la transferencia de archivos entre un servidor y un cliente.

PROTOCOLO PUNTO A PUNTO (Point to Point Protocol – PPP): protocolo estándar que permite la interacción de software de acceso remoto de diversos proveedores.

Q

Q.931: especificación ITU-T para la señalización en el establecimiento, mantenimiento y terminación de conexiones de red ISDN.

R

RARP (Protocolo de Resolución de Direcciones Inverso – Reverse Address Resolution Protocol): protocolo del conjunto TCP/IP que permite la resolución de direcciones MAC a direcciones IP para paquetes IP.

RED DE ÁREA EXTENSA (Wide Area Network - WAN): extensión de una red de datos que utiliza enlaces de telecomunicaciones para conectarse con áreas separadas geográficamente. Son más lentas que las LAN y pueden enlazar muchas oficinas que se encuentran a través del mundo utilizando protocolos especiales de enrutamiento y filtros para minimizar los costos de enviar datos a través de grandes distancias.

RED DE ÁREA LOCAL (Local Area Network - LAN): sistema de comunicación intra - oficina e intra-edificio que tiene algún tipo de procesamiento de comunicaciones y transferencia de información transparente entre usuarios y/o dispositivos electrónicos.

RED DE ÁREA LOCAL VIRTUAL (Virtual Local Area Network - VLAN): agrupación lógica de hosts en una o más LAN que permite la comunicación entre ellos como si estuvieran en la misma LAN física.

RED DIGITAL DE SERVICIOS INTEGRADOS (Integrated Services Digital Network- ISDN): red que ha evolucionado en general a partir de la Red Digital Integrada (RDI) para telefonía y que proporciona una conectividad digital de extremo a extremo para apoyar una amplia gama de servicios vocales y no vocales, a los cuales los usuarios tiene acceso mediante un conjunto limitado de interfaces polivalentes normalizadas usuario-red.

REPETIDOR: equipo que trabaja en el nivel físico del modelo OSI ya que se encarga de regenerar los bits tal como llegan para luego retransmitirlos.

ROUTER: equipo que opera a nivel tres del modelo OSI responsable de discernir cual es el camino más adecuado para la transmisión de mensajes en una red compleja que está soportando un tráfico intenso de datos.

S

SERVICIO DE NOMBRES DE DOMINIO (Domain Name Service – DNS): proporciona el servicio de traducción de nombres de domino en direcciones IP reales.

SERVICIOS DE RED XEROX (Xerox Network Services - XNS): protocolo de comunicación de la firma Rank Xerox.

SERVIDOR: computadora dedicada a gestionar el uso de la red por otras computadoras llamadas clientes. Contiene archivos y recursos que pueden ser accesados desde otras terminales.

SISTEMA BÁSICO DE ENTRADA Y SALIDA DE RED (Network Basic Input/Output System - NetBIOS): interfaz de programación de aplicaciones que pueden utilizar los programas en una red de área local. Proporciona a los programas un conjunto uniforme de comandos para solicitar los servicios de bajo nivel necesarios para administrar nombres, dirigir sesiones y enviar datagramas entre los nodos de una red.

SUN (Stanford University Network): Sun Microsystems es la empresa líder en soluciones globales con productos y servicios de alta tecnología informática para sistemas abiertos.

SVGA (Super Video Graphics Array): mejoramiento del estándar para monitor de matriz de gráficos de video capaz de presentar por lo menos 800 pixeles en posición horizontal y 600 líneas en posición vertical, y hasta 1024 pixeles por 768 líneas con 16, 256 o 16.7 millones de colores exhibidos simultáneamente.

SWITCH: equipo que opera en la capa de enlace de datos del modelo OSI diseñado para agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera, bajar el costo por puerto y resolver problemas de rendimiento en la red debido a anchos de banda pequeños y cuellos de botella.

SYBASE: empresa especializada en la fabricación de programas de bases de datos, herramientas de desarrollo, portales empresariales y servidores móviles e inalámbricos.

T

TCP/IP (Protocolo de Control de Transmisión / Protocolo Internet – Transmision Control Protocol/ Internet Protocol): conjunto de protocolos de red utilizados en Internet que proporcionan comunicación entre redes interconectadas formadas por equipos con distintas arquitecturas de hardware y diversos sistemas operativos.

TELNET: protocolo que permite a los usuarios conectarse a una computadora remota en Internet. Ésta puede localizarse en una oficina próxima o en cualquier lugar del mundo.

TOKEN RING: arquitectura de red estandarizada en la norma IEEE 802.5 en la cual los dispositivos en un anillo transmiten datos mientras está en posesión de un Token, el cual pasa de nodo a nodo continuamente. Opera a 4 o 16 Mbps.

TRACERT: esta herramienta de diagnóstico determina el camino tomado hacia un destino enviando paquetes de eco ICMP con valores variables de período de vida para el destino.

TRAYECTO VIRTUAL (Virtual Path – VP): grupo de canales virtuales que pueden soportar múltiples circuitos virtuales.

TRIGGER: son acciones que se realizan ante la presencia de determinados eventos o condiciones.

TROUBLESHOOTING: localización y arreglo de fallas en la red.

X

X.25: protocolo de nivel tres utilizado principalmente en ambientes WAN y, sobre todo, en las redes públicas de transmisión de datos. Funciona por conmutación de paquetes, esto es, los bloques de datos contienen información del origen y destino para que la red los pueda entregar correctamente aunque cada uno circule por un camino diferente.

ACRÓNIMOS

ATM: Asynchronous Transfer Mode. Modo de transferencia asincrónico.

AUI: Attachment Unit Interface. Interfaz de unidad de conexión.

BOP: Bit Orientated Protocol. Protocolo orientado a bit.

CD: Carrier Detect.

CEPT: Conference of European Postal and Telecommunications Administrations. Conferencia europea de las administraciones de correos y telecomunicaciones.

CHAP: Challenge Handshake Authentication Protocol. Protocolo de autenticación por desafío mutuo.

CLP: Cell Loss Priority. Prioridad de pérdida de celdas.

CTS: Clear to Send.

DCE: Data Terminal Circuit Equipment. Equipo Terminal del Circuito de Datos.

DLCI: Data Link Connection Identifier. Identificador de conexión de enlace de datos.

DNS: Domain Name Server. Servidor de nombres de dominio.

DTE: Data Terminal Equipment. Equipo Terminal de Datos.

DTR: Data Terminal Ready.

DSR: Data Set Ready.

EIA: Electronic Industries Association. Asociación de Industrias Electrónicas.

ETSI: European Telecommunications Standards Institute. Instituto europeo de estándares en telecomunicaciones.

Gbps: Gigabits per Second. Gigabits por segundo.

HDLC: High Level Data Link Control. Control de enlace de datos de alto nivel.

IBM: International Business Machine.

IGP: Internal Gateway Protocol. Protocolo de pasarela interior.

IPCP: IP Control Protocol. Protocolo de control para IP.

IPET: Instituto de Postgrados en Electrónica y Telecomunicaciones.

IPXCP: IPX Control Protocol. Protocolo de control para IPX.

ITU-T: International Telecommunication Union – Telecommunication. Unión Internacional de Telecomunicaciones – Sector Telecomunicaciones.

Kbps: Kilobits per second. Kilobits por segundo.

LAP - B: Link Access Procedure – Balanced. Procedimiento de acceso al enlace en modo balanceado.

Mbps: Megabits per Second. Megabits por segundo.

MGCP: Media Gateway Control Protocol. Protocolo de control de puerta de enlace al medio.

NIC: Network Interface Card. Tarjeta de interfaz de red.

NT: Network Termination. Terminador de red.

PAP: Password Authentication Protocol. Protocolo de autenticación mediante password.

PDU: Protocol Data Unit. Unidad de datos de protocolo.

PLCP: Physical Layer Convergence Protocol. Protocolo de convergencia del nivel físico.

POP3: Post Office Protocol-3. Protocolo de oficina postal versión 3.

RMON: Remote Monitoring. Monitoreo remoto.

RTP: Real Time Transport Protocol. Protocolo de transporte en tiempo real.

RTS: Request to Send.

SDLC: Synchronous Data Link Control. Control de enlace de datos sincrónico.

SGCP: Simple Gateway Control Protocol. Protocolo de control de puerta de enlace simple.

SGMP: Simple Gateway Monitoring Protocol. Protocolo sencillo de supervisión de pasarelas.

SIP: Session Initiation Protocol. Protocolo de inicio de sesión.

SMDS: Switched Multimegabit Data Service.

SNA: Systems Network Architecture.

STM-1/OC-3: Synchronous Transfer Mode –1/ Optical Carrier –3.

TE: Terminal Equipment. Equipo terminal.

TDS: Tabular Data Stream.

TFTP: Trivial FTP. FTP trivial.

TNS: Transparent Network Substrate.

VoIP: Voz sobre IP.

VPN: Virtual Private Network. Red privada virtual.

W – CDMA: Wideband – Code Division Multiple Access. Acceso múltiple por división de código de banda ancha.

WWW: World Wide Web. Red Mundial de Documentos HTML.

UTP: Unshielded Twisted Pair. Par trenzado sin apantallar.

BIBLIOGRAFÍA

- CASTILLO E, Edgar. **"Red Digital de Servicios Integrados"**. Universidad del Cauca. 1.989.

- CÚJAR OTERO, Carlos Fernando. NARVÁEZ JOAQUÍ, Oscar Felipe. **"Evolución de la Red de Datos de la Universidad del Cauca hacia una Infraestructura de Red de Área Local de Alta Velocidad".** Universidad del Cauca. 2001.

- IBÁÑEZ PÉREZ, Luis Hernán. **"Análisis de desempeño de los protocolos de enrutamiento RIP y OSPF en una red corporativa"**. Bogotá D.C. Agosto de 2.000.

- TERÁN CUARÁN, Francisco Javier. **"Redes Globales de Información"**. Universidad del Cauca. 2.001.

- Artículo: **"Protocolos IPX/SPX"**. Disponible online en http://www.lugna.linux.org.ar/docuOk/.

- Artículo: **"Tipos de errores en redes Ethernet"**. Disponible online en http://download.wg.com/guides/troubleshooting_guides.

- 3Com Corporation. "**SuperStack II Dual Speed Hub 500 User Guide".** 3Com Press**.** 1.998. Disponible online en http://www.3com.com.

- 3Com Corporation. "**SuperStack Switch Management Guide".** 3Com Press. 2.000. Disponible online en http://www.3com.com.

- Agilent Technologies. **"Advisor Async/BiSync Getting Started"**. Agilent Technologies Press. 2.000. Disponible online en http://onenetworks.comms.agilent.com.

- Agilent Technologies. **"Advisor with IP Telephony Analyzer & XoIP Commentator"**. Agilent Technologies Press. 2.001. Disponible online en http://onenetworks.comms.agilent.com.

- Agilent Technologies. **"Finding and Solving 10/100 Ethernet Problems with the Internet Advisor"**. Agilent Technologies Press. 2.000. Disponible online en http://onenetworks.comms.agilent.com.

- Agilent Technologies. **"Internet Reporter LAN/WAN/ATM"**. Agilent Technologies Press. 2.000. Disponible online en http://onenetworks.comms.agilent.com.

- Agilent Technologies. **"Switch Advisor – Getting Started"**. Agilent Technologies Press. 2.001. Disponible online en http://onenetworks.comms.agilent.com.

- Agilent Technologies. **"T1/E1 (Bantam), E1/T1 (DB-9), E1 (BNC) Line Interface Modules. User Guide"**. Agilent Technologies Press. 2.002. Disponible online en http://onenetworks.comms.agilent.com.

- Bay Networks. **"Reference for the Accelar Management Software".** Bay Networks Press. 1.997. Disponible online en http://www.baynetworks.com.

- Bay Networks. **"Using the Accelar 1200/1250 Routing Switch".** Bay Networks Press 1.997. Disponible online en http://www.baynetworks.com.

- Cisco Systems. **"Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide"**. Cisco Press. 2.002. Disponible online en http://www.cisco.com.

- Hewlett-Packard. **"HP Internet Advisor LAN. HP J3711A Sybase Commentator Software"**. Hewlett-Packard Press. 1.998. Disponible online en http://www.hp.com/go/internetadvisor.

- Hewlett-Packard. **"HP Internet Advisor WAN Getting Started"**. Hewlett-Packard Press. 1.999. Disponible online en http://www.hp.com/go/internetadvisor.

- Hewlett-Packard. **"HP Internet Advisor WAN High Speed Toolkit"**. Hewlett-Packard Press. 1.997. Disponible online en http://www.hp.com/go/internetadvisor.

- Hewlett-Packard. **"HP J3710A – MS-DOS. HP J3710B – Windows. LAN Oracle Commentator User's Guide"**. Hewlett-Packard Press. 1.998. Disponible online en http://www.hp.com/go/internetadvisor.

- Hewlett-Packard. **"LAN en Windows Getting Started"**. Hewlett-Packard Press. 1.999. Disponible online en http://www.hp.com/go/internetadvisor.

- Hewlett-Packard. **"Mainframe Features System Guide J2300C/D, J3446C/D y J3754C"**. Hewlett-Packard Press. 1.999. Disponible online en http://www.hp.com/go/internetadvisor.

- Lucent Technologies. **"Max 6000 Installation and Basic Configuration Guide"**. Lucent Technologies Press. 2.001. Disponible online en http://www.lucent.com.

- RFC 1234: **"Encaminamiento del Tráfico IPX a través de redes IP"**. Disponible online en http://www.arrakis.es/~pjleon/rfc-es.

- RFC 1213: **"Management Base for Network Management of TCP/IP – based internets: MIB - II"**. Disponible online en http://rfc.sunsite.dk/rfc/rfc1213.html.

- RFC 1662: **"PPP in HDLC like – Framing"**. Disponible online en http://www.cis.ohio-state.edu/cgi-bin/rfc.

- RFC 1757: **"Remote Network Monitoring Management Information Base".** Disponible online en http://rfc.sunsite.dk.

- RFC 1661: **"The Point to Point Protocol"**. Disponible online en http://rfc.sunsite.dk.

- Tutorial: **"HP Internet Advisor LAN CBT"**.

- Tutorial : **"RDSI"**. Disponible online en http://personales.mundivia.es/jtoledo/angel.

- Tutorial: **“Red Digital de Servicios Integrados (RDSI)”**. Disponible online en http://www.cybercursos.net.

- Tutorial: **“TCP/IP”**. Disponible online en http://ditec.um.es/laso/docs/tut_tcpip.