

SIMULACIÓN DE PROTOCOLOS DE COMUNICACIONES

Manuel Antonio Freire Medina, Johnny Eduardo Rivero Guevara, Roberto Carlos Muñoz Jaramillo
Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil, Ecuador
rmunoz@fiec.espol.edu.ec, jrivero@fiec.espol.edu.ec, mfreire@fiec.espol.edu.ec
Ing. José Escalante
joescala@espol.edu.ec

Resumen

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

Palabras Claves: Analizador, MAC, IP, HDLC Frame Relay, ATM.

Abstract

To share data across the network requires an advance notice, and this communication is governed by certain protocols, under compliance, they allow communication. This premise led to the idea of the project "Simulation of Communication Protocols" that with simulation equipments allow to analyze and understand how a package or plot travels through a network to provide voice services, data and telephony using a protocol analyzer equipment Radcom RC-100WL. They will be treated with different types of tools for analyzing and monitoring networks, as well as analyzers and / or simulators, revise a software used to analyze and simulate networks with different protocols LAN and WAN. An analysis of the structure of the frames or packets of the protocols in use today as MAC, IP LAN and HDLC, Frame Relay and ATM WAN network will be done.

1. Introducción.

En el análisis se darán a conocer los modelos de arquitectura de comunicaciones como OSI y TCP/IP.

Se analizarán protocolos de capa 2 como MAC, Frame Relay, HDLC y ATM para obtener servicio de la capa física para la transmisión de datos, notificación de errores, topología de la red y control de flujo.

Como protocolo de capa 3 se analiza IP que contiene información de dirección y control que permite el paquete ser encaminado o enrutado.

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

2. Protocolos de Comunicación.

Un protocolo es un método por el cual dos ordenadores acuerdan comunicarse, una especificación que describe cómo los ordenadores hablan el uno al otro en una red.

El protocolo determina lo siguiente:

- El tipo de comprobación de errores que se utilizará.
- El método de compresión de los datos, si lo hay.
- Cómo indicará el dispositivo que envía que ha acabado el enviar un mensaje.
- Cómo indicará el dispositivo que recibe que ha recibido un mensaje.

2.1.1.- MAC

El protocolo MAC (Control de acceso al medio), Pertenece al estándar Ethernet, es parte de la capa 2, este permite direccionamiento y mecanismos de control al canal de acceso que hace posible que varias host se puedan comunicar dentro de una red; típicamente una LAN (Área de red local) o MAN (Área de red metropolitana). Ethernet es un método de acceso al medio que permite a todos los host de una red compartir el mismo medio. Ethernet es popular pues es muy escalable, por esto es fácil de integrar a nuevas tecnologías como Fast Ethernet dentro de la misma infraestructura. Para el direccionamiento en Ethernet se utiliza la dirección MAC o física del host; es decir cada host en la red tiene un identificador de 48 bits (6 bytes) escrito en formato hexadecimal como se muestra en la figura 1. Esta dirección es también llamada dirección unicast porque identifica a una NIC (Network Interface Card).

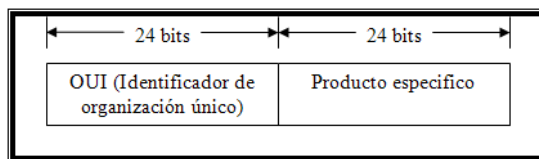


Figura 1. Dirección MAC

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

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

El bit mas significativo indica si la dirección es individual (0) o de grupo (1). Entonces para

transmisiones broadcast la dirección es FF.FF.FF.FF.FF.FF, o simplemente todo 1.

2.1.2.- HDLC

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

Este es un protocolo de propósito general, que opera a nivel de enlace de datos y ofrece una comunicación confiable entre el trasmisor y el receptor.

Es el protocolo más importante para el enlace de datos (ISO 3309, ISO 4335).

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

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

La estructura de la trama se muestra en la figura 2.

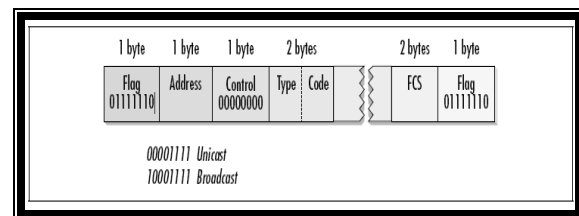


Figura 2. Trama cHDLC

2.1.3.- FRAME RELAY

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

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

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

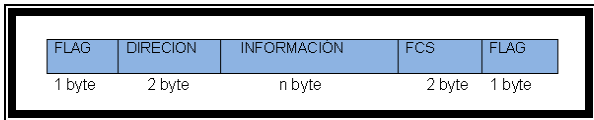


Figura 3. Estructura de la trama

Campo de Dirección.- Se llama campo de dirección a los bytes que siguen al Flag y que están por delante de los Datos de usuario. Puede tener varios formatos, pero normalmente suele tener 16 bits de longitud (2 octetos), como se muestra en la figura 4.

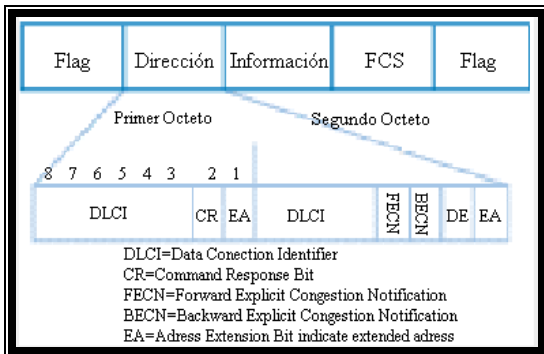


Figura 4. Campo de Dirección

Campo de Información.- La figura 5 muestra el campo de información que puede contener datos de usuario o el mensaje de señalización, definido por el estándar Frame Relay.

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

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

El primer octeto del campo de información de usuario de FR es el campo de control Q.922, para

la transferencia de información sin confirmación, se usa el valor UI (0x03).

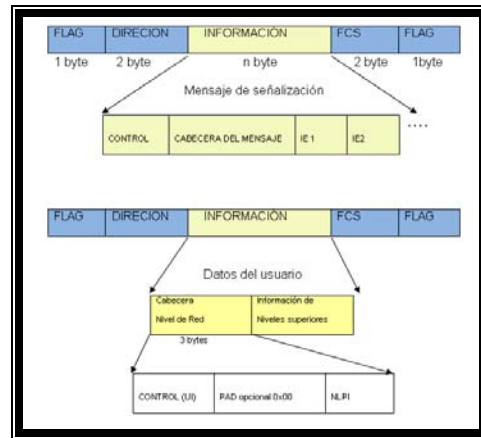


Figura 5. Campo de Información

2.1.4.- ATM

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

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

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

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

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

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

La figura 6 muestra el modelo de referencia del protocolo ATM.

La primera capa llamada capa física (Physical Layer), define las interfaces físicas con los medios

de transmisión y el protocolo de trama para la red ATM es responsable de la correcta transmisión y recepción de los bits en el medio físico apropiado.

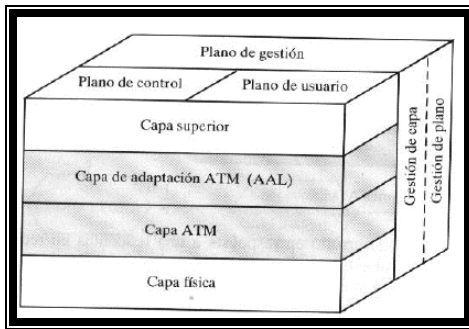


Figura 6. Modelo de referencia del protocolo ATM

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

La capa ATM provee un solo mecanismo de transporte para múltiples opciones de servicio.

Es independiente del tipo de información que es transmitida (datos, voz, video) con excepción del tipo de servicio (QOS) requerido.

La capa de adaptación ATM provee las funciones orientadas al usuario no comprendidas en la Capa ATM.

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

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

2.1.5.- IP

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

Un paquete IP contiene varios campos de información mostrados en la siguiente figura:

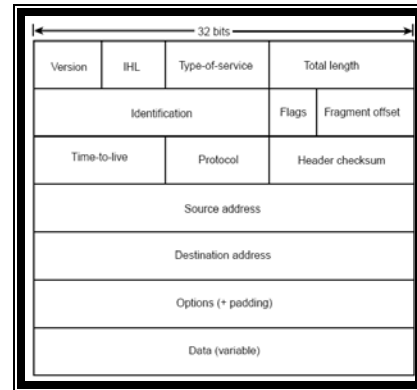


Figura 7. Formato estructura IP

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

3. Herramientas de Simulación de Protocolos de Comunicaciones.

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

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

Actualmente las desventajas de éste son que al agregar más componentes al modelo, su procesamiento será más lento, siendo dependiente de la capacidad de procesamiento de la computadora en la cual se encuentra instalado. En otras herramientas de análisis tenemos los analizadores de red (analizadores de protocolos o sniffers), estos realizan el proceso de capturar el tráfico de la red. Este a su vez decodifica la información, generalmente, tramas o paquetes de varios protocolos de comunicaciones y lo presenta de una manera comprensible al usuario. Una de las primeras aplicaciones de captura y análisis del tráfico de red fue Sniffer, de Network General, es por esto que una aplicación de análisis de red es conocida como Sniffer o Packet Sniffer.

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

3.1.1.- RADCOM RC-100WL

En las pruebas realizadas se utiliza el equipo RADCOM RC-100WL para análisis y simulación de redes con diferentes protocolos a nivel LAN y WAN. En la actualidad este equipo ha sido reemplazado por la familia de equipos Prism Lite y Performer Analyzer de Radcom. Debido a que este modelo de equipo no soporta interfaz ATM y la práctica de ATM será realizada con la versión demo del equipo Prism Lite de Radcom.



Figura 8. Panel frontal de equipos Radcom

4.- Pruebas realizadas

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

Se implementaron los siguientes cuatro laboratorios para obtener las respectivas tramas capturadas:

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

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

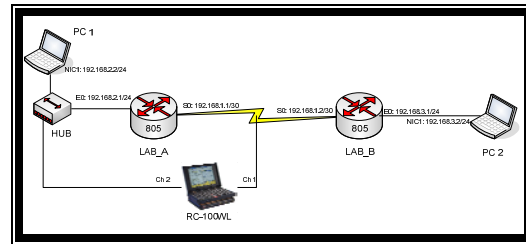


Figura 9. Diagrama de la red

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

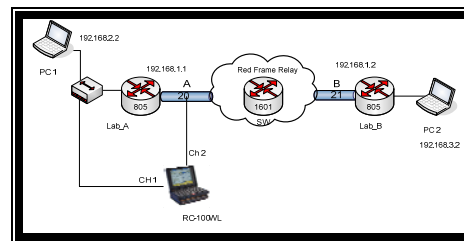


Figura 10. Diagrama de la red Frame Relay

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

4.1.2. Análisis de las tramas ICMP

En la siguiente figura se observa el análisis de distribución por tipo de las tramas ICMP. Esta figura indica el tipo de código ICMP dentro del paquete, en este caso se tienen 55 paquetes tipo petición de eco y 48 de respuesta de eco.

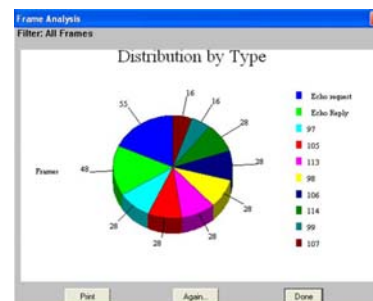


Figura 11. Análisis por ICMP

Además se visualizan otros tipos que no son válidos como tipo 97, 105, 113, 98, 106, 114, 99 y

107. Estos aparecen pues al realizar un ping con un tamaño mayor a la unidad máxima de transferencia (MTU = 1500bytes) el paquete IP se fragmenta. Por lo tanto en la cabecera IP el campo Protocolo=ICMP pero la cabecera ICMP solo esta en el primer paquete y no en todos los fragmentos como se aprecia en la figura 12.

```

Frame: 0 Captured at: +02:30.258
Length: 1506 From: user Status: ok
Cisco Router: Protocol is IP <0800>
IP: Version = 4 <45>
IP: IHL = 20 [Bytes]
IP: Type of Service: 0x00 <00>
IP: Routine
IP: Normal Delay
IP: Normal Throughput
IP: Normal Reliability
IP: Total Length = 1500 <05DC>
IP: Identification = 31761 <7C11>
IP: Flags & Fragment Offset: 0x2172 <2172>
IP: 0..... Reserved
IP: 0..... May Fragment
IP: ..... More Fragment
IP: Fragment Offset = 2960 [Bytes]
IP: Time To Live = 127 [Seconds/Hops] <7F>
IP: Protocol: 1 ICMP <01>
IP: Header Checksum = 0x1249 <1249>
IP: Source Address = 192.168.3.2 <0A80302>
IP: Destination Address = 192.168.2.2 <0A80202>
ICMP: ERROR: Unknown message type
ICMP: Type: 105
User Data
OFFSET DATA ASCII
0019: 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 61 62 jklmnopqrstuvwxyz
0029: 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 cdefghijklmnopqr
0039: 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6A 6B stuvwxyzefghijk

```

Figura 12. Fragmento de paquete ICMP

4.1.3. Análisis por distribución de protocolo

Se pueden realizar análisis de la distribución de los protocolos en la red. En la figura 14 se muestra la el gráfico en diagrama de barras y en la figura 14 se muestra en forma tabular. Ambas figuras muestran la cantidad de tramas de cada protocolo. La figura en forma de tabla muestra con más detalle la distribución de protocolos en la red.

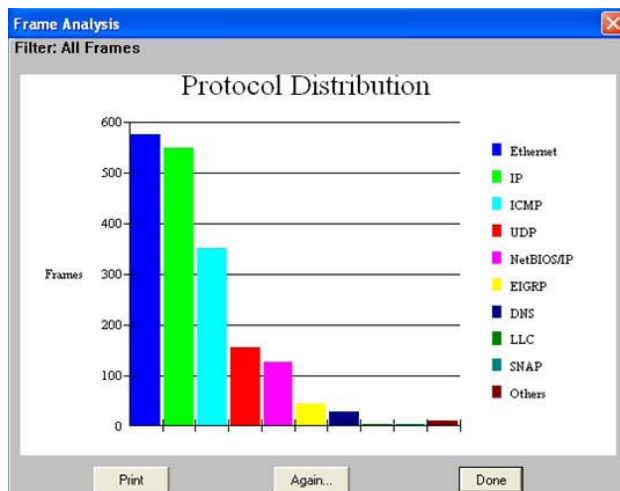


Figura 14. Distribución de protocolos

5. Conclusiones y recomendaciones

En el desarrollo de la tesis se ha implementado un procedimiento con el analizador de protocolos

RC-100 WL para los laboratorios de simulación del protocolo HDLC, simulación del protocolo MAC/IP, simulación del protocolo Frame Relay, y un procedimiento diferente con el software demo del Radcom Prism-Lite para la simulación del protocolo ATM, con la finalidad de que el estudiante se familiarice con las herramientas utilizadas para poder analizar, simular y comprender la estructura de los protocolos e interpretar como las tramas viajan por una red.

En los laboratorios que se utiliza el equipo Radcom RC-100 WL se procedió con la configuración de equipos ruteadores para obtener la red que se desea implementar, se realizan pruebas de conectividad luego de lo cual se procede con la captura de datos en tiempo real y su respectivo análisis de las primeras tramas y graficación de todos los datos capturados con gráficos pre-establecidos.

Además se utiliza el programa gratuito Packet Builder disponible en internet que es una herramienta útil y fácil para la creación de paquetes de red y en las prácticas se lo utilizo para enviar paquetes ICMP y poder encapsular dentro de los protocolos analizados.

En la práctica de laboratorio de simulación Frame Relay con analizar su cabecera se puede diferenciar si el campo de información corresponde a mensajes de señalización o datos del usuario identificando el DLCI utilizado en la trama, además en los mensajes de señalización se identifica que LMI se esta utilizando, en los datos del usuario se analiza el protocolo superior encapsulado.

En la práctica de laboratorio de simulación HDLC se implementa una red con dos ruteadores y se comprobó la estructura de la trama cHDLC de Cisco Systems; que es una extensión del protocolo HDLC que utiliza sistema de verificación del estado del enlace mediante mensajes keep-alive

En la práctica IP se detallo la encapsulación de IP sobre Ethernet revisando sus campos

En la práctica de laboratorio de ATM unos de los problemas encontrados fue que el analizador utilizado en los laboratorios no tiene capacidades para analizar una red ATM y además no se disponía de una red básica de ATM para su análisis por tal motivo se utilizo un demo que permite probar las capacidades del analizador antes de proceder con la compra del analizador Prism Lite.

En ATM se analiza la subcapa AAL5 debido a que permite trabajar con protocolos no orientados a conexión, en nuestro caso protocolo IP.

En el desarrollo de nuestra tesis un obstáculo es que debido a la demanda de un analizador de protocolos en las empresas que lo poseen; tuvimos que regirnos a la poca disponibilidad del mismo y aprovechar al máximo esta herramienta.

El analizador de protocolos utilizado en los laboratorios es un equipo que tiene ciertas carencias en ATM y en IPv6, actualmente ha sido reemplazado por el analizador Ultra Prism Lite que posee mejoras para el análisis de una red de datos.

Se recomienda utilizar los procedimientos con el programa Dynamips debido a que este permite capturar el tráfico que viaja a través de las interfaces de los routers. Esto es muy recomendado para poder visualizar la estructura de las tramas, aunque no permite capturas sobre interfaces ATM.

Se recomienda que luego de tener los conocimientos básicos de análisis se proceda a implementar redes complejas para su respectivo análisis

Se recomienda a la universidad implementar un laboratorio de redes para simular y analizar protocolos de comunicaciones, dado que es muy utilizado por instituciones de control como Senatel/Conatel y Supertel.

6. Referencias

- [1] IP/MPLS Forum. “Frame Relay Forum Implementation Agreements”.
http://www.ipmplsforum.org/tech/fr_ia.shtml
- [2] RFC 791. IP. <http://www.rfc-editor.org/rfc/rfc791.txt>
- [3] RFC 792. ICMP. <http://www.rfc-editor.org/rfc/rfc792.txt>
- [4] RFC 826, 923. ARP – RARP. <http://www.rfc-editor.org/rfc/rfc826.txt>
- [5] Cisco System, Inc. CCNA Curriculum v3.1. <http://cisco.netacad.net>

- [6] Cisco System, Inc. “Asynchronous Transfer Mode (ATM) Switching”.
<http://www.cisco.com/en/US/docs/internetworking/technology/handbook/atm.html>
- [7] Cisco System, Inc. “Internet Protocols (IP)”.
<http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Internet-Protocols.html>
- [8] Cisco System, Inc. “Frame Relay”.
<http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Frame-Relay.html>
- [9] Cisco System, Inc. “Ethernet”.
<http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Ethernet.html>
- [10] Todd Lammle. “Cisco CCNA Study Guide”, Editorial Sybex. Quinta edición. Capítulo 2, 11.
- [11] Angela Orebaugh. “Wireshark and Ethereal Network Protocol Analyzer Toolkit”. Editorial Syngress. Capítulo 1, 2.
- [12] Wendell Odom, “CCIE Routing and Switching”. Editorial Cisco. Tercera edición. Capítulo 1, 4, 15.
- [13] Laura Chappell’s Lab kit. Versión 9. <http://www.novell.com/ncmagopenxtest/laurachappell.html>
- [14] Rad Tutorials. “ATM”.
<http://www2.rad.com/networks/infrastructure/atm/main.htm>
- [15] Rad Tutorials. “Packet Switching”.
<http://www2.rad.com/networks/2004/PacketSwitching/main.htm>
- [16] Programa Wireshark.
<http://www.wireshark.org>
- [17] Programa Packet Builder.
<http://www.engagesecurity.com/products/engagepacketbuilder/>
- [18] Radcom Ultra Prism Lite.
<http://www.radcom.com/LeadForm1.aspx?BoneId=381&ObjID=-1&staticname1=2&FileName=632616552728437500125.pdf>