UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE CUENCA

FACULTAD DE INGENIERÍAS

CARRERA DE INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del Título de:

Ingeniero de Sistemas

TÍTULO DEL TEMA:

Análisis, diseño e implementación de un sistema en software libre para el monitoreo por usuario y aplicación del uso de ancho de banda en conexiones de internet orientado a la pequeña y mediana empresa. Creación de una imagen basada en GNU-Linux para su distribución

AUTORES:

Eugenia Beatriz Llivigañay Pacheco

Verónica Gabriela Serrano Pinos

DIRECTOR:

Ing. Byron Carrión

Cuenca, Febrero del 2011

Dedicatoria

Este proyecto dedico a todas y cada una de las personas que participaron directa o indirectamente en mi vida universitaria pero de manera especial:

A Dios por acompañarme y guiarme en mi diario vivir.

A mi hermano, mi madre y mis madrinas que me dieron su apoyo económico y estuvieron pendientes de mí.

A Christian y Sabina quienes me dieron ánimos y su apoyo incondicional para continuar con nuestra tesis.

A mi compañera y amiga de tesis Verónica ya que con ella compartí durante muchos ciclos conocimientos, alegrías, tristezas y me ha dado consejos cuando los he necesitado.

A todos y cada uno de mis amigos, que me han brindado su amistad incondicional así como su ayuda cuando lo he requerido.

Eugenia Llivigañay

Agradecimientos

En primer lugar agradezco a Dios por darme un sentido especial a mi vida, ayudarme a cumplir mis metas y sueños pero sobretodo por enseñarme a levantar de los duros golpes que da la vida.

A mi familia en especial a mi hermano que no está en la Ciudad pero que me dio su apoyo económico y comprensión para que continúe en esta etapa universitaria. Así como a mi madre, mis madrinas que siempre han estado pendientes de que me encuentre bien y me han guiado por el sendero de la vida.

Al economista José Herrera que ha sido como un padre por su cariño y su preocupación.

A Christian y Sabina que una u otra forma me han hecho participe de su vida, así como he contado con sus apoyos y ánimos de una manera incondicional cuando lo he requerido.

A mi amiga Verónica por haberme escogido como su compañera de Tesis y brindarme su amistad a lo largo de la carrera.

A todos y cada uno de mis amigos por brindarme su amistad incondicional ya que con ellos hemos compartido momentos inolvidables a lo largo de mi vida estudiantil.

A todos y cada uno de mis profesores que han sido participes en mi formación académica dentro de esta Institución pero de manera especial a nuestro director de Tesis Ing. Byron Carrión y al Ing. Wilson Quintuña.

Eugenia Llivigañay

Dedicatoria

Este proyecto de Tesis está dedicado de manera muy especial:

A Dios, por estar siempre a mi lado.

A mis padres, a los que sin su apoyo incondicional nada de esto no hubiese sido posible.

A mis hermanos, que me han incentivado y acompañado tanto de cerca como de lejos en todos los momentos de mi vida.

A mis abuelitos que al igual que el resto de mi familia siempre están pendientes de todas las cosas que me pasan y se alegran con cada triunfo que logro en mi vida.

A mis amigos y compañeros, que han compartido conmigo parte de sus vidas y con su amistad han sido participes en la culminación de este proyecto

Verónica Serrano

Agradecimientos

En primer lugar como no podía ser de otra manera a Dios por estar a mi lado a lo largo de mi vida y aunque seguramente no comparte muchas de mis actitudes siempre ha encontrado la manera de hacerse participe en cada paso que doy, frente a cada situación que se presenta.

A mis padres, a su esfuerzo económico pero sobre todo al apoyo incondicional que solamente unos padres como ustedes han sabido brindarme día a día, muchas gracias por todo siempre.

Gracias a mis hermanos, al que tengo cerca y a la que no, ¡Son un incentivo importante y constante en mi vida!

A mi gran amiga Eugenia con la cual he compartido éste proyecto, por tu paciencia, comprensión y amistad que en todo momento me enseña el valor de un verdadero amigo.

A todos mis familiares y amigos, gracias por estar presentes en mi vida.

A mis profesores, entre los que incluyo de manera especial al Ing. Byron Carrión y Wilson Quintuña por la oportuna ayuda que nos han brindado cuando más lo hemos necesitado.

Verónica Serrano

CERTIFICADO

El presente trabajo de tesis previo a la obtención del título de Ingeniero de Sistemas fue guiado satisfactoriamente por el Ing. Byron Carrión, quien autoriza su presentación para continuar con los trámites correspondientes.

Cuenca, 3 de Febrero del 2011

Ing. Byron Carrión

DIRECTOR DE TESIS

DECLARACIÓN DE RESPONSABILIDAD

Los conceptos desarrollados en este trabajo, así como todo el estudio e implementación de este Proyecto, son de exclusiva responsabilidad de los Autores.

Cuenca, 3 de Febrero del 2011

Eugenia Beatriz Llivigañay Pacheco

AUTOR

Verónica Gabriela Serrano Pinos

AUTOR

ÍNDICE DE CONTENIDOS

CAPÍTULO II

ARQUITECTURA DE PROTOCOLOS DE LA INTERNET (TCP/IP)

CAPÍTULO III

ANÁLISIS DE HERRAMIENTAS, PROTOCOLOS Y METODOLOGÍAS PARA MONITOREO Y CONTROL DE ANCHO DE BANDA

CAPÍTULO IV

DESARROLLO DEL SISTEMA

CAPÍTULO V

DESARROLLO DE IMAGEN CON DISTRIBUCIÓN GNU-LINUX

OBJETIVOS

General:

Analizar, diseñar e implementar un sistema en software libre para el monitoreo por usuario y aplicación del uso de ancho de banda en conexiones de Internet orientado a la pequeña y mediana empresa. Crear una imagen basada en GNU-Linux para su distribución.

Específicos:

- Proporcionar una herramienta para el control detallado del uso de ancho de banda por usuario y aplicación.
- Acoplar herramientas basadas en Software Libre que permita el control de tráfico en internet.
- Desarrollar una aplicación web de fácil manejo para la administración del sistema.
- Recolectar información en una base de datos para la generación de reportes.
- Generar reportes que permitan el análisis de datos históricos por rangos de fechas.
- Implementar control de alertas mediante mensajes por correo electrónico.
- Personalizar una distribución GNU-Linux mediante la creación de una imagen del sistema.

INTRODUCCIÓN

La elaboración de ésta tesis nace a partir de la necesidad de disponer con una herramienta que permita obtener información precisa, detallada y oportuna para el análisis del uso de la Internet dentro de la pequeña y mediana empresa.

Ésta necesidad se ve justificada debido a la importancia que tiene la Internet en la actualidad ya que está considerada dentro de los servicios informáticos más utilizados e influyentes de todos los tiempos.

Nos orientamos a soluciones hacia la pequeña y mediana empresa puesto que si bien existen dispositivos de red que cumplen con ésta función, representan una inversión demasiado costosa que no puede ser solventada fácilmente por este tipo de empresas.

Antes y durante el desarrollo de éste trabajo se evaluaron herramientas existentes, pero uno de los factores claves que intervenían era el costo puesto que la mayoría eran soluciones basadas en Software privativo llámese Windows y las que no, resultaban complejas de configurar o con muy escasa información.

Es por ello, que con éste proyecto de tesis lo que se buscó es integrar en un solo sistema las tareas de instalación, configuración y administración; que sea de fácil manejo por parte del usuario final y presente la documentación necesaria para su correcta utilización, como complemento de nuestro Sistema se añadieron módulos de alarmas vía mail y un portal de descarga y documentación. Qué mejor forma de

colaborar con el Software Libre, en el que creemos fielmente, que basarnos en una distribución GNU-Linux para su desarrollo.

La distribución escogida para la implementación total de nuestro sistema fue Debian por diversas razones, entre la que más destaca su estabilidad, también se realizó una distribución personalizada mediante la creación de una Imagen ISO que incluye un demo del Sistema.

Finalmente, a continuación presentamos el desarrollo de nuestra tesis que consta de 5 capítulos, cada uno de los cuáles ha sido estructurado de tal manera que sirva de base para el desarrollo del siguiente sucesivamente hasta llegar a la culminación del proyecto.

CAPÍTULO 1

Objetivos:

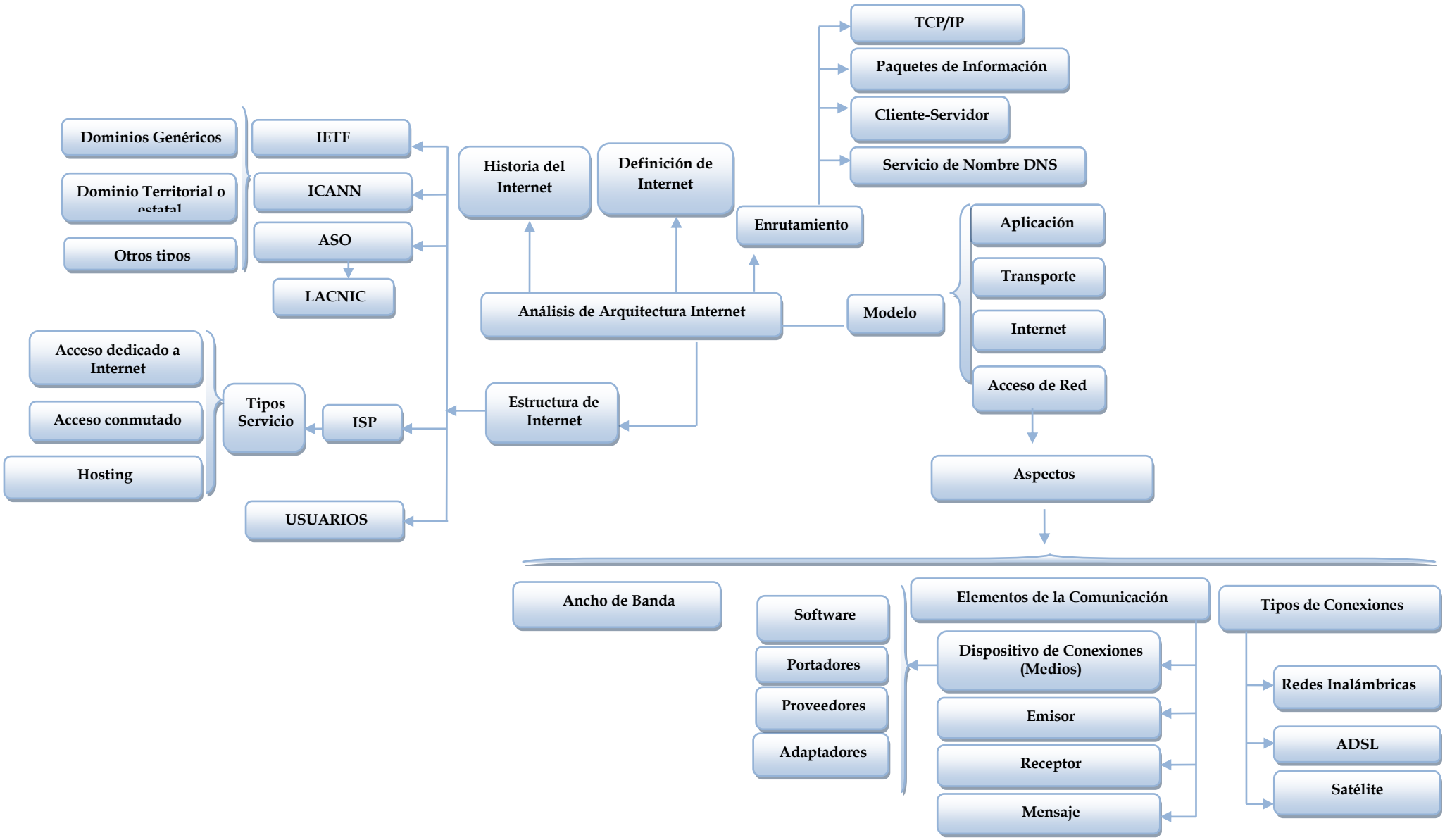
Objetivo General:

¬ Conocer la arquitectura del modelo TCP/IP a profundidad.

Objetivos Específicos:

- ¬ Analizar y estudiar aspectos importantes que abarquen el concepto de La Internet
- ¬ Observar la estructura que posee La Internet
- ¬ Profundizar un estudio del Modelo TCP/IP en la capa de Acceso de Red

Esquema (Mapa Conceptual)


TCP/IP
Paquetes de Información
Cliente-Servidor
Servicio de Nombre DNS
Enrutamiento
Dominios Genéricos
IETF
Dominio Territorial o estatal
ICANN
Otros tipos
ASO
LACNIC
Historia del Internet
Definición de Internet
Análisis de Arquitectura Internet
Modelo
Aplicación
Transporte
Internet
Acceso de Red
Acceso dedicado a Internet
Acceso conmutado
Hosting
Tipos Servicio
ISP
Estructura de Internet
USUARIOS
Aspectos
Ancho de Banda
Software
Portadores
Proveedores
Adaptadores
Elementos de la Comunicación
Dispositivo de Conexiones (Medios)
Emisor
Receptor
Mensaje
Tipos de Conexiones
Redes Inalámbricas
ADSL
Satélite

ANÁLISIS DE ARQUITECTURA DE LA INTERNET

Introducción

Aunque la idea inicial para la que fue creada la Internet ha variado considerablemente, hoy se ha convertido en uno de los servicios más utilizados por las personas a nivel mundial ya que nos permite una comunicación en tiempo real sin importar la zona geográfica en donde estén ubicados los entes participantes.

Es debido a la importancia de la que actualmente goza la Internet en el ámbito social, político, religioso, económico, etc., que hemos visto la necesidad de presentar en éste capítulo un estudio más detallado acerca de ésta herramienta. La comprensión adecuada de los puntos a evaluarse a lo largo de éste capítulo nos servirá de base para el desarrollo general de nuestro proyecto de tesis.

1.1 Historia de la Internet

En 1969, durante la guerra contra la Unión Soviética, el Departamento de Defensa de los EEUU se ve en la necesidad de crear DARPA (Agencia de Investigación de Proyectos Avanzados de Defensa) conformada por científicos e investigadores militares liderados por Licklider. De esta Agencia nace el proyecto denominado ARPANET que consistió en la creación de una red que descentralice las comunicaciones que hasta ese momento eran dirigidas hacia un servidor central, para tal propósito se utilizaron 4 computadoras.

Otra herramienta que fue esencial para dar origen a la Internet fue el e-mail, desarrollado en 1971 por Ray Tomlinson, que constaba de dos programas: un programa de mail como intra – máquina (SENDMSG) y otro experimental de transferencia (CPYNET).

Posteriormente, el profesor Vinton Cerf desarrolla TCP/IP, al que se lo adopta como protocolo en 1973 un año después de ser utilizado dentro del proyecto de

ARPANET para la conexión entre 40 computadores, con éste protocolo se pudo realizar una conexión fuera de los EEUU con NORSAR en Noruega.

Luego en 1983, UNIX integra TCP/IP dentro de su plataforma comercial con la versión 4.2, de ésta manera se convirtió en un protocolo estandarizado de la Internet obligando a los proveedores de éste servicio que lo adapten tanto en sistemas operativos como en equipos de comunicaciones. En la actualidad se presenta en UNIX, DOS, Windows, Macintoch, OS/2, AS/400 OS/400, Linux.

Para el año 1984, NSF (Fundación de Ciencias de los EEUU) da origen a NSFnet, con la finalidad de compartir la potencia de las supercomputadoras con la comunidad científica, quienes al ver que ARPANET se encontraba saturada crearon su propia infraestructura.

En 1990 ARPANET deja de existir, rebautizándose como INTERNET, servicio que en 1991 con la caída del muro de Berlín se abre para todo el mundo,

1.2 Definición de la Internet

Para una definición precisa es necesario analizar la diferencia entre Internet con "I" e internet con "i":

El internet, *"es un término genérico usado para determinar una serie de redes interconectadas"*[1]

La Internet, es una interconexión de redes con una infraestructura de servicios entre ellos la web es decir, *"una red especifica de ámbito mundial"*[1]

Analizando los dos conceptos propuestos podemos concluir que el término correcto a utilizar acorde a nuestro tema de tesis es: **la Internet**.

1.3 Modelos de la Internet.

Un modelo consta de una pila en la que cada capa alberga un sin número de protocolos, los mismos que desde un nivel inferior van corrigiendo los problemas relacionados con la transmisión de datos del nivel superior inmediato.

Existen dos modelos de la Internet:

OSI, considerado como referencia para fines educativos y **TCP/IP** que es el modelo sobre el que se basa la Internet.

- **Modelo OSI (Interconexión de Sistemas Abiertos):**

Su estudio se inició en 1984 por ISO (Organización Internacional de Estandarización creada en 1947), es un modelo base orientado a la enseñanza que utiliza un concepto en capas indicando los protocolos que se ejecutan en cada una de ellas.

Aunque estén relacionadas entre sí, cada capa se maneja de manera independiente, lo que significa que en caso de presentarse un problema la solución no altera el funcionamiento de las demás capas. Es empleado con la finalidad de facilitar la detección errores y la transferencia de datos.

El modelo OSI consta de 7 capas:

Tabla 1.1 Definición de las capas del Modelo OSI

Capa	Descripción
Física	Se encarga de establecer los métodos necesarios para la transmisión del flujo de datos a través de un medio físico. Se presenta en dos casos en una transmisión:[1] - **Decodificación:** Se encarga de convertir la información binaria que viaja por la red en impulsos acordes con el canal de

[1] FOROUZAN, BEHROUZ A.; COOMBS, CATHERINE; CHUNG FEGAN, SOPHIA, Transmisión de datos y redes de comunicaciones

	comunicación que tenga en una transmisión. ¬ **Codificación:** Se procede a transformar los impulsos eléctricos provenientes de los medios de comunicación en paquetes de datos binarios que serán enviados a la capa de enlace de datos.
Enlace de datos	Permite que la capa física aparezca como un medio fiable al ser libre de errores. Debido a que cumple con las siguientes funciones: ¬ **Control de errores:** Es utilizada con la finalidad de volver a transmitir en caso de la existencia de tramas defectuosas o si se han perdido alguna de ellas, también se la utiliza para controlar la duplicación de tramas, contando con: ¬ Técnicas de detección ¬ Técnicas de corrección ¬ **Control de flujo:** asegura que los paquetes entre receptor y emisor viajen a una velocidad parecida, previniendo de esta manera el desbordamiento de paquetes del receptor. ¬ **Control de acceso al medio:** determina que dispositivo tiene el control de la transmisión. ¬ **Tramado:** crea tramas, al dividir los bits recibidos
Red	Se encarga de hacer que los paquetes lleguen desde el origen al destino tratándolos independientemente a cada uno de ellos al proporcionar conectividad y siguiendo la dirección adecuada a través de la Internet, mediante la utilización de dispositivos de conexión. Esta capa tiene las siguientes responsabilidades: ¬ **Direccionamiento:** este nivel permite añadir un nuevo campo al paquete donde incluye la dirección lógica tanto del origen como del destino, así como la solicitud de servicios ¬ **Enrutamiento:** mediante la utilización de dispositivos de enrutamiento permite que los paquetes lleguen a su destino final.
Transporte	Permite la transferencia para que el mensaje llegue tal y como fue entregado por el receptor. Debido a que en esta capa se realiza: ¬ **Control de errores:** hace que el mensaje llegue al receptor sin pérdidas, daños o duplicaciones. Se lo realiza end to end y no solo en un único enlace.

	¬ **Control de flujo:** previene el desbordamiento de paquetes. Se lo realiza end to end y no solo en un único enlace. ¬ **Segmentación:** Se refiere a cuando el mensaje es dividido en segmentos que contienen numeración, lo que le permite unificar al mensaje correctamente en el destino y en el caso de pérdida se pide que el paquete sea retransmitido. ¬ **Multiplexación de Aplicaciones:** cuando un mensaje viene de diferentes aplicaciones, estos utilizan un mismo flujo que se dirija a la capa de red. Para lo cual se requiere la utilización de un identificador.
Sesión	Utiliza mecanismos que permitan controlar que el dialogo y las actividades sean a nivel de aplicación de los sistemas finales. Proporcionando los siguientes servicios: ¬ **Control de dialogo**: Permite que la comunicación sea: ¬ **Half - Dúplex:** se realiza la comunicación en un sentido a la vez. O bien envía o bien recibe. ¬ **Full – Dúplex:** comunicación en ambos sentidos al mismo tiempo. ¬ **Agrupamiento:** Permite la definición de grupo de datos ¬ **Recuperación:** Se retransmite la información desde la última parte que fue considerada como libre de errores.
Presentación	Se encarga de que el mensaje que van a ser utilizadas por las aplicaciones utilicen los formatos adecuados (semántica y la sintaxis) para su transmisión. Responsabilidades: ¬ **Traducción:** En el emisor la información es cambiada a sistemas de codificación entendibles para el computador, y el receptor hacer una traducción inversa para que se presente como el mensaje original ante el receptor. ¬ **Cifrado:** es la conversión de un mensaje en un nuevo formato con la finalidad de asegurar privacidad. ¬ **Compresión:** merma la cantidad de bits a ser transmitidos.

Aplicación	Permite tanto a software como a usuarios el acceso a la red. Proporcionando interfaces de usuario así como protocolos que manejan programas como http, smtp, imap, etc.

Figura 1.1. Capas del Modelo OSI

Fuente: http://frikeando007.files.wordpress.com/2008/07/350px-pila-osi-es_svg1.png, http://es.wikipedia.org/wiki/Modelo_OSI

- **Modelo TCP/IP:**

  Los dos protocolos que conforman sus siglas son:

  - **TCP (***"Protocolo de Control de Transmisión")*

    Es el encargado de asegurar que los datos transmitidos lleguen correctamente y en el orden establecido, lo hace mediante el control de un ACK (acuse de recibo).

- **IP** *("Protocolo de Internet")*
  Define el rango de direccionamiento de la Internet, considerando que a cada host le corresponde una IP.

En base a las funciones que cumplen los protocolos anteriormente citados presentamos un breve concepto sobre TCP/IP:

TCP/IP abarca a un conjunto de protocolos de red en los que se basa la Internet, es un estándar que permite la comunicación origen-destino entre diferentes ordenadores, siendo compatible con cualquier hardware y Sistema Operativo.

Este modelo utiliza cinco capas:

Tabla 1.2. Definición de las capas del Modelo TCP/IP

Capas	Descripción
Capa Física	Se encarga de definir los medios de comunicación, velocidad, etc., a ser utilizados durante una transmisión.
Capa de Acceso a la Red	Se encarga de intercambiar la información entre usuarios finales.
Capa de Internet	Enruta los paquetes por diferentes caminos perteneciente a la Internet
Capa de Transporte	Permite intercambiar mensaje de una manera fiable, ya que permite que reciba el mensaje en el mismo orden como fue enviada por el emisor.

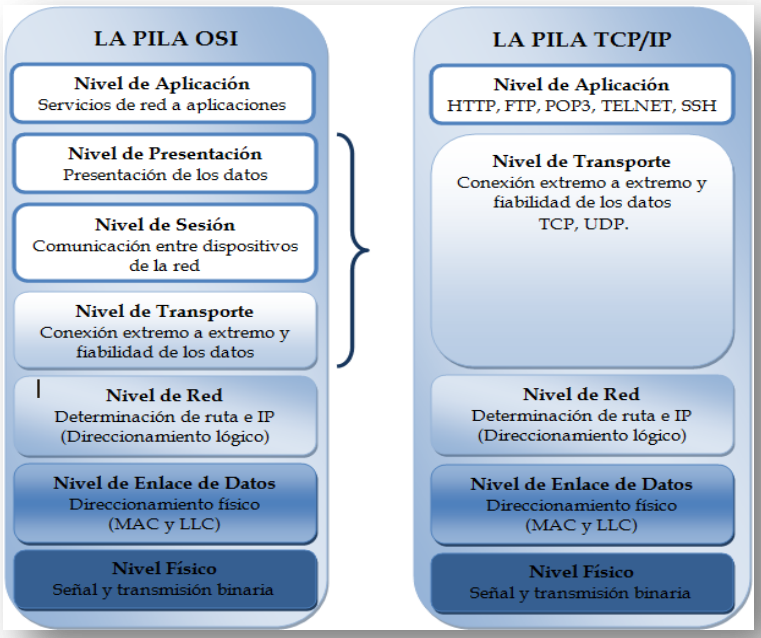
Capa de Aplicación	Brinda aplicaciones para que sean utilizadas por el usuario.

Figura 1.2. Estructura de modelo TCP/IP

Fuente: http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

Un estudio más detallado de éste modelo se desarrollará en el capítulo 2.

Figura 1.3. Cuadro comparativo entre el modelo OSI y TCP/IP



Fuente: http://facusdelacruz.wordpress.com/2008/11/16/ipsec-seguridad-en-layer-3/

1.4 Enrutamiento

Es la forma como un paquete busca posibles caminos en todas las rutas existentes dentro de una red para llegar a un destino, siempre tratando de utilizar la más óptima. Esto se lo realiza a nivel de la Capa 3 del modelo TCP/IP (Capa de Red).

El software que decide qué ruta tomar se denomina router, también existe el switch que es otro medio de enrutación más rápido que trabaja a nivel de hardware y no utiliza tablas de enrutamiento como lo haría un router.

1.5 Estructura de la Internet

En la estructura de la Internet intervienen las siguientes entidades:

IETF (Grupo Especial sobre Ingeniería de Internet).

Es una organización sin fines de lucro con la capacidad de realizar modificaciones sobre los parámetros técnicos de la arquitectura y protocolos que intervienen en el correcto funcionamiento de la Internet.

ICANN (Corporación de Internet para la Asignación de Nombres y Números)

Organización sin fines de lucro, encargada de funciones como:

- Asignación de direcciones numéricas IP (Protocolo de Internet) e identificadores de protocolo.

- Gestión y administración del sistema de nombres de dominio y códigos de países.
- Administración de servidores raíz.

ASO (Organismos de Soporte a Direcciones)

Son los encargados de formular políticas para las direcciones IP. Apoyan a miembros de ICANN.

LANIC (Registro de Direcciones de Internet para América Latina y Caribe)

Entre otras funciones, es la entidad encargada de asignar y administrar las direcciones IP para América Latina y el Caribe, en forma abierta y transparente.

ISP (Proveedor de Servicios de Internet)

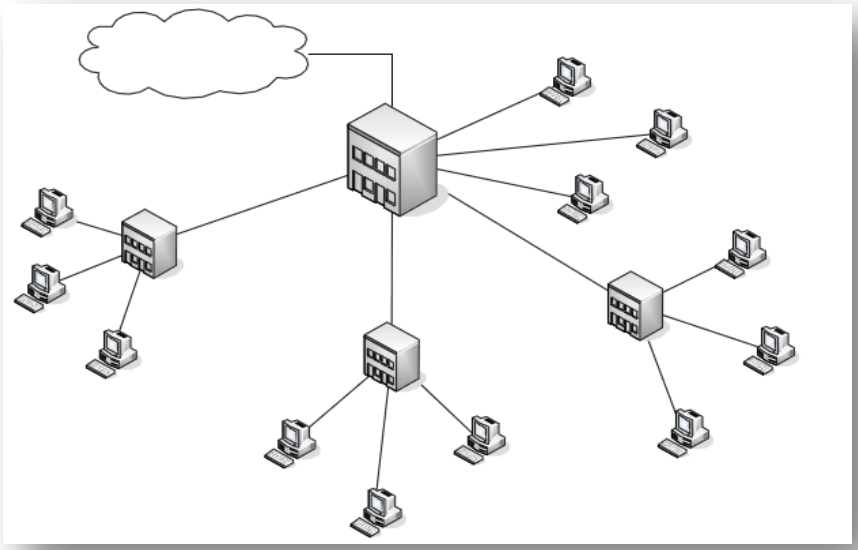
Empresa que brinda a sus clientes conectividad hacia la Internet mediante la utilización de tecnologías como DSL, Dial-up, etc.

Tipos de ISP:

- **Por la cobertura Geográfica**
  - **ISP local**

    Consiste en una oficina central encargada de administrar y suministrar la Internet a los diferentes proveedores locales mediante la utilización de servidores y ruteadores. Su cobertura abarca el área de una ciudad o parte de ella.

Figura 1.4. Esquema de un ISP local

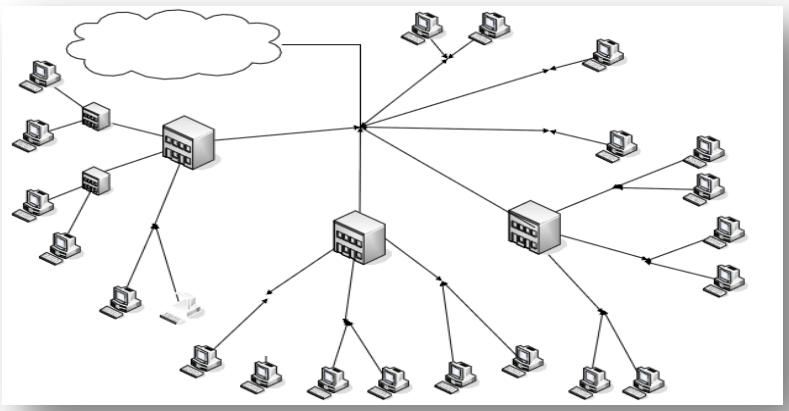


Fuente:
http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/751/14/T10506CAP1.pdf

¬ **ISP Regional**

La infraestructura de este tipo de ISP es de mayor complejidad y robustez que el anterior, brinda cobertura en todas aquellas ciudades en las que el ISP opera. Consta de varias oficinas centrales, regionales y locales interconectadas entre sí.

Figura 1.5 ISP Regional



Fuente: http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/751/14/T10506CAP1.pdf

- **ISP Nacionales o Internacionales**

  Los ISP nacionales cubren el área de un país y los internacionales el área de varios países, se caracterizan por contar con su propia infraestructura de telecomunicaciones que accede al backbone principal de Internet, sus clientes llegan a ser grandes compañías proveedoras de servicios de interconexión.

  Dentro de esta categoría se pueden presentar los siguientes ISPs:

  - **ISPs Integrados:** Cuando los ISP regionales crecen al unir varias oficinas centrales convirtiéndose en redes de gran velocidad.
  - **ISPs de Acceso Outsourced:** Alquilan proveedores locales, reduciendo costos y brindando un mejor servicio a sus clientes.
  - **Multimodo:** Proporcionan una mayor cobertura y servicios debido a que son empresas telefónicas con una infraestructura propia.

Servicios que proporcionados por los ISP

A continuación se describen algunos de los servicios que ofrecen los ISP:

- **Servicio de Acceso dedicado a Internet**

  Es un tipo de conexión flexible que permite a todos los usuarios iguales derechos dentro de la Internet, es muy costosa y necesita de una estructura de mantenimiento para la red, una vez que el usuario esté conectado el proveedor solo se responsabiliza del enrutador y la línea telefónica, más no de lo que suceda con su red.

- **Servicio de Acceso conmutado**

  El equipo de cómputo no forma parte de la Internet, pero si accede a un servicio que se conecta de manera permanente a la red, como se comparte la

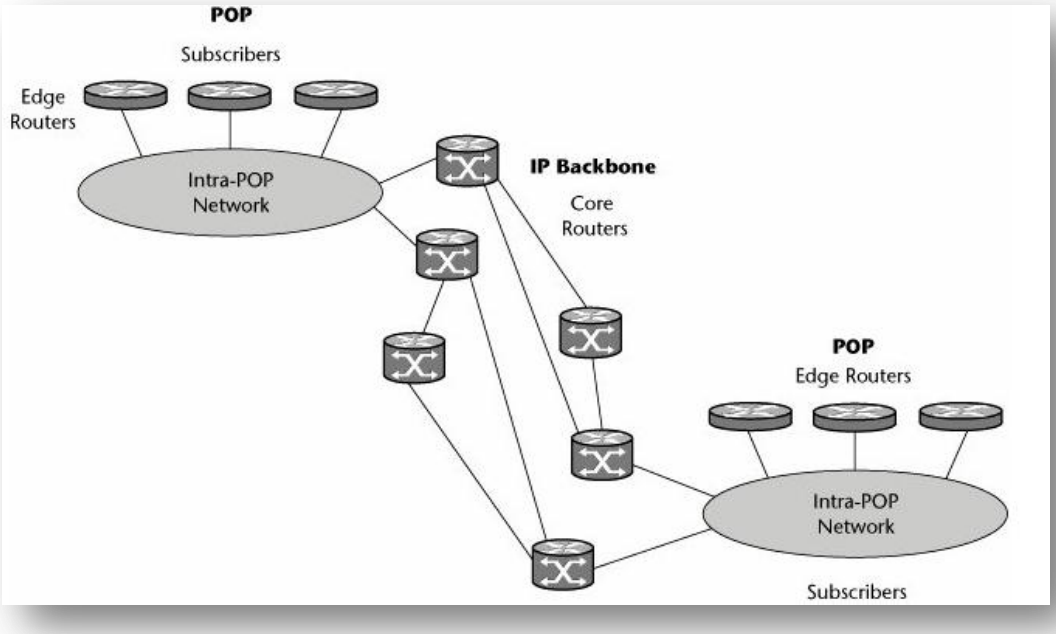
conexión con otros usuarios el valor por dicho servicio disminuye. Los proveedores tienen la capacidad de limitar tanto las aplicaciones de Internet como la cantidad de espacio en disco a utilizar.

¬ **Servicio de Hosting**

Este servicio proporciona espacio en un servidor para que una empresa pueda hospedar su sitio web durante las 24 horas del día, garantizándole de ésta manera su presencia en Internet y otorgándole todas las facilidades de gestión para que las peticiones de todos sus usuarios sean oportunamente atendidas.

Una vez que tenemos una idea clara sobre lo que es un ISP se comienza a analizar la arquitectura de red de un ISP ilustrada de la siguiente manera:

Figure 1.6. Arquitectura de red de un ISP



Fuente: Addison.Wesley.Telecommunications.Essentials.2nd.Edition.Oct.2006.chm

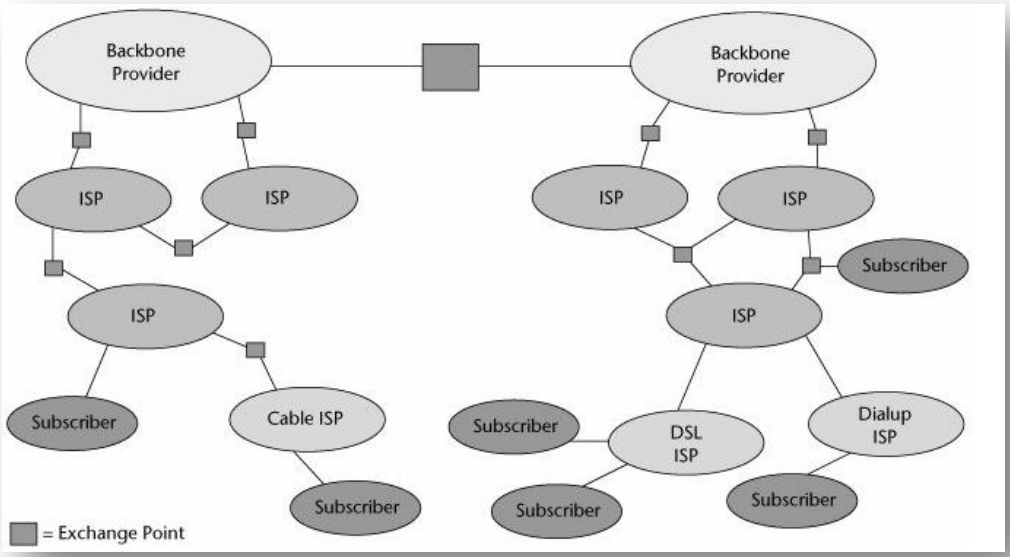
En la **Figura 1.6** observamos una estructura de un ISP backbone que lo describiremos a continuación.

- **ISP backbone:** tiene un núcleo compuesto de una serie de routers y de enlaces de transmisión entre ellos.

"Por ejemplo el ISP backbone sirve para el nivel más alto de la jerarquía y provee conectividad entre las decenas de miles de ISP de todo el mundo.

Debajo de ellos existen varias clases de ISP's, incluyendo aquellos que pueden cubrir grandes áreas y cuentan con apoyo tanto de clientes de negocios como de los consumidores base. Así como los ISP locales que centran sus servicios y precios bajos a comunidades pequeñas en vez de proveer a las empresas"[2].

Figura 1.7. Composición del Internet



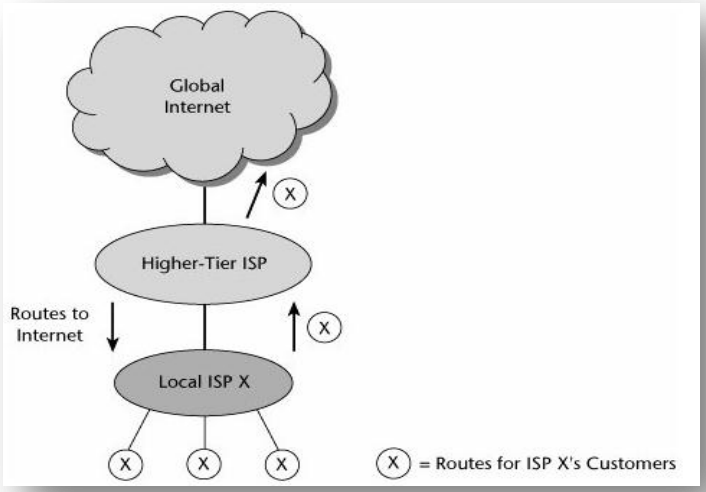
Fuente: Addison.Wesley.Telecommunications.Essentials.2nd.Edition.Oct.2006.chm

Los ISP's compiten basados en el "*nombre de la marca, servicios de valor añadido, rendimiento, fiabilidad, precio, servicio al cliente y otros factores.*

[2] Addison.Wesley.Telecommunications.Essentials.2nd.Edition.Oct.2006.chm

La conexión de Internet depende de la cooperación privada que existe entre los ISP y estos a su vez requieren relaciones comerciales, interconexiones físicas, capacidad para enrutar información y políticas de pago"[3].

Figura 1.8. ISP arquitectura de tránsito



Fuente: Addison.Wesley.Telecommunications.Essentials.2nd.Edition.Oct.2006.chm

En esta gráfica se observa ISP's de nivel inferior o proveedores locales que se conectan a los ISP de nivel superior, y estos están conectados a la Internet. Los ISP de nivel bajo pagan tarifas de tránsito a los grandes proveedores para tener acceso a las tablas de enrutamiento global.

1.6 Capa de Acceso de Red del Modelo TCP/IP.

- **Ancho de Banda:**

Es la cantidad de información que se transmite a través de una red en un tiempo determinado, lo que significa que a mayor ancho de banda mayor velocidad de transmisión y número de usuarios que se conecten a la vez.

Se mide en:

- Bits por segundo (bps)

[3] Addison.Wesley.Telecommunications.Essentials.2nd.Edition.Oct.2006.chm

- Kilobits por segundo (Kbps)
- Megabits por segundo (Mbps)

Su desempeño depende de factores como:

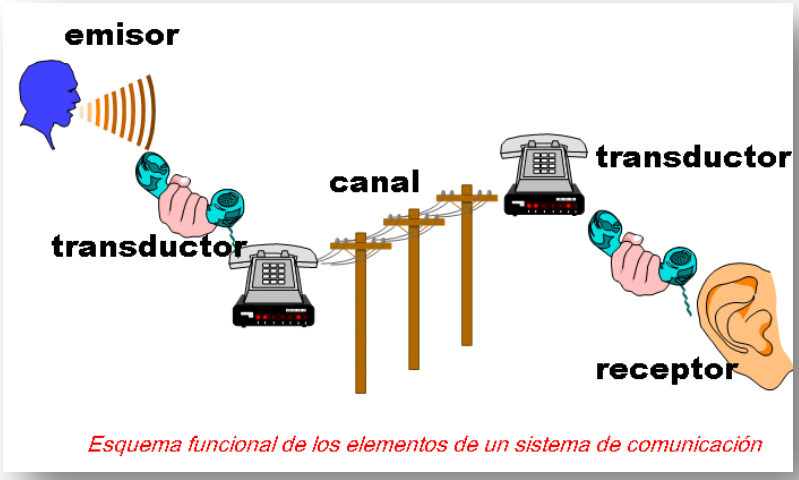
- Medio físico
- Cantidad de tráfico,
- Protocolos de software
- Tipo de conexión de la red

- **Elementos de la Comunicación**

¿Qué es la Comunicación?

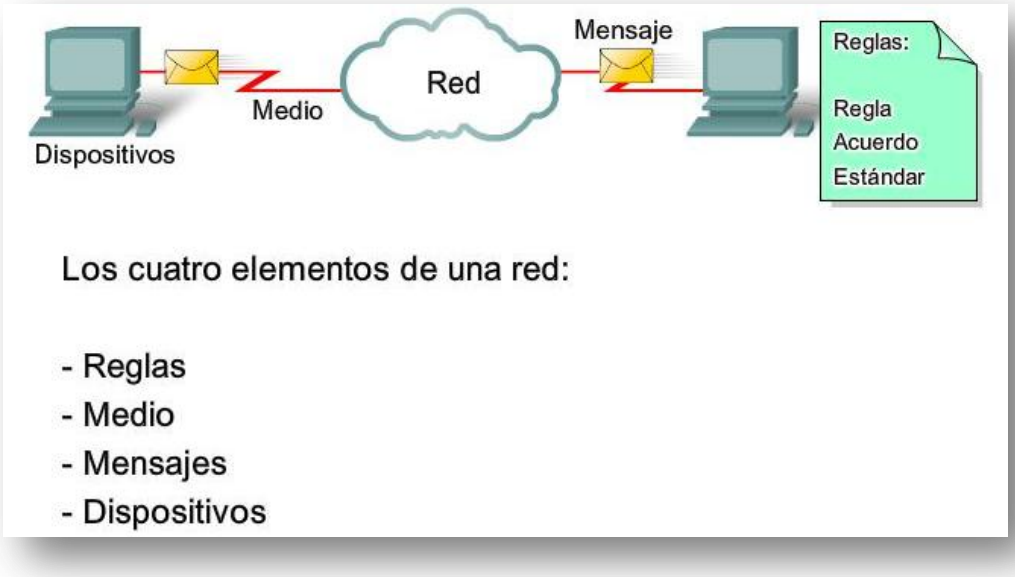
En el campo informático se refiere a la transmisión de datos entre dos o más entidades a través de la utilización de un medio (cables–medios inalámbricos).

Figura 1.9. Elementos de la comunicación



Fuente: http://html.rincondelvago.com/proceso-telematico-o-teleinformatico.html

Figura 1.10. Intervención de los Elementos de la Comunicación



Fuente: http://www.taringa.net/posts/info/3887809/Elementos-de-una-Red-!!!.html

Elementos: Dentro de la comunicación se tienen los siguientes componentes:

1. **Dispositivos:** Elementos que cumplen las funciones de:

   - **Emisor:** cuando se lo utiliza para enviar un mensaje ó
   - **Receptor:** cuando es quien recibe el mensaje.

   Ejemplos de dispositivos que intervienen en la comunicación:

   - **Switch**

Figura 1.11. Switch

Fuente: http://www.monografias.com/trabajos7/swich/swich.shtml

Permite la interconexión de múltiples redes que transportan los datos entre segmentos según la dirección MAC del destino, este trabaja a nivel de la capa de red.

- **Router**

Figura 1.12. Router Inalámbrico

Fuente: http://darkub.wordpress.com/2008/01/19/diferentes-tipos-de-dispositivos-de-redes/

Trabaja al nivel de la capa 3, este dispositivo permite determinar la ruta a tomar y encamina los paquetes hacia su destino. Con este dispositivo se puede controlar la seguridad, el acceso de los dispositivos así como su administración.

- **Host.**

Se puede decir que un host es cualquier equipo conectado a la red.

- **Servidor.**

Figura 1.12: Computador Servidor

Fuente: http://darkub.wordpress.com/2008/01/19/diferentes-tipos-de-dispositivos-de-redes/

Es un computador que tiene programas para manejar una red y provee de servicios a otros equipos que realizan las peticiones, utilizan sistemas operativos como Windows, Red Hat, Open Suse, etc.

- **Cliente:** Es el computador que hace peticiones al servidor.

2. **Reglas:** Protocolos que se utilizan al momento de transmitir un mensaje.

3. **Mensaje:** Datos que van a ser transmitidos por ejemplo: texto, gráficos, videos, etc.

4. **Medio:** Ruta física por la que viaja la información entre el emisor y receptor, puede estar ubicado en diferentes zonas geográficas.

Clasificación de los Medios:

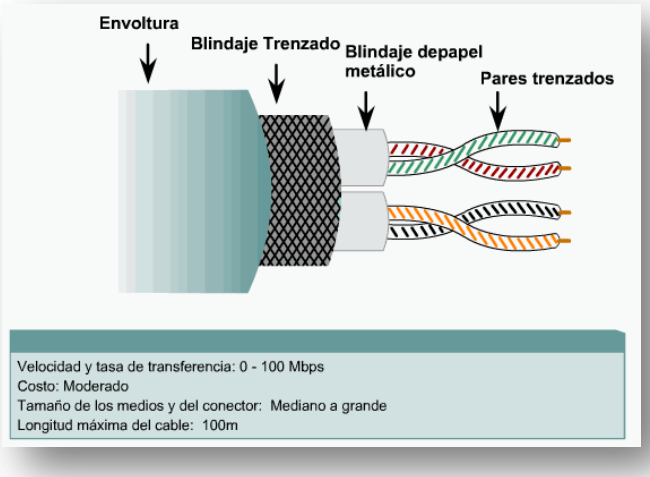
Medios Guiados.- El componente que se utiliza para la difusión del mensaje es físico y de contextura sólida, por ejemplo:

- **Cable de par trenzado.**

  Está conformado por pares de líneas de cobre separados por cubiertas de plástico de color que sirve para su identificación, entrelazados de manera espiral.

  - En cada par existe la línea que transmite la señal y la que le envía a tierra.
  - Se lo utiliza en telefonía y en sistemas de conexiones de red (LAN).
  - En una LAN alcanza una velocidad de 10Mbps, aunque según el entrelazado del cable puede llegar hasta los 1Gbps.
  - Respecto a otros medios, el par trenzado cubre distancias cortas y alcanza velocidades de transmisión bajas.
  - En transmisiones a larga distancia su velocidad alcanza los 4Mpbs.

Figura 1.13. Cable par trenzado



Fuente: http://zafiro17.blogspot.com/

- Durante la transmisión es susceptible al ruido e interferencias que según la manera de cómo los cables se trencen pueden disminuir o eliminarse.

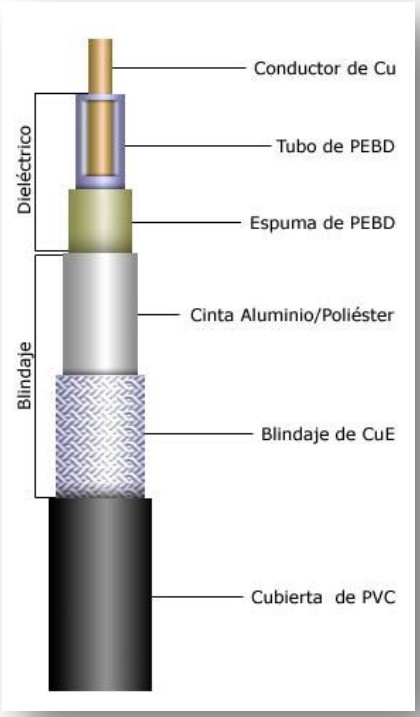
Se muestra en diferentes presentaciones como:

- **Par Trenzado sin blindaje (UTP- Unshield Twisted Pair).-** Es el que mayormente se utiliza por su bajo costo y fácil maniobrabilidad e instalación. Es susceptible a la interferencia electromagnética debido a que no cuenta con un apantallado.
  La Asociación de Industrias Electrónicas (EIA) las separo por categorías comprendidas entre el 1 al 5 según su calidad, siendo el de mayor transcendencia el de ***Categoría 5*** los mismos que son diseñados para soportar frecuencias de hasta 100MHz y alcanzar velocidades de hasta 100 Mbps. Debido al rango de frecuencia que utiliza se lo usa como un medio para transportar tanto datos como voz.

- **Par Trenzado con blindaje (STP- Shield Twisted Pair)**
  En cada par de líneas entrelazadas es protegido por una malla o funda conductora de metal, que elimina el ruido electromagnético e interferencias, puede alcanzar una mayor velocidad de transmisión aunque es más costoso y difícil de manipular.

¬ **Cable coaxial**

Figura 1.14. Cable Coaxial

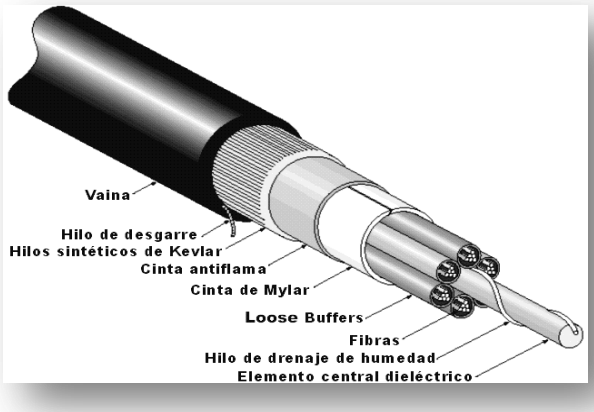


Fuente: http://zafiro17.blogspot.com/

Su velocidad oscila los 550Mbps a distancias entre 10-100Km., éste cable posee un núcleo de cobre recubierto por material aislante de ruido en una cubierta de plástico, es más costoso y rígido que un par trenzado. Se clasifica según el Radio Gobierno (RG), que es un estándar propio de los cables coaxiales donde se determinan los aspectos físicos como el grosor, tipo de cubierta, etc...Entre los más utilizados para conexiones Ethernet están los de contextura gruesa RG-8, RG-9, RG-11, RG-58.

- **Cable de Fibra óptica**

Figura 1.15. Fibra Óptica



Fuente: http://zafiro17.blogspot.com/

Tiene un núcleo que está compuesto ya sea por fibra de vidrio o plástico en donde se conducen los pulsos luz que representan los datos a ser transmitidos, alcanza velocidades de alrededor de 2Gbps con un ancho de banda de 2GHz, su cobertura es de aproximadamente 40km por tierra brindando una buena calidad en la transmisión. El tamaño de este medio es de aproximadamente 0.1mm y se compone de tres secciones:

- **Núcleo:** parte interna compuesta de una o más fibras con un espesor de 8 a 100 micras.

- **Revestimiento:** Es otro tipo de cristal o plástico con propiedades distintas al núcleo. Al separarse del núcleo, actúa como un reflector, limitando así al haz de luz para que viaje dentro del núcleo.

- **Cubierta:** es una protección hecha de plástico contra la humedad, etc.

Medios no guiados

- **Medios inalámbricos: Microondas Terrestres**

Figura 1.16. Microondas Terrestres

Fuente:

http://www.google.com.ar/url?sa=t&source=web&cd=10&ved=0CEAQFjAJ&url=http%3A%2F%2Fjemarinoi.googlepages.com%2F9.-ComunicacionyRedes.ppt&rct=j&q=elementos+de+la+comunicacion+en+redes&ei=HRUgTIvCD4L48Aauuf16&usg=AFQjCNHbKDZ8IP8_IjtuWeIr2ZS6gdaSrQ

La transmisión de datos se da por medio de ondas de radio que siguen dos frecuencias en direcciones contrarias, cada frecuencia cuenta con su transmisor y receptor que combinados origina el transceptor, mientras más altas sean las antenas mayor distancia recorrerá la señal libre de interferencias. Pueden ser instaladas sobre montañas o colinas, para que este medio cuente con un mayor alcance utiliza

repetidores en cada antena, lo aconsejable es utilizarlos cada 20 millas debido a la curvatura de la tierra.

1.7 Tipos de Conexiones hacia la Internet:

- **Red Inalámbrica**

La transmisión se da mediante ondas electromagnéticas evitando así la manipulación de cable físico, para envío y recepción de mensajes utiliza los puertos.

Tabla 1.12: Tabla comparativa de Redes Inalámbricas

Especificación	Estatus	Máxima tasa de bits	Frecuencia de operación
IEEE 802.11	Utilizado por la mayoría de fabricantes de WLANs.	2 Mbps	2.4 GHz
IEEE 802.11b	Especificación reciente	11 Mbps	2.4 GHz
IEEE 802.11a	En desarrollo	24 – 54 Mbps	5.0 GHz
HiperLAN	Desarrollado por ETSI	24 Mbps	5.0 GHz
Bluetooth	Promovido por 3Com, Ericson, IBM, Intel Microsoft, Motorola, Nokia y Toshiba.	1 Mbps	2.4 GHz

IEEE: Institute of Electrical and Electronic Engineers

ETSI: European Telecommunications Standards Institute

Fuente: http://tutorial.galeon.com/inalambrico.htm#_Toc68830817

En este tipo de conexiones se pueden presentar los siguientes elementos:

- **Access Point:** es un dispositivo que funciona como estación base que brinda cobertura a los usuarios conectados a esta red inalámbrica.

- **Dispositivos clientes:** se refiere a cada uno de los hosts que poseen una tarjeta para redes inalámbricas.

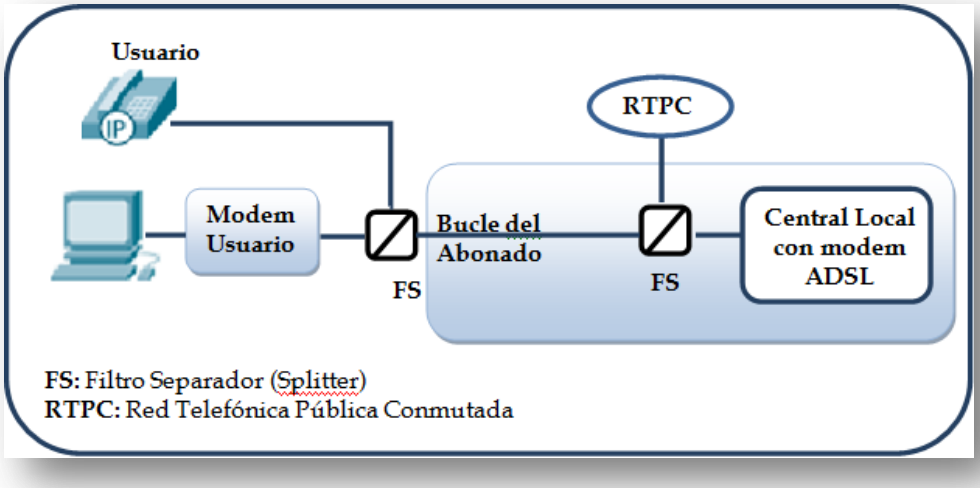
- **ADSL**

  Sus siglas significan Abonado Digital Asimétrica, esta conexión utiliza una línea telefónica convencional para la transmisión de la señal, la misma que es modulada a una frecuencia más alta que permita obtener un acceso a Internet de banda ancha.

  Este tipo de conexión cuenta con tres canales que funcionan de manera independiente, los dos primeros canales son de velocidad, uno para el envió de datos y el otro de mayor velocidad para la recepción, finalmente un tercer canal es utilizado para el servicio telefónico.

  Alcanza velocidades de hasta 8Mbps. Si la distancia entre el modem del usuario y la central local sobrepasa los 3 kilómetros pierden calidad y la tasa de transferencia baja.

Figura 1.17 Conexión ADSL



Fuente:http://www.isftic.mepsyd.es/w3/programa/usuarios/ayudas/tipo_conexion.htm#adsl

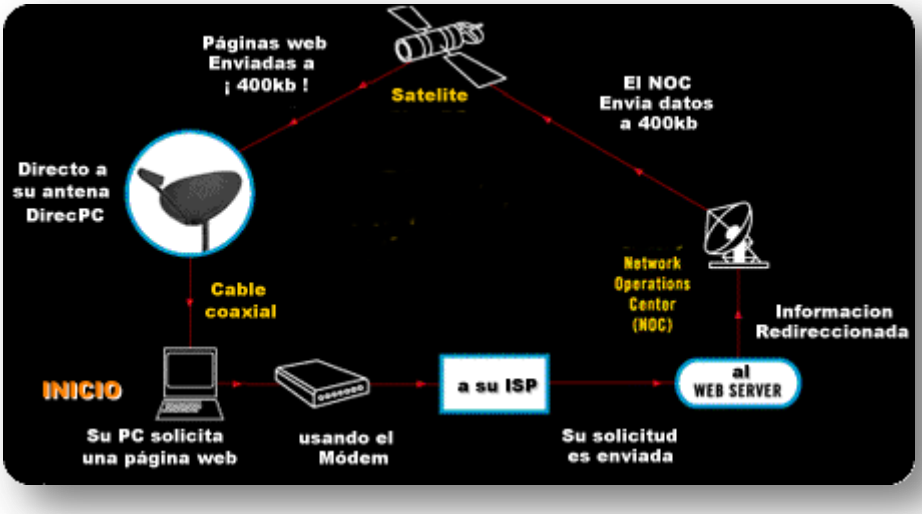
¬ **Satelital**

Cuenta con dispositivos que se encuentran ubicados en la órbita alrededor de la Tierra. En tierra firme existe una estación emisora que envía los datos hacia el satélite que amplifica la señal y la reenviar con diferente frecuencia a la estación receptora de la tierra.

Para realizar este tipo de conexiones se emplea una combinación hibrida que requiere la presencia de un satélite, una antena parabólica, un acceso telefónico a Internet como por ejemplo ADSL, y la subscripción a un proveedor satelital.

La velocidad en la que se puede transmitir los datos mediante un satélite puede alcanzar los 400 Kbps.

Figura 1.18. Conexión Satelital



Fuente: http://www.isftic.mepsyd.es/w3/programa/usuarios/ayudas/tipo_conexion.htm#satelite

Conclusiones:

Una vez culminado éste capítulo que nos permitió conocer más a detalle conceptos relacionados con la Internet así como la estructura de los modelos OSI y TCP/IP, brindando mayor énfasis a la capa de acceso a la red de éste último, nos preparamos para el siguiente.

CAPÍTULO 2

Objetivos:

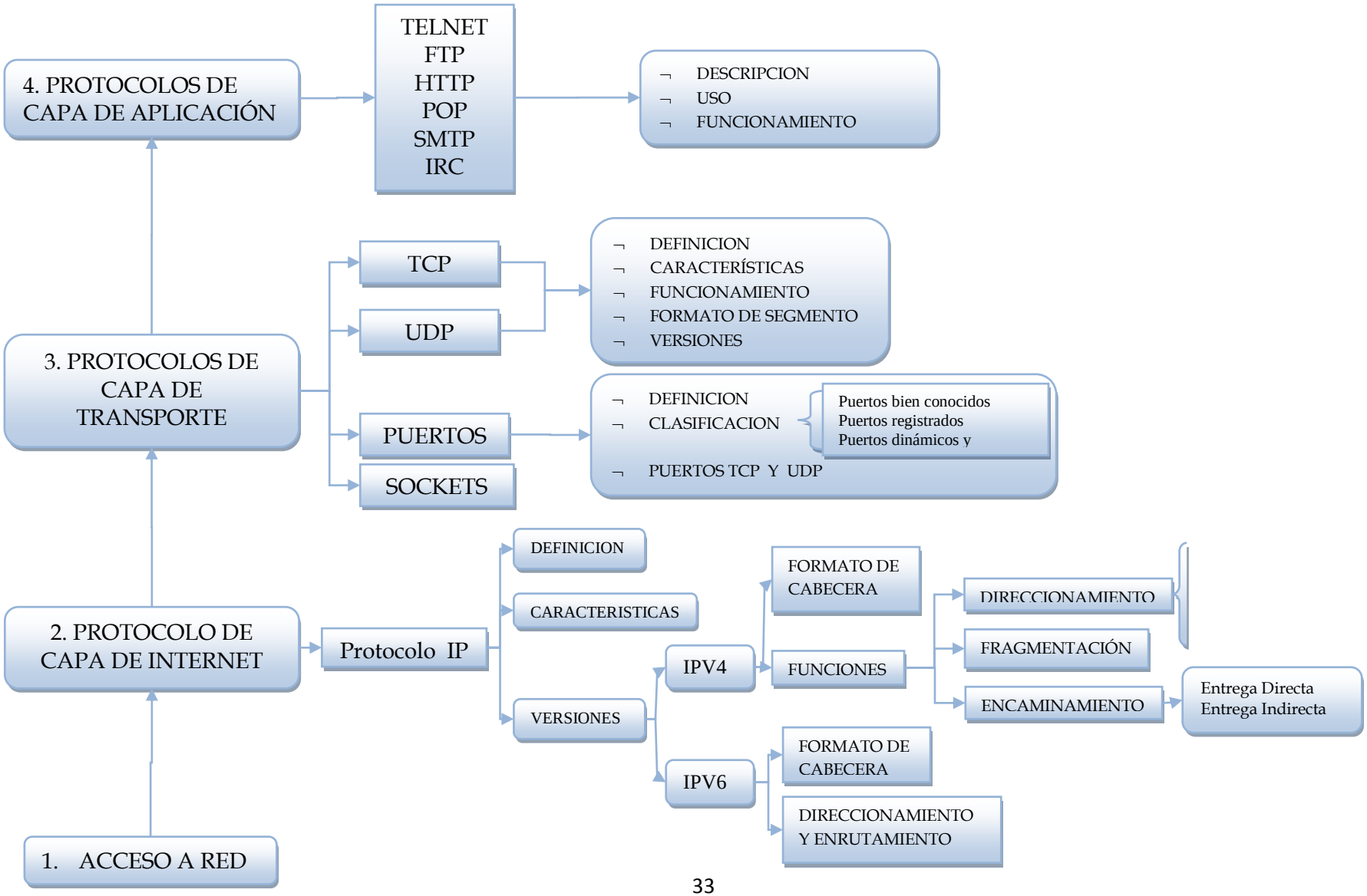
Objetivo General:

- Realizar un estudio avanzado sobre los protocolos más importantes de las capas superiores del Modelo OSI.

Objetivos Específicos:

- Determinar las características y estructura de una IP.
- Investigar sobre los protocolos de la capa de Transporte
- Realizar un estudio de los protocolos más utilizados de la capa de Aplicación por los usuarios de la Internet.

Esquema Capitular (Mapa Conceptual):


4. PROTOCOLOS DE CAPA DE APLICACIÓN
TELNET
FTP
HTTP
POP
SMTP
IRC
¬ DESCRIPCION
¬ USO
¬ FUNCIONAMIENTO
3. PROTOCOLOS DE CAPA DE TRANSPORTE
TCP
UDP
PUERTOS
SOCKETS
¬ DEFINICION
¬ CARACTERÍSTICAS
¬ FUNCIONAMIENTO
¬ FORMATO DE SEGMENTO
¬ VERSIONES
¬ DEFINICION
¬ CLASIFICACION
Puertos bien conocidos
Puertos registrados
Puertos dinámicos y
¬ PUERTOS TCP Y UDP
2. PROTOCOLO DE CAPA DE INTERNET
Protocolo IP
DEFINICION
CARACTERISTICAS
VERSIONES
IPV4
IPV6
FORMATO DE CABECERA
FUNCIONES
DIRECCIONAMIENTO
FRAGMENTACIÓN
ENCAMINAMIENTO
Entrega Directa
Entrega Indirecta
FORMATO DE CABECERA
DIRECCIONAMIENTO Y ENRUTAMIENTO
1. ACCESO A RED

ARQUITECTURA DE PROTOCOLOS DE LA INTERNET (TCP/IP)

Introducción:

En este capítulo nos centraremos al estudio detallado de los protocolos más importantes de cada una de las capas de modelo TCP/IP citado anteriormente, para ello partiremos desde la capa 2 hacia adelante ya que es ahí donde comienzan las operaciones de los distintos protocolos, además porque si recordamos la capa de acceso a la red que comprendían los enlaces físicos y tipos de conexiones hacia la Internet se vieron a detalle a lo largo del capítulo 1.

Es muy importante tener una idea clara de lo que son estos protocolos, la función que cumplen dentro de cada capa del modelo TCP/IP y la manera en que lo hacen puesto que ello nos ayudará a la comprensión de conceptos que nos guiarán durante el desarrollo de la tesis en lo posterior.

Niveles TCP/IP:

Figura 2.1 Niveles TCP/IP

CAPAS	PROTOCOLOS
4. APLICACIÓN	HTTP,FTP,TELNET,ICR,POP3,SMTP
3. TRANSPORTE	TCP, UDP
2. INTERNET	IP
1. ACCESO A LA RED	Ethernet- IEEE

Fuente: http://www.saulo.net/pub/tcpip/a.htm

Protocolo[4]

Es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.

Modelo TCP/IP Capa de Internet.

El protocolo más representativo de ésta capa es el Protocolo Internet (IP), el mismo que cuenta con 2 versiones, la 4 que se utiliza en la actualidad y la 6 considerado de la nueva generación, ambos detallados a continuación.

2.1 Protocolo IP.

2.1.1 Definición.

El Protocolo Internet (IP), trabaja a nivel de la capa de internet del modelo TCP/IP, tanto en dispositivos finales como enrutadores permitiendo el desarrollo y transporte de los datos en datagramas, sin garantizar su entrega.

Datagrama IP.- Es la unidad básica de transmisión en la Internet, son bloques de datos conocidos también como paquetes.

Formato de Datagrama: Están conformados del encabezado y datos

Formato de Datagrama:

Encabezado	Datos

[4] **Protocolo (informática):** http://es.wikipedia.org/wiki/Protocolo_%28inform%C3%A1tica%29

2.1.2 Funciones.

Este protocolo cumple con 3 funciones fundamentales: Direccionamiento, Fragmentación y Encaminamiento.

1. **Direccionamiento.-** En todo tipo de direccionamiento es necesario considerar 3 aspectos: nombre, dirección y ruta, en el caso específico de IP se centra en la dirección.

    - **Dirección IP.-** Es un número único e irrepetible asignado a cualquier dispositivo conectado a una red para permitir su identificación.

2. **Fragmentación.-** Se refiere a la acción de "dividir" la información de un paquete en distintas partes denominadas fragmentos para que puedan ser transmitidos por una red que está limitada transportar paquetes pequeños. Es necesario fragmentar cuando tamaño del datagrama es mayor a la unidad máxima de transmisión (MTU).

3. **Enrutamiento.-** Es el camino o ruta que utiliza un paquete para la llegar a su destino. El dispositivo que se encarga de este proceso es el Router.

2.1.3 Características

- **No Orientado a la conexión.-** Transmite datagramas sin necesidad de intercambiar información para establecer primero una conexión host-to-host.
- **Mejor Esfuerzo (Best effort)**.- Distribuye paquetes intentando hacer lo mejor posible pero sin garantizar su entrega.
- **No confiable (Unreliable).-** Los datagramas podrían llegar dañados, desordenados, duplicados o simplemente no llegar
- **Direccionamiento.-** mediante direcciones lógicas IP.
- Los datagramas no recibidos permanecerán en la red con un límite de tiempo.

2.1.4 Versiones

Se analizarán los 2 tipos de versiones de este protocolo: IPv4 e IPv6.

NOTA: Debido a la extensión de algunos temas tratados a continuación referidos a direccionamiento IP, formato de direcciones, transición de IPV4 e IPV6 hemos decidido no entrar en detalle minucioso, puesto que consideramos que nuestro objetivo es el de obtener un conocimiento general en algunos de estos puntos puesto que consideramos que el tema de estudio de esta tesis no se centra en esto.

2.1.4.1 Protocolo Internet versión 4 (IPv4)

Es la versión utilizada en la actualidad para identificar dispositivos conectados a la red.

Formato de Cabecera.- El tamaño de la cabecera IPv4 es de 32 bits (4 bytes), distribuidos en diferentes campos de longitud variable que cumplen una función determinada. A continuación en la figura 2.1 se presenta la distribución de este encabezado:

Figura 2.1 Formato de Cabecera IPV4

<table>
<tr><th>0-3</th><th>4-7</th><th>8-15</th><th>16-18</th><th>19-31</th></tr>
<tr><td>VERSIÓN</td><td>TAMAÑO CABECERA</td><td>TIPO DE SERVICIO</td><td colspan="2">LONGITUD TOTAL</td></tr>
<tr><td colspan="3">IDENTIFICADOR</td><td rowspan="2">INDICADORES</td><td rowspan="2">POSICIÓN DE FRAGMENTO</td></tr>
<tr><td colspan="3">CHECKSUM CABECERA</td></tr>
</table>

DIRECCIÓN IP DE ORIGEN	
DIRECCIÓN IP DE DESTINO	
OPCIONES	RELLENO

Fuente: http://f34k.files.wordpress.com/2008/01/microsoft-word-abecera-ip.pdf

Descripción de los campos de la cabecera IPv4:

Tabla 2.1 Descripción de los campos de encabezado de datagrama IPV4

VERSIÓN	
Tamaño	4 bits
Descripción	Versión sobre la cual se va a construir el datagrama en este caso 4
Valor	0100
TAMAÑO DE CABECERA (IHL)	
Tamaño	4 bits
Descripción	Cantidad de palabras de 32 bits que componen el encabezado.
Valor	Su valor mínimo es de 5 para una cabecera correcta, y el máximo de 15.
TIPO DE SERVICIO (TOS)	
Tamaño	8 bits

Descripción	Indica la importancia de los datos en la que se debe procesar el datagrama.

Valor

BIT 5, 6 ,7	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
PRIO **En casos de Congestión**	**Demora**	**Rendimiento**	**Fiabilidad**	**Costo**	**Sin Uso**
000 De Rutina **001** Prioritario **010** Inmediato **011** Relámpago (Urgente) **100** Muy Urgente **101** Procesando Llamada Critica y de emergencia **110** Control de Trabajo de Internet **111** Control de Red	0 Normal 1 Mínima	0 Normal 1 Máximo	0 Normal 1 Máxima	0 Normal 1 Mínimo	0

LONGITUD TOTAL

Tamaño	16 bits
Descripción	Tamaño total del datagrama en bytes, incluyendo el tamaño de la cabecera y los datos.
Valor	El tamaño del datagrama no puede exceder los 65536 bytes.

IDENTIFICADOR ,INDICADORES (FLAGS) y POSICION DE FRAGMENTO

Tamaño	16, 3 y 13 bits respectivamente.
Descripción	Utilizados para la fragmentación de los datagramas

TIEMPO DE VIDA (TTL)

Tamaño	8 bits
Descripción	Indica el máximo número saltos (pasos por un router), por los que un paquete puede atravesar, evitando que la red se sobrecargue con datagramas perdidos.

Valor	Para TCP/IP es de 255 En host XP 128 Valor normal recomendado es de 60 saltos Disminuye en 1 cada vez que pasa por un router y al llegar a 0 el router destruye el datagrama.
PROTOCOLO	
Tamaño	8 bits
Descripción	Permite saber el protocolo del siguiente nivel usado en la parte de datos del datagrama
Valor	TCP se representa con el número 6 y UDP con el 17
SUMA DE COMPROBACIÓN (CHECKSUM)	
Tamaño	16 bits
Descripción	Código de protección de errores, sirve para controlar si el encabezado se ha modificado durante la transmisión.
Valor	Se suman todos los bits de la cabecera, se complementa la suma a uno y se pone el resultado en el campo checksum. A la hora de calcular la suma de control, el valor inicial de este campo es cero. Esta suma se recalcula en cada lugar donde la cabecera es procesada.
DIRECCIÓN IP ORIGEN	
Tamaño	32 bits
Descripción	Este campo representa la dirección IP del equipo remitente y permite que el destinatario responda
DIRECCIÓN IP DESTINO	
Tamaño	32 bits

Descripción	Dirección IP del destinatario del mensaje.
OPCIONES IP	
Tamaño	32 bits
Descripción	De uso opcional, puede o no aparecer en los datagramas, proporcionan funciones de control para que los investigadores prueben nuevos conceptos con información de recursos para marcas de tiempo, seguridad y encaminamiento especial.
RELLENO	
Tamaño	32 bits
Descripción	Ajusta las opciones a 32 bits
Valor	El valor usado es 0.

Funciones.- El protocolo IP en su versión 4 realiza las funciones de Direccionamiento, Fragmentación y Encaminamiento de la siguiente manera:

- **Direccionamiento.-** IPv4 ofrece un direccionamiento jerárquico lo que permite encontrar un destino de manera más rápida. La institución a cargo del direccionamiento es la "Autoridad de Números asignados a Internet".

  La cantidad de direcciones dispuestas por este protocolo es algo más de 4.000.000.000, que no son suficientes en la actualidad para abastecer toda la demanda generada a nivel mundial.

Formato de Direcciones IPv4.

Son de longitud de 32 bits, segmentadas en 4 octetos (8 bits), representadas con números decimales de 0 a 255 separadas por puntos denominados punto decimal.

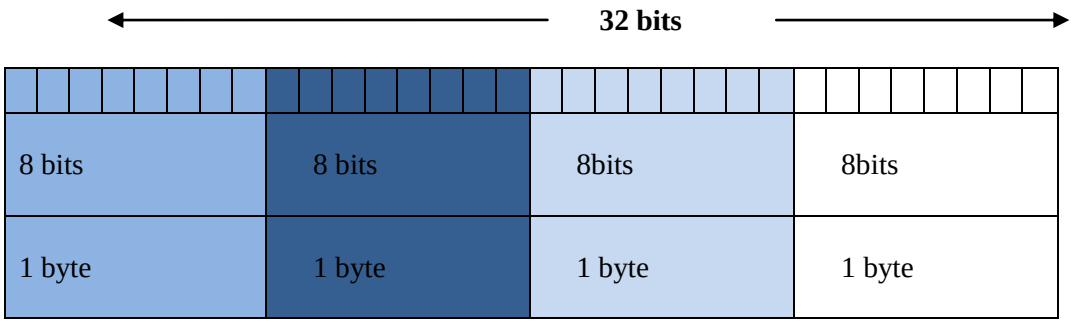


Figura 2.2 Formato de direcciones IPV4

Ejemplo: La dirección 11000000.10101000.01100100.00000001 en puntos decimales se representa como: 192.168.100.1

Esta dirección a su vez se conforma de 2 partes: los bits de orden superior que sirven como identificador de RED y el resto de bits para la identificación del HOST.

Tabla 2.2 Partes de una dirección IP

32 bits

IDENTIFICADOR DE RED	IDENTIFICADOR DE HOST
Información para ruteo.	Nodo especifico dentro de la red

- **Tipos de direcciones de una IPv4.-** Existen 3 tipos de direcciones: Dirección de Red, Broadcast y de Host.

- **Dirección de Red**: Se utiliza para referirse a la red en la que se ubica una dirección IP. Tiene un 0 por cada bit que conforma la parte de host de la dirección.
- **Dirección de Broadcast**: Ocupa la última dirección de la red en uso, es decir con todos los bits de la parte de host en 1, basta enviar datos a esta dirección para lleguen a todos los hosts de la red.
- **Direcciones Host**: Se asignan a los dispositivos finales de la red.

- **Tipos de Comunicación:** Unicast, Broadcast, Multicast

Tabla 2.3 Tipos de Comunicación

Tipo	Description
Unicast	Envía paquetes de host a host individual
Broadcast	Envía paquetes de un host a todos los hosts de la red. **Broadcast dirigido:** hacia una red específica (routers). **Broadcast limitado:** para la comunicación que está limitada a los hosts en la red local.
Multicast	Envía Paquetes de un host a un grupo seleccionado de hosts

- **Clases:** Los segmentos de una dirección IP ayudan a clasificar las direcciones en 5 clases: A, B, C, D y E.

  Para identificar el esquema utilizado, es necesario tomar en consideración los primeros bits: si el primero es **0** se trata de **clase A**, si los dos primeros son **10**, se trata de **clase B**, finalmente si el esquema inicial es **110**, se trata de la **clase C.** La clase D se reconoce si empieza con **1110**, y en la **Clase E** sus bits iniciales en **1111**.

A continuación se presenta una tabla con el rango de valores en decimal de las direcciones IP asignadas para cada clase.

Figura 2.3 Rangos de Direcciones para cada Clase

DIRECCIONES IPV4	RANGO	Bits Iniciales
Clase A /8	1.0.0.0 a 127.255.255.255	0
Clase B /16	128.0.0.0 a 191.255.255.255	10
Clase C /24	192.0.0.0 a 223.255.255.255	110
Clase D	224.0.0.0 a 239.255.255.255	1110
Clase E	240.0.0.0 a 247.255.255.255	1111

Fuente: http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP#Direcciones_IPv4

Los identificadores que contiene la IP se distribuyen de la siguiente manera:

CLASE A (/8).-Asigna el primer octeto para la identificar la RED y los 3 siguientes para los HOSTS.

CLASE B (/16).-Asigna los dos primeros octetos para identificar la red y los siguientes dos octetos finales para los hosts

CLASE C (**/24**).-Asigna los 3 primeros octetos para identificar la red y el último para hosts.

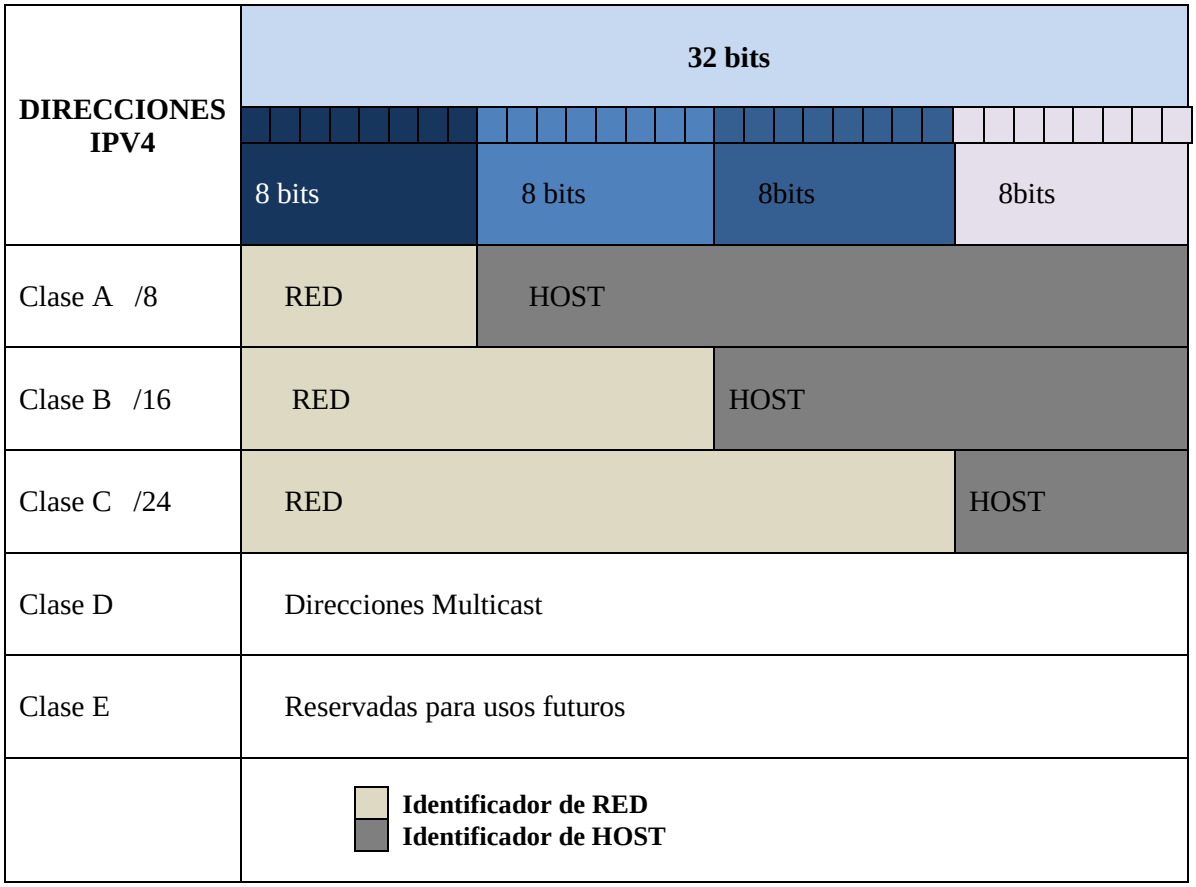
CLASE D, utilizada para **IP Multicast**.

De 224.0.0.0 a 224.0.0.255 se utilizan para Multicast en una red local.

De 224.0.1.0 a 238.255.255.255 para Multicast en Internet.

CLASE E, reservada para uso investigativo o experimental.

Figura 2.4 Identificadores de RED y HOST en Clases de Direcciones IPV4



Espacio de Direccionamiento.- Es la cantidad de redes y hosts disponibles según el tipo de direccionamiento (clase A, B, C).

Fórmulas:

$REDES\ disponibles\ = 2^n$, dónde "n" es el número de bits utilizados para identificar la red.

$HOSTS\ disponibles\ = 2^n - 2$, dónde "n" es el número de bits que identifican el HOST según el esquema utilizado

Se restan 2 host que se refieren a la primera y la última dirección, reservadas para dirección de red y de Broadcast respectivamente.

Figura 2.5 Espacio de Direccionamientos en direcciones IPV4

DIRECCIONES IPV4	**HOST**				
	Bits Iniciales	**Nº Bits RED**	**Espacio de Direccionamiento**	**Nº Bits**	**Espacio de Direccionamiento**
Clase A	0	7	2^7 -2= 126	24	2^{24}-2=16777214
Clase B	10	14	2^{14} = 16.384	16	2^{16} – 2=65534
Clase C	110	21	2^{24} -2= 16.777.214	8	(2^8)-2=254

En la parte que corresponde a las redes es necesario ignorar el bit que se utiliza como código para identificar el esquema puesto que nunca va a cambiar. En la clase A, se restaron 2 redes reservadas 0.0.0.0 (0/8) y 127.0.0.0 (127/8) consideradas direcciones especiales.

Direcciones IPV4 Especiales.- Además de las direcciones de red y broadcast tenemos:

¬ **Dirección de bucle local** o **Loopback.- 127.x.x.x** para pruebas de conectividad hacia sí mismo (retroalimentación).

¬ **Ruta predeterminada.- 0.0.0.0** utilizada por defecto cuando no se cuenta con una ruta más específica.

Direcciones Públicas y Privadas

Las direcciones públicas son aquellas que permiten la comunicación de los equipos en la Internet y son alquiladas o vendidas por los ISP (Proveedores de Servicios de Internet), en cambio las privadas son un bloque determinado de direcciones que se asignan a los equipos de una red local y no utilizan los servicios de la Internet.

El rango de direcciones privadas que pueden ser utilizadas en la administración de redes locales de cualquier empresa es:

Clase A: 10.0.0.0 a 10.255.255.255

Clase B: 172.16.0.0 a 172.31.255.255

Clase C: 192.168.0.0 a 192.168.255.255

Si se desea que los host de una dirección privada puedan acceder a internet, es necesario utilizar un servidor de traducción de direcciones de redes (NAT) o un Proxy.

Máscara de Subred.- Sirve para saber si la dirección IP pertenece o no a una red, identificando la porción de bits para red y host respectivamente. Para esto coloca 1 en todos los bits que corresponden a la parte de red y subred y 0 en los

del al host. Así en formato binario todas las máscaras de red tienen los "1" agrupados a la izquierda y los "0" a la derecha.

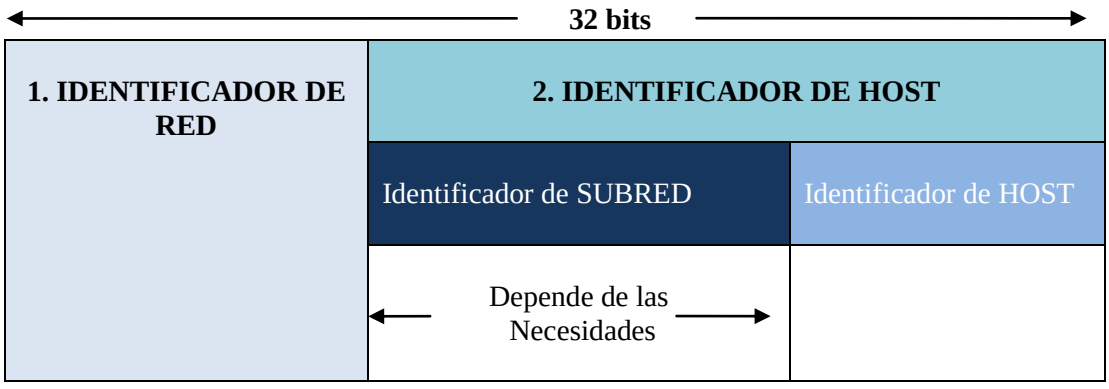
Por ejemplo para una dirección IP: **192.168.1.100** usaríamos la máscara: **11111111.11111111.11111111.00000000** que en formato decimal sería **255.255.255.0**

Ésta dirección IP también se puede escribir como 192.168.1.100/24 el símbolo "/"representa el prefijo de red para especificar la máscara.

Subredes (subneting).- Es el proceso de dividir un espacio de direcciones clase A, B o C en redes más pequeñas que permitan acrecentar el número de direcciones IP disponibles y facilitar su gestión.

Procedimiento.

- En la dirección IP la parte del Host original se divide en 2, así:



Lo que hacemos es considerar el número de subredes y host requeridos en nuestro plan de direccionamiento.

Así, en una dirección IP con una máscara de red /28

255.255.255.240 **11111111.11111111.11111111.11110000**

Para saber el número de subredes y de hosts válidos respectivamente aplicamos lo siguiente:

$\mathbf{2^n - 2}$, donde "n " es el numero de bits tomados para subred ó para host.

Es decir que la máscara anterior nos provee de $\mathbf{2^4 - 2 = 14}$ subredes válidas

(Las 2 subredes que se restaron corresponden a la dirección de red y de broadcast que dan un total de 16 subredes)

y $2^4 - 2 = 14$ hosts válidos por cada subred generada

(Las direcciones de RED y BROADCAST no se asignan a una dirección de HOST porque invalidan la red.)

Ejemplo:

En la dirección IP clase C: 192.10.20.18/28.

La dirección de Red es: 192.10.20.16/ 28

Direcciones válidas van desde: 192.10.20.17 hasta 192.10.20.30

Finalmente la dirección de Broadcast es: 192.10.20.31

- **Tipos de Subnetting**.- Existen 2 tipos de subneting estático y de longitud variable.
  - **Estático.-** Es sencillo, se utilizan las subredes generadas con una misma máscara de subred, por lo que no se aprovecha de manera óptima el espacio de direcciones.
  - **De longitud variable (variable length subnet mask - vlsm).-** se utilizan máscaras diferentes de las subredes generadas, optimizando el espacio de

direcciones aunque en relación al subneting estático su implementación y mantenimiento es más complejo. Este término se utiliza en redes privadas.

- **Encaminamiento inter-dominios sin clases** (**Classless Inter-Domain Routing - CIDR**).- Similar al VLSM, se utiliza al referirse a la red pública Internet.

Asignación Estática y Dinámica de Direcciones.

- **Estática.-** la información de red para cada host, es configurada manualmente por el administrador de red, es aconsejable en redes pequeñas
- **Dinámica.-** Facilita la asignación de direccionamiento IP en empresas con gran número de hosts ya que mediante el Protocolo de configuración dinámica de host (DHCP) se lo realiza automáticamente.

2.1.5 Fragmentación IPv4

La fragmentación en IPV4 se la realiza en los equipos Router, para ello utilizan los campos de la segunda fila de la cabecera ipv4 mencionados anteriormente:

Fig. 2.6 Campos utilizados para la fragmentación en la cabecera IPV4

0-3	4-7	8-15	16-18	19-31
Identificador			Indicadores	Posición de Fragmento

Cuando un paquete que necesita ser fragmentado esta marcado como "no fragmentar", será descartado.

Descripción de Campos destinados a la Fragmentación:

Tabla 2.4 Descripción de los Campos de Fragmentación IPV4

<table>
<tr><td colspan="2">IDENTIFICACIÓN</td></tr>
<tr><td>Tamaño</td><td>16 bits</td></tr>
<tr><td>Descripción</td><td>Identificador único del datagrama, utilizado en caso de que el datagrama deba ser fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro.</td></tr>
<tr><td>Valor</td><td>Valor único para la pareja origen-destino asignado por el remitente.</td></tr>
<tr><td colspan="2">INDICADORES (FLAGS)</td></tr>
<tr><td>Tamaño</td><td>3 bits</td></tr>
<tr><td>Descripción</td><td>Indica si el paquete está fragmentado o no</td></tr>
<tr><td>Valor</td><td>
<table>
<tr><td>BIT 2</td><td>BIT 1</td><td>BIT 0</td></tr>
<tr><td>Más Fragmento (MF)</td><td>No Fragmentar (DF)</td><td>Reservado</td></tr>
<tr><td>1 Mas Fragmentos
0 Ultimo Fragmento</td><td>0 Fragmentarse
1 No fragmentar</td><td>0</td></tr>
</table>
</td></tr>
<tr><td colspan="2">POSICIÓN DE FRAGMENTO</td></tr>
<tr><td>Tamaño</td><td>13 bits</td></tr>
<tr><td>Descripción</td><td>Indica la posición del paquete fragmentado dentro del datagrama original.</td></tr>
<tr><td>Valor</td><td>El primer fragmento tiene un valor de 0</td></tr>
</table>

- La Unidad Máxima de Trasmisión (MTU) del paquete es de 65635 bytes.
- Si los fragmentos no han sido re ensamblados en un determinado tiempo, es necesario el reenvío de datagrama completo.

Enrutamiento.- la entrega puede ser de 2 maneras directa e indirecta.

- **Entrega Directa.-** es la que se da dentro de la misma red física
- **Entrega Indirecta.-** es aquella en la que interviene un router intermedio en la comunicación ya que se disponen de múltiples redes.

Tabla de Enrutamiento IP,

Tanto los equipos host como los routers tienen una **Tabla de Enrutamiento IP**, que contiene información acerca de la dirección IP de los posibles destinos, indicando si la entrega es directa o indirecta.

Tipos de enrutamiento.- Se consideran 3 tipos: Estático, predeterminado y dinámico.

1. **Enrutamiento Estático.-** El administrador de red es el encargado de brindar información a la tabla de enrutamiento del router de manera manual por lo que en caso de que surjan cambios en la red no permite al equipo adaptarse por sí, no consumen gran cantidad de recursos del sistema y es recomendable en una red cuya topología incluya pocos enrutadores.

2. **Enrutamiento Predeterminado**.-Denomino como ruta por defecto, considera a la red destino como la ruta estática 0.0.0.0/0.0.0.0 se la usa como camino para los datagramas cuyos destinos no coincidan con los que

se incluyen en las tablas de enrutamiento, por lo general es configurada en el router del ISP.

3. **Enrutamiento Dinámico**.-La información de la tabla de enrutamiento es adquirida mediante protocolos de enrutamiento que son más rápidos en situaciones complejas, permiten ajustar las actualizaciones que sufre la red e inclusive son capaces de evaluar la mejor ruta para su destino, es ideal en topologías de red que incluyen un número considerable de enrutadores aunque claro, consumen mayor recursos del sistema y dinero.

Protocolos de Enrutamiento Dinámico.

Las técnicas de enrutamiento de los protocolos pueden ser **por vector distancia** en los que se comparte información entre enrutadores vecinos acerca de cómo llegar a los destinos y de **estado de enlaces** que obtiene información sobre los enlaces. La diferencia entre uno y otro es que en el primer caso se obtiene una convergencia lenta, mientras que en el otro es rápida.

- **Protocolos internos de pasarela (Interior Gateway o IGP).-** Se encarga de las rutas dentro de un sistema autónomo por ejemplo una universidad, compañía grande, etc.

Ejemplos:

Por Vector Distancia:

RIP v1 (Protocolo de Enrutamiento de Información Versión 1**).-** No soporta VLSM, recomendado en sistemas de redes pequeñas.

RIP v2 (Protocolo de Enrutamiento de Información Versión 2**).-** Soporta VLSM

EIGRP (Protocolo de enrutamiento de Gateway interior mejorado**).-** Es un protocolo desarrollado por Cisco que permite VLSM. Usado en sistemas de redes grandes.

Por Estado de Enlace:

OSPF (Primero la ruta libre más corta, Open Shortest Path First), soporta VLSM ampliamente implantado en redes públicas y privadas.

Protocolos externos de pasarela (EGP).- Administran rutas que conectan diferentes sistemas autónomos.

Ejemplo: BGP (Border Gateway Protocol)

Tabla2.5. Comparativa entre Protocolos.

CARACTERÍSTICAS	**RIP**	**OSPF**	**EIGRP**
Tiempo de Convergencia	Lento	Rápido	Rápido
Soporta VLSM	No	Si	Si
Consumo de Recursos	Bajo	Alto	Bajo
Mejor escalamiento	No	Si	Si
De libre uso o propietario	Libre Uso	Libre Uso	Propietario

Fuente: http://www.solticom.com/uts/protocolos.pdf

Protocolo Internet Versión 6 (Ipv6).

IPV6 es conocido también como IP de nueva generación (IPNG), nace a partir de la necesidad de direccionamiento en conexiones hacia la Internet puesto que hoy en día el acceso a este servicio cuenta con gran demanda no solo por parte de los PC's fijos o portátiles sino por gran variedad de dispositivos de alta tecnología, gracias a la experiencia que se obtuvo con la versión anterior IPV4 a integrado componentes muy útiles para suplir deficiencias en cuanto a velocidad y seguridad. Es el más exitoso hasta el momento.

Características:

- Gran cantidad de direccionamiento.
- Permite conexión host to host lo que significa mayor velocidad de transmisiones.
- Mejor aprovechamiento del ancho de banda.
- Implementa mayores seguridades IPsec.
- Mayor Flexibilidad
- Simplicidad

Formato de Datagrama IPv6.- En un datagrama IPV6 la cabecera cuenta con 2 partes: una fija conocida como Cabecera IPv6 y otra con opciones que puede o no estar presente dependiendo de las necesidades denominada Cabecera de Extensión.

40 octetos	**0 o mas**			
Cabecera Fija	Cabecera de extensión 1	…	Cabecera de extensión n	Datos
	Opcional			

Fuente: http://halley.ls.fi.upm.es/~jyaguez/pdfs/RESUMENGRAFICOTRANSCUARTOFRAGMENTAR2005.pdf

Formato de Cabecera IPv6.- Su tamaño es de 40 Bytes, siempre se sitúa al inicio del datagrama, existan o no cabeceras de extensión:

Figura 2.6 Formato de Cabecera IPV6

128 bits

<table>
<tr><td>Versión</td><td>Clase de Trafico (prioridad)</td><td colspan="2">Etiqueta de Flujo</td></tr>
<tr><td colspan="2">Longitud de la Carga Útil</td><td>Cabecera Siguiente</td><td>Límite de Saltos</td></tr>
<tr><td colspan="4">Dirección Origen</td></tr>
<tr><td colspan="4">Dirección Destino</td></tr>
</table>

Fuente: http://tecnoem.blogspot.com/2008_10_01_archive.html

Descripción de Campos de Cabecera Fija IPv6

Tabla 2.6 Descripción de los campos de la cabecera IPV6

VERSIÓN	
Tamaño	4 bits
Descripción	Versión sobre la cual se va a construir el datagrama en este caso 6
Valor	0110
CLASE DE TRAFICO	
Tamaño	8 bits
Descripción	Lleva un control del tráfico mediante la asignación de prioridades a cada paquete

	Similar al TOS en IPV4.
Valor	Tomando en cuenta el nivel de prioridad más bajo como los datagramas de menor importancia entonces tenemos que en caso de congestión: Las prioridades: De 0 a 7, pueden disminuir su velocidad de transmisión. De 8 a 15, debe mantenerse a una velocidad constante puesto que se trata de tráfico en tiempo real (datos de audio y video)
ETIQUETA DE FLUJO	
Tamaño	20 bits
Descripción	Valor único que identifica a los paquetes forman parte de una misma transmisión, facilitando la tarea de los routers y QoS.
Valor	Se elige aleatoriamente en el rango de 1 a 2^{24}-1 No se puede reutilizar un valor mientras no se termine su tiempo de vida.
LONGITUD DE LA CARGA UTIL	
Tamaño	16 bits
Descripción	Tamaño del paquete sin la cabecera.
Valor	Si el paquete es mayor a 65.536 bites, este campo vale 0 y se utiliza la opción de jumbograma de la extensión "salto a salto".
CABECERA SIGUIENTE	
Tamaño	8 bits
Descripción	Identifica la siguiente cabecera a procesarse en el desencapsulamiento.
Valor	Utiliza el valor similar al del campo de protocolos de IPV4 para representarlo. En caso de TCP=6, UDP=17, o una cabecera IPv6 opcional llamándola según su respectivo código de representación.

LÍMITE DE SALTOS	
Tamaño	8 bits
Descripción	Similar a la función del TTL en IPV4. Indica el máximo número saltos (pasos por un router), por los que un paquete puede atravesar antes de descartarse.
Valor	Este número entero disminuye su valor en 1 en cada paso por un router, si llega a cero el paquete será descartado.
DIRECCION ORIGEN	
Tamaño	128 bits
Descripción	Dirección ipv6 del equipo donde se origina el paquete
DIRECCION DESTINO	
Tamaño	128 bits
Descripción	Dirección ipv6 del equipo a donde se envía el paquete

Cabeceras de Extensión.-Pueden o no incluirse en el datagrama IPV6, son similares a las opciones que vienen en la cabecera ipv4 y dependiendo de su utilización deberían aparecer luego de la cabecera ipv6 en el siguiente orden:

Figura 2.7 Cabeceras de extensión ipv6

CABECERAS	CÓDIGO DE REPRESENTACION
CABECERA DE OPCIONES DE SALTO-A-SALTO.	0

CABECERA DE OPCIONES PARA EL DESTINO:OPCIONES QUE SE PROCESAN EN EL PRIMER DESTINO IPV6	
CABECERA DE ENCAMINAMIENTO	43
CABECERA DE FRAGMENTACIÓN	44
CABECERA DE AUTENTIFICACIÓN	51
CABECERA DE ENCAPSULAMIENTO DE LA CARGA DE SEGURIDAD	50
CABECERA DE LAS OPCIONES PARA EL DESTINO: SE PROCESAN SOLO POR EL DESTINO FINAL DEL PAQUETE	60
NO NEXT HEADER	59
CABECERA DE CAPA SUPERIOR.	Tcp, udp, icmp v6

Fuente: http://es.wikipedia.org/wiki/ipv6#cabeceras_de_extensi.c3.b3n

Secuencias de las Cabeceras en un Datagrama IPv6

El orden como se procesa un paquete ipv6 sin cabeceras de extensión:

Cabecera Fija IPV6 *Cabecera Siguiente= 6 (TCP)*	Segmento TCP

Con cabeceras de extensión:

Cabecera Fija IPV6 *Cabecera Siguiente= 0*	**Cabecera de Salto a salto** *Siguiente=43*	**Cabecera de encaminamiento** *Siguiente= 44*	**Cabecera de fragmentación** *Siguiente= 60*	**Cabecera de Opciones para destino** *Siguiente =6*	**Segmento TCP**

Fuente: http://halley.ls.fi.upm.es/~jyaguez/pdfs/RESUMENGRAFICOTRANSCUARTOFRAGMENTAR2005.pdf

Tamaño y descripción de cabeceras de extensión ipv6:

Tabla 2.7 Descripción de Cabeceras de Extensión.

CABECERAS	TAMAÑO
CABECERA DE OPCIONES DE SALTO-A-SALTO Datos necesarios a examinarse por cada nodo a través de la ruta de envío de un paquete	Variable
CABECERA DE ENCAMINAMIENTO Métodos para especificar la forma de rutear un datagrama.	Variable
CABECERA DE FRAGMENTACIÓN Parámetros para la fragmentación de los datagramas	Variable
CABECERA DE AUTENTIFICACIÓN Información para verificar la autenticación de la mayor parte de los datos del paquete (IPsec)	64 bits
CABECERA DE ENCAPSULAMIENTO DE LA CARGA DE SEGURIDAD Lleva la información cifrada para comunicación segura	Variable
CABECERA DE LAS OPCIONES PARA EL DESTINO: Información que necesita ser examinada solamente por los nodos destino del paquete.	Variable
NO NEXT HEADER Indica que no hay más cabeceras	Vacio

Fuente: http://es.wikipedia.org/wiki/IPv6#Cabeceras_de_extensi.C3.B3n

Funciones.- A continuación se describen las funciones de Direccionamiento, Fragmentación y Enrutamiento de IPV6.

1. Direccionamiento IPv6

Permiten un direccionamiento con más de 340.000.000.000.000.000.000.000.000.000.000.000.000 de direcciones disponibles.

Direcciones:

Se distinguen 3 tipos de direcciones en IPV6: UNICAST, ANYCAST Y MULTICAST.

- **Unicast**.- comunicación host a host, un origen un destino.
- **Anycast**.- Comunicación de un origen al más cercano del grupo de hosts destino.
- **Multicast.-** comunicación de un origen a todos los hosts destino que pertenecen al grupo.

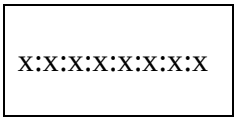
Formato de Direcciones IPv6.

Las direcciones tienen una longitud de 128 bits, segmentadas en 8 campos separados por 2 puntos de 16 bits cada uno. La dirección consta de 2 partes: un prefijo y un identificador de interfaz.

Tabla 2.8 Partes de una dirección ipv6

128 bits	
64 bits	**64 bits**
PREFIJO	**IDENTIFICADOR DE INTERFAZ**
¿Quién Eres? Depende de la topología de la red	¿Donde estas conectado? Identifica a un nodo

Cada campo debe tener al menos un número y no es necesario escribir ceros a la izquierda para completar los 16 bits.



Cada "x" es un valor hexadecimal de 16 bits.

Si se tienen muchas cadenas de bits con ceros se puede colocar :: para indicar uno o más grupos de 16 bits en cero, tomando en cuenta que este símbolo solo puede utilizarse una vez en cada dirección

Por ejemplo:

FF01:0:0:0:0:0:0:101 equivale a => FF01::101

En caso de contar con equipos con IPv4 e IPv6

Donde "x" son valores hexadecimales de 16 bits cada uno y "d", son valores decimales de 8 bits cada una, de la representación de direcciones en formato IPv4.

Ejemplos:

0:0:0:0:0:0:13.1.68.3 => ::13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38 =>::FFFF:129.144.52.38

Para indicar la máscara de red es similar que en ipv4, dirección /longitud del prefijo

- 12AB::CD30:0:0:0:0/60

  Es una dirección con una máscara de red de 60 bits.

Direcciones IPv6 Reservadas

Tabla 2.9 Direcciones IPV6 Reservadas

Dirección ipv6	**Longitud prefijo**	**Descripción**	**Notas**
::	128 bits	Sin especificar	Como 0.0.0.0 en ipv4
::1	128 bits	Dirección de bucle local (loopback)	Como las 127.0.0.1 en ipv4
::00::xx:xx:xx:xx	96 bits	Direcciones ipv6 compatibles con ipv4	Los 32 bits más bajos contienen una dirección ipv4 se usan para representar direcciones ipv4 se denominan direcciones "empotradas"
::ff:xx:xx:xx:xx	96 bits	Direcciones ipv6 mapeadas a ipv4	Los 32 bits más bajos contienen una dirección ipv4 se usan para representar direcciones ipv4 mediante direcciones ipv6
Fe80::-feb::	10 bits	Direcciones link-local	Equivalentes a la dirección de loopback de ipv4
Fec0::-fef::	10 bits	Direcciones site-local	Equivalentes al direccionamiento privado de ipv4

Ff::	8 bits	Multicast	
001(base 2)	3 bits	Direcciones unicast globales	Todas las direcciones ipv6 globales se asignan a partir de este espacio. Los primeros bits siempre son “001”

Fuente: http://www.freebsd.org/doc/es/books/handbook/network-ipv6.html

¬ **Direcciones Unicast**

Las Direcciones Unicast son de 2 tipos: Globales y de Enlace local (Link-Local)

Unicast Globales: Utilizadas para acceder al servicio de la Internet

Formato 2000::/3:

Figura 2.8 Formato Direcciones Unicast Globales IPv6

FP 001	45 bits	16 bits	64 bits
TOPOLOGÍA PÚBLICA		**TOPOLOGÍA DEL SITIO**	**IDENTIFICADOR DE LA INTERFAZ**

Fuente: http://fmc.axarnet.es/tcp_ip/tema-03/tema-03.htm

De manera general se observa que el direccionamiento consta de 3 niveles: topología pública que manejan las empresas encargadas de distribución de Servicio de Internet RIRs e ISPs, topología del sitio asignada en los enrutamientos dentro de la organización y finalmente interfaz que identifica de manera individual a cada equipo generalmente coincide con la dirección .

El Prefijo del formato (**FP**), sirve para identificar que se trata de una dirección ipv6 Unicast Global, es administrado por el IANA

Unicast Enlace Local.- Similares a las redes privadas en IPV4 son útiles para configuración de redes de área local en organizaciones que no incluyen routers en su topología.

Formato: FE80::<id interfaz>/10

10 bits	54 bits	64 bits
1111111010	0	IDENTIFICADOR DE INTERFAZ
		Generalmente coincide con la dirección de capa de enlace de interfaz (MAC)

Direcciones de IPv6 con direcciones de IPv4 integradas

Es una dirección IPV6 Unicast compatible con IPv4, facilita la transición de direccionamiento IPV4 a IPV6

Formato: Direcciones IPV6

80 bits	16 bits	32 bits
00000……000000	0000 ó FFFF	Dirección IPV4

Fuente: http://fmc.axarnet.es/tcp_ip/tema-03/tema-03.htm

Direcciones Anycast Ipv6

Una dirección Unicast se convierte en Anycast cuando es asignada más de una interface. Por el momento se han planteado ciertas restricciones en su uso, mientras se concluyen con los estudios necesarios:

- No puede ser utilizada como dirección origen de un paquete IPv6
- Puede ser asignada solamente a un Router IPV6 (no host).

Un tipo de dirección Anycast denominada "dirección Anycast del router de la subred" es utilizada para comunicar un nodo a alguno del conjunto de routers, su identificador de interfaz consta de ceros:

Figura 2.9 Formato Dirección Anycast del Router de la subred IPv6

PREFIJO DE SUBRED	**IDENTIFICADOR DE INTERFAZ**
	00000000000

Direcciones Multicast IPv6.

Formato: FF::/8

8 bits	**4bits**	**4bits**	**112 bits**
11111111	000T	Ámbito	Identificador de Grupo
Prefijo de Formato Multicast		Entorno en el que se desenvuelve la conexión	Grupo multicast al que nos referimos

Fuente: http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

Los 8 primeros bits indican que se trata de una dirección multicast.

"T=0" indica: dirección permanente, asignada por la autoridad de numeración global en internet

"T=1" indica una dirección temporal

IPv6 sobre Ethernet

El formato de la dirección IPV6 utiliza las direcciones MAC origen y destino junto con el código de valor hexadecimal 86DD.

Tabla 2.10 Formato de una dirección IPv6 sobre Ethernet

48 bits	48 bits	16 bits
Dirección Ethernet Destino	**Dirección Ethernet Fuente**	1000011011011101 (86DD)

El tamaño máximo de la unidad de transmisión (MTU), para IPv6 sobre Ethernet, es de 1.500 bytes.

2. Fragmentación IPv6

A diferencia de IPV4 en IPV6 la fragmentación ya no es realizada en el router sino directamente en el equipo origen y el reensamblado se lo realiza en el destino, para ello cuenta con la cabecera de extensión de fragmentación, al no existir fragmentación en los routers agiliza el proceso de transmisión presentando mayor rapidez y menor probabilidad de perder un datagrama.

3. Enrutamiento (Routing) Ipv6

Similar a IPV4 es decir enrutamiento estático y los mismos protocolos de enrutamiento dinámico con pequeñas mejoras con soporte para IPV6 entre los que tenemos RIPv6 o RIPng, OSPF, EIGRP, etc.

Además en esta versión de IP se ha implementado una manera de realizar encaminamiento fijado en origen que consiste en el uso de la cabecera de extensión determinada para el encaminamiento que contiene el siguiente formato:

Fig. 2.16 Formato cabecera de extensión de Encaminamiento

Cabecera siguiente 8bits	**Tipo de encaminamiento 8 bits**	**16 bits**
Datos específicos del tipo		

Cuando el campo de tipo de encaminamiento es cero, la función de esta cabecera es la de implementar una lista de direcciones de los nodos que son "visitados" hasta llegar al destino del datagrama para permitir mayor agilidad sobre todo cuando se cuenta con varios proveedores mediante rutas conocidas, en caso de que el tipo de encaminamiento no sea cero se procederá a ignorar la cabecera o a su vez descartar el paquete.

Métodos de Transición de IPv4 a IPv6

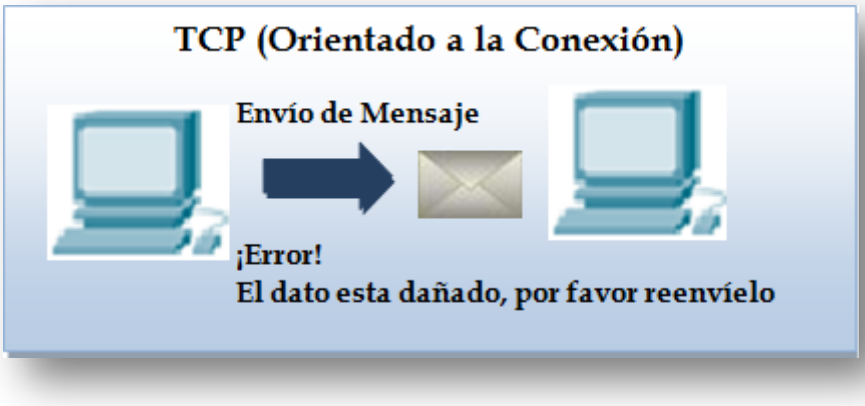
- Doble pila (IPv4 a IPv6)
- Túneles IPv6 sobre IPv4
- Transmisión de IPv6 sobre dominios IPv4
- Conexión de dominios IPv6 sobre redes IPv4
- "Tunnel Server" y "Tunnel Broker"

Se prevé que la migración a ipv6 en el Ecuador podría darse en su totalidad hacia finales del año 2011 aunque algunas instituciones y empresas ya lo han hecho. Además ya se trabaja en la creación de aplicaciones con soporte ipv6.

2.2 Protocolos de Transporte

Dentro de la Capa de Transporte del modelo TCP/IP encontramos los protocolos TCP y UDP, ambos cumplen la función de transportar los datos pero con claras diferencias en cuanto a la manera de como lo realizan. Nos daremos cuenta que ambos son muy útiles y dependiendo del tipo de información que se maneja nos resultará ventajoso el uso del uno u otro respectivamente. Una de las principales características de estos protocolos es el uso de puertos y sockets por lo que a continuación de los protocolos TCP y UDP hemos considerado realizar un análisis acerca de los mismos. En estos protocolos la unidad de datos del protocolo (PDU) es el segmento**.**

2.2.1 Protocolo de Control de Transmisión (TCP).



Fuente: http://www.learn-networking.com/wp-content/oldimages/tcp-versus-udp.jpg

2.2.1.1 Definición

TCP trabaja a nivel de la capa de transporte permitiendo que la transmisión de los datos de un paquete se realice en forma confiable a través de la red.

2.2.1.2 Características

- **Orientado a la Conexión.-** Primero crea una conexión mediante un modelo cliente-servidor para comenzar a transmitir información.

- **Fiable.-** Como veremos más adelante en la descripción de los campos del segmento TCP, cuenta con un campo que contiene un número de secuencia colocado al inicio de cada transmisión del segmento que permiten controlar la transmisión mediante bits de confirmación ACK, lo que permite la recuperación de datos en caso de corrupción, perdida duplicación o desorden que se puedan generar en el proceso de comunicación.[5]

- **Multiplexación.-** Permite que el envío de múltiples aplicaciones en la Internet desde una conexión se maneje en paralelo (multiplexación/demultiplexación), es decir brinda la posibilidad de que uno o más usuarios ejecuten en su equipo una o más aplicaciones de Internet al mismo tiempo, esto lo logra a través del manejo de PUERTOS, además ayuda a identificar de manera específica el equipo y aplicación ejecutada a través de SOCKETS.

- **Control de Flujo.-** Ayuda a aprovechar mejor el ancho de banda utilizando el mecanismo de Ventana Deslizante que se detallara en lo posterior.

- Es representado con el protocolo número 6 en el campo de datos del datagrama IP

[5] Fuente: El Protocolo TCP, " Transmisión Fiable", Calvaras Augé, Anna, http://www.tdr.cesca.es/TDX/TDX_UPC/TESIS/AVAILABLE/TDX-1222106-164746//04AMCA04de15.pdf

Figura 2.10 Formato de Segmento TCP

32 bits

<table>
<tr><td colspan="3">Puerto Origen</td><td>Puerto Destino</td></tr>
<tr><td colspan="4">Número de Secuencia</td></tr>
<tr><td colspan="4">Confirmación Piggy back (Ack)Acknowledgment</td></tr>
<tr><td>Long cabecera</td><td>Reservado</td><td>Bits de Código Flags</td><td>Tamaño de la Ventana</td></tr>
<tr><td colspan="3">Checksum</td><td>Puntero datos Urgente</td></tr>
<tr><td colspan="4">Opciones (0 o más palabras de 32 bits)</td></tr>
<tr><td colspan="4">Datos</td></tr>
</table>

Fuente: http://www.tdr.cesca.es/TDX/TDX_UPC/TESIS/AVAILABLE/TDX-1222106-64746//04AMCA04de15.pdf

2.2.1.3 Descripción de Campos del Segmento

PUERTO ORIGEN	
Tamaño	16 bits
Descripción	Identifica el puerto origen.
PUERTO DESTINO	
Tamaño	16 bits
Descripción	Identifica el puerto destino
NÚMERO DE SECUENCIA	
Tamaño	32 bits
Descripción	Indica el número de secuencia del primer byte de datos.
Valor	Su valor es igual al número de secuencia del último octeto recibido más uno. Es necesario que la bandera ACK del campo de bits de código, esté activado.
NÚMERO DE ACUSE DE RECIBO	
Tamaño	32 bits
Descripción	Valor del siguiente numero de secuencia que recibe el emisor del segmento, para ello el campo ACK debe estar activo en 1
Valor	Su valor es igual al número de secuencia del último octeto recibido más uno

<table>
<tr><th colspan="2">LONGITUD DE CABECERA</th></tr>
<tr><td>Tamaño</td><td>4 bits</td></tr>
<tr><td>Descripción</td><td>Indica la longitud de la cabecera TCP</td></tr>
<tr><td>Valor</td><td>Máximo 15, es decir, 60 octetos.</td></tr>
<tr><th colspan="2">RESERVADO</th></tr>
<tr><td>Tamaño</td><td>6 bits</td></tr>
<tr><td>Descripción</td><td>Uso reservado</td></tr>
<tr><td>Valor</td><td>0</td></tr>
<tr><th colspan="2">BITS DE CÓDIGO</th></tr>
<tr><td>Tamaño</td><td>6 bits</td></tr>
<tr><td>Descripción</td><td>Está formado por 6 opciones de 1 bit cada una. Para activar cada una es necesario ponerla en 1</td></tr>
<tr><td>Valor</td><td>
<table>
<tr><td>URG: Activa el campo Puntero Urgente</td></tr>
<tr><td>ACK: Acuse de Recibo, activa el número de reconocimiento, es utilizado como bit de confirmación.</td></tr>
<tr><td>PSH: Función Entregar datos inmediatamente</td></tr>
<tr><td>RST: Reinicializa la conexión</td></tr>
<tr><td>SYN: sincroniza los números de secuencia al inicio o al reiniciar la conexión</td></tr>
<tr><td>FIN: indica la finalización de datos por parte del emisor</td></tr>
</table>
<table>
<tr><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td></tr>
</table>
</td></tr>
<tr><th colspan="2">VENTANA</th></tr>
<tr><td>Tamaño</td><td>16 bits</td></tr>
<tr><td>Descripción</td><td>Tamaño máximo de octetos que el emisor se está dispuesto a aceptar</td></tr>
<tr><th colspan="2">SUMA DE CONTROL (CHECKSUM)</th></tr>
<tr><td>Tamaño</td><td>16 bits</td></tr>
<tr><td>Descripción</td><td>Realiza el respectivo control acerca de la integridad de los datos y la cabecera.</td></tr>
<tr><th colspan="2">PUNTERO URGENTE</th></tr>
<tr><td>Tamaño</td><td>16 bits</td></tr>
<tr><td>Descripción</td><td>Indica el desplazamiento que es necesario añadir al número de secuencia del segmento para determinar al último octeto de datos como urgentes
Funciona siempre que el bit de control URG esté activo.</td></tr>
<tr><th colspan="2">OPCIONES</th></tr>
</table>

Tamaño	Variable
Descripción	Son campos opcionales que permiten la administración de ciertas características del protocolo.

Tabla 2.11 Descripción de los campos del Segmento TCP

2.2.1.4 Funcionamiento

- **Establece Conexión.-** Lo realiza en 3 pasos (SYN, SYN/ACK y ACK), que son los bits de código descritos anteriormente dentro de los campos del Segmento TCP.

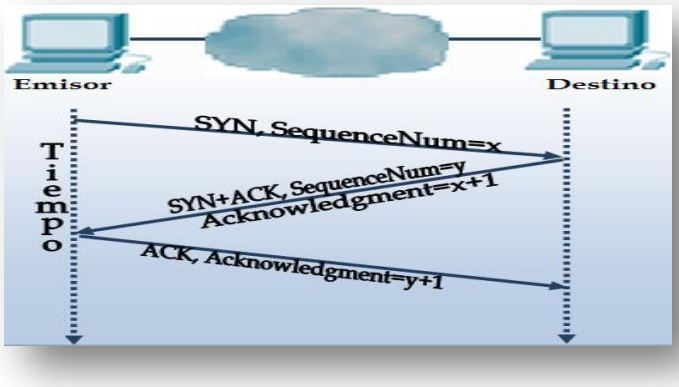
  El proceso se presenta de la siguiente manera:

  1. El Emisor envía el segmento con el bit SYN activo, junto con el valor del campo Número de Secuencia para iniciar al servidor.

  2. Una vez que llega al destino, aquí interviene el bit RST de comprobación para saber si el puerto está disponible y devuelve un SYN válido con un segmento SYN/ACK.

  3. Finalmente el cliente con un Acuse de Recibo (ACK), da a conocer que la respuesta respectiva por parte del destino ha sido debidamente procesada.

Figura 2.11 Inicio Conexión del Protocolo TCP



Fuente: http://bibing.us.es/proyectos/abreproy/11306/fichero/TEORIA%252F09+-+Capitulo+4.pdf

- **Transferencia de datos.-** Ordena los segmentos TCP recibidos y detecta errores.

  La manera en que TCP realiza el control de flujo de los paquetes en una transferencia de datos es mediante el uso del algoritmo ventana deslizante que permite la transmisión de varios paquetes mientras se recibe el ACK correspondiente lo que significa un mejor aprovechamiento del ancho de banda, el número de paquetes que pueden ser transmitido viene especificado en el campo ventana del segmento [6]

- **Fin de la conexión.-**Termina la conexión, puede producirse desde cualquiera de los 2 lados, es decir, por parte del Emisor o de parte del destinario.

2.2.1.5 Versiones

Durante la existencia de este protocolo se elaboraron múltiples versiones, entre las más destacables tenemos:

TCP de Berkeley (1983), TCP TAHOE (1988)

TCP RENO (1990), TCP Net/3: (1993)

TCP New Reno:

TCP Sack: (1996-98)

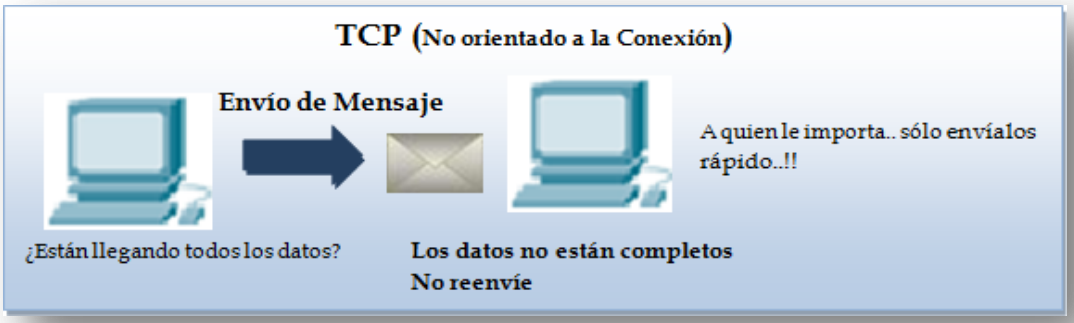
TCP VEGAS:

El más utilizado es el TCP reno por prestar mejoras de rendimiento en banda ancha.[7]

[6] El Protocolo TCP, " Control de Flujo", Calveras Augé, Anna, http://www.tdr.cesca.es/TDX/TDX_UPC/TESIS/AVAILABLE/TDX-1222106-164746//04AMCA04de15.pdf

[7] Wikipedia.org, Reno TCP: http://es.wikipedia.org/wiki/Reno_TCP

2.2.2 Protocolo de Datagrama de Usuario (UDP)



Fuente: http://www.learn-networking.com/wp-content/oldimages/tcp-versus-udp.jpg

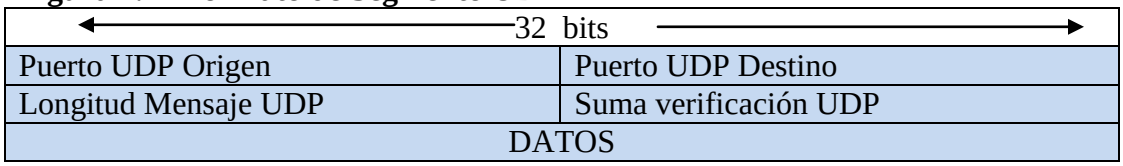
2.2.2.1 Definición.- Es el protocolo de entrega de datagramas más sencillo, ofrece un servicio de entrega de datagramas no fiable y no ordenado, idéntico al protocolo IP, lo único que integra son los puertos origen y destino. Generalmente utilizado para transmisión de videos.

2.2.2.2 Características

- **No orientado a la Conexión.-** Transmite datos sin asegurarse de que exista una conexión previa.
- **Máximo esfuerzo. (Best-Effort).-** Hace lo mejor posible para que los datos se transmitan eficientemente pero no garantiza nada
- **No Fiable.-** puede presentarse perdida duplicación o desorden de los datos durante el proceso de transmisión.
- **Multiplexación**.-Al igual que en TCP, permite que el envió de múltiples aplicaciones en internet
- Es representado con el protocolo número 17 en el campo de datos del datagrama IP

2.2.2.4 Formato de Segmento

Figura 2.11 Formato de Segmento UDP



2.2.2.5 Descripción de Campos del Segmento UDP

PUERTO UDP ORIGEN	
Tamaño	16 bits
Descripción	Es opcional, identifica el puerto emisor.
Valor	En caso de que no se use utiliza el 0 por omisión
PUERTO UDP DESTINO	
Tamaño	16 bits
Descripción	Identifica el puerto destino
LONGITUD MENSAJE UDP	
Tamaño	16 bits
Descripción	Tamaño del datagrama(datos y cabecera), 8 bits como mínimo
SUMA DE VERIFICACIÓN UDP	
Tamaño	16 bits
Descripción	Similar al de TCP, brinda protección de datagramas mal encaminados.

Figura 2.12 Descripción del Segmento UDP

2.2.2.6 Funcionamiento:

Los datos se empiezan a transmitir sin asegurarse de que exista conexión, el origen y destino son identificados por puertos, al no incluir métodos de detección de errores permite una rápida transmisión de datos.

2.2.3 Puertos y Sockets

Tanto en TCP y UDP hablamos acerca de PUERTOS y SOCKETS por lo que es necesario conocer más acerca de las funciones que éstos cumplen, a continuación presentamos un breve análisis:

2.2.3.1 Puertos

2.2.3.1.1 Definición

Utilizado tanto en TCP como UDP. Es un número de 16 bits que representa un mecanismo para acceder a las diferentes aplicaciones que se ofrecen desde Internet en la capa superior del modelo TCP/IP, asocia el número de puerto asignado con la aplicación solicitada.

2.2.3.1.2 Estados de un Puerto: Un puerto puede estar en cualquiera de los siguientes 3 estados:

- **Abierto:** Escuchando, existe la posibilidad de conectarse
- **Cerrado:** No se tiene acceso al puerto por lo que rechaza la conexión.
- **Bloqueado o sigiloso:** No permite obtener respuesta

NetStat.- En caso de que los puertos estén abiertos existen un gran número de herramientas que permiten su escaneo, entre las cuales esta **Netstat** que mediante línea de comandos presenta un listado de estos puertos, esto puede resultar sumamente peligroso en caso de que la persona que lo utilice lo haga con intenciones de atacar las seguridades de la red.

2.2.3.1.3 Clasificación:

Al ser un número de 16 bits permite contar con 65536 combinaciones de los que la IANNA (Internet Assigned Numbers Authority [Agencia de Asignación de Números de Internet]) dispone:

Figura 2.13 Clasificación de los Puertos

Puertos bien conocidos	0 al 1023
Puertos Registrados	del 1024 al 49151
Puertos Dinámicos y/o Privados	del 49152 al 65535

El número de un puerto utilizado por un cliente para solicitar aplicaciones desde internet a un servidor es asignado de manera aleatoria entre los puertos denominados "registrados" y, el servidor a su vez utiliza puertos "bien conocidos" en sus aplicaciones.

2.2.3.1.4 Puertos TCP Y UDP

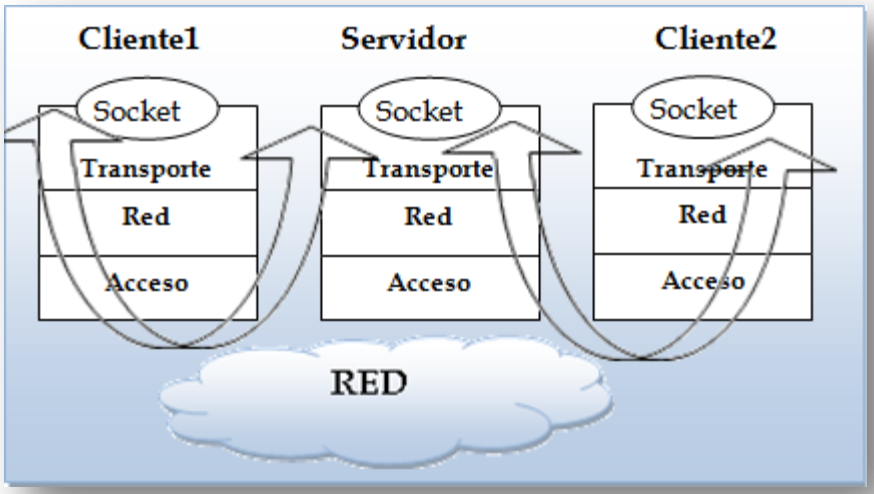
Algunos de los puertos utilizados por el protocolo TCP y UDP para acceder a las aplicaciones de internet se detallan en la tabla 2.12 a continuación:

Tabla 2.12 Puertos TCP/UDP

Número de Puerto	Tipo Puerto TCP/UDP	Protocolo de Aplicación
21	TCP/UDP	FTP
22	TCP/UDP	SSH
23	TCP/UDP	Telnet
25	TCP/UDP	SMTP
66	TCP/UDP	Oracle SQLNet
79	TCP/UDP	Finger
80	TCP/UDP	HTTP-Web
107	TCP/UDP	Remote Telnet Service
110	TCP/UDP	POP3
118	TCP/UDP	SQL Services

119	TCP/UDP	NNTP-News
150	TCP/UDP	SQL-Net
161	TCP	SNMP
194	TCP/UDP	IRC- Internet Relay Chat
443	TCP	HttpS
3128 (TCP)	TCP	Squid Proxy
6891-6900 (TCP) MSN	TCP	MSN menssenger (archivos)

2.2.3.2 Sockets



Fuente: http://www.scribd.com/doc/12363294/Modelo-de-Procesos

2.2.3.2.1 Definición:

La combinación de la dirección IP + el número de un puerto se le denomina SOCKET, es un punto de conexión que se utiliza para la comunicación entre procesos de diferentes maquinas a través de la red[8], permite la identificación de la maquina y la aplicación especifica que está ejecutando dicho proceso.

[8] DOCTORADO EN INFORMÁTICA, "Sockets: Comunicación entre procesos distribuidos", Miguel Rueda Barranco
http://es.tldp.org/Universitarios/seminario-2-sockets.html

2.2.3.2.2 Tipos:

Stream sockets (sock_stream).- sockets de flujos de datos en bytes, orientados a la conexión, son fiables y ordenados conocidos como sockets tcp

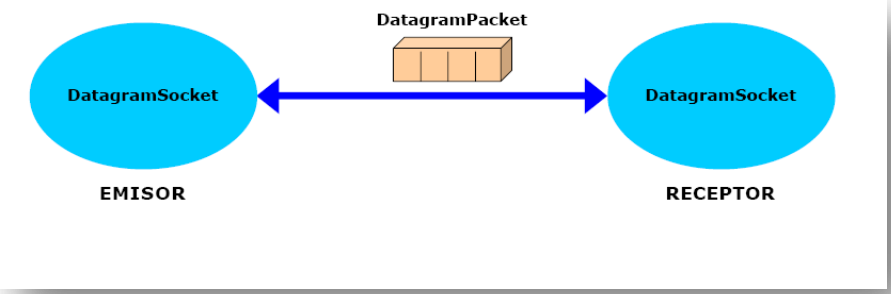
Datagram sockets.- sockets de datagramas**,** no orientados a la conexión, no asegura el orden de transmisión de los datagramas, son los sockets udp.

Socket raw (sock_raw): implementados para trabajar en niveles más bajos como con el protocolo IP.

2.2.3.2.3 Sockets TCP y UDP

Los TCP establecen una conexión previa a la transmisión de flujos de información entre 2 procesos (Cliente-Servidor). La comunicación se da punto a punto

Figura 2.14 Sockets TCP, Inicio de Conexión



Fuente: http://www.it.uniovi.es/docencia/GestionGijon/redes/Redes-Practica1-4.pdf

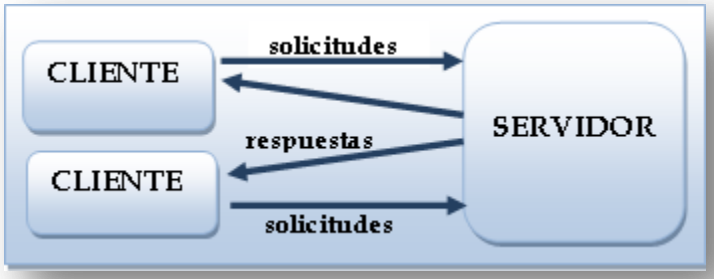
Los Sockets UDP pueden brindar una comunicación punto a punto (Datagram Socket) o multipunto uno a muchos (Multicast Socket)

2.3 Protocolos de Capa de Aplicación

Cada aplicación en la Internet está representada por un protocolo encargado de definir los estándares de comunicación entre el cliente y servidor, es por ello que antes de comenzar

con los protocolos primero explicaremos el término Cliente- Servidor que se maneja en todas las aplicaciones en este nivel del modelo TCP/IP y que fue considerado levemente en el Capítulo 1

Entorno Cliente/Servidor



Fuente: http://es.kioskea.net/contents/cs/csintro.php3

Es un modelo en el que intervienen un equipo denominado Cliente y otro denominado Servidor dentro de la comunicación en una red.

- **Equipo Cliente.-** Es el que inicia las peticiones hacia servicios almacenados en el equipo Servidor, estas peticiones se realizan generalmente mediante aplicaciones denominadas Cliente que interactúan directamente con los usuarios.

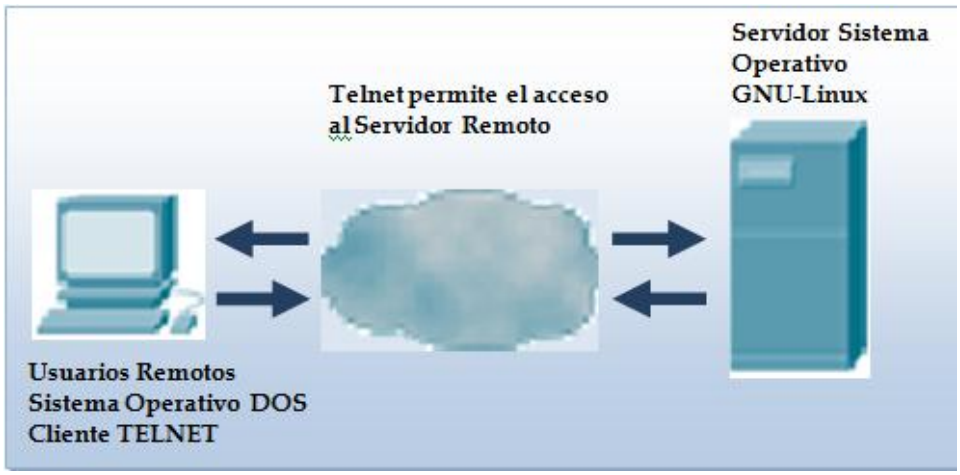
- **Equipo Servidor.-** Responde las peticiones, brindando los servicios solicitados, generalmente cuenta con mejores características físicas y de procesamiento para ejecutar las solicitudes que llegan de múltiples clientes aquí se denominan aplicaciones Servidor, casi no interactúan con los usuarios finales.

Para facilitar el proceso de enrutamiento en ésta capa se utiliza el protocolo de sistemas de nombre de dominio DNS (Domain Name System). Entre los protocolos de aplicación que podemos citar están: TELNET, FTP, HTTP, POP3, SMTP e IRC.

2.3.1 Protocolo de Red de Telecomunicaciones (Telnet)

2.3.1.1 Descripción

Es un protocolo de la capa de aplicación que permite operar remotamente los recursos de una computadora a la que se tuvo acceso a través una conexión de red, de la misma manera como si se realizara físicamente.



2.3.1.2 Uso

Aunque su uso no es muy común hoy en día debido a la poca seguridad que brinda, ya que carece de encriptación y autentificación, el manejo se lo realiza mediante una aplicación Telnet basada en el protocolo TCP que utiliza generalmente el puerto 23 y trabaja en un entorno Cliente/Servidor.

El manejo de la aplicación se lo realiza mediante la introducción de comandos a través del teclado, es decir, en modo terminal.

Los comandos para iniciar sesión en telnet son:

telnet nombre_del_servidor número_puerto donde: "***nombre_del_servidor"*** es el nombre o dirección IP del equipo remoto al que se quiere conectar el usuario y el numero: puerto el puerto que se desea utilizar así: telnet 132.64.12.77 80

2.3.1.3 Funcionamiento

El protocolo se basa en 3 puntos claves:

1. **Un terminal Virtual de Red (NVT).-** Se trata de la representación imaginaria de un terminal que permita a cualquier host acceder a otro sin necesidad de conocer sus características

2. **Principio de opciones negociadas**.- Permite la configuración de opciones de comunicación en cada parte (Cliente / Servidor), mediante la respectiva autorización.

   Estas pueden ser:
   DO => Desea usar;
   DON'T=> Se niega a usar;
   WILL=> Desea que la otra parte utilice;
   WON'T=> Se niega a que la otra parte utilice.[9]

3. **Reglas de negociación.-**Asegura que las opciones se generen de manera ordenada. Mantiene una comunicación half-duplex, es decir en los 2 sentidos pero no al mismo tiempo.

2.3.2 Protocolo de Transferencia de Archivos (FTP)

2.3.2.1 Descripción.

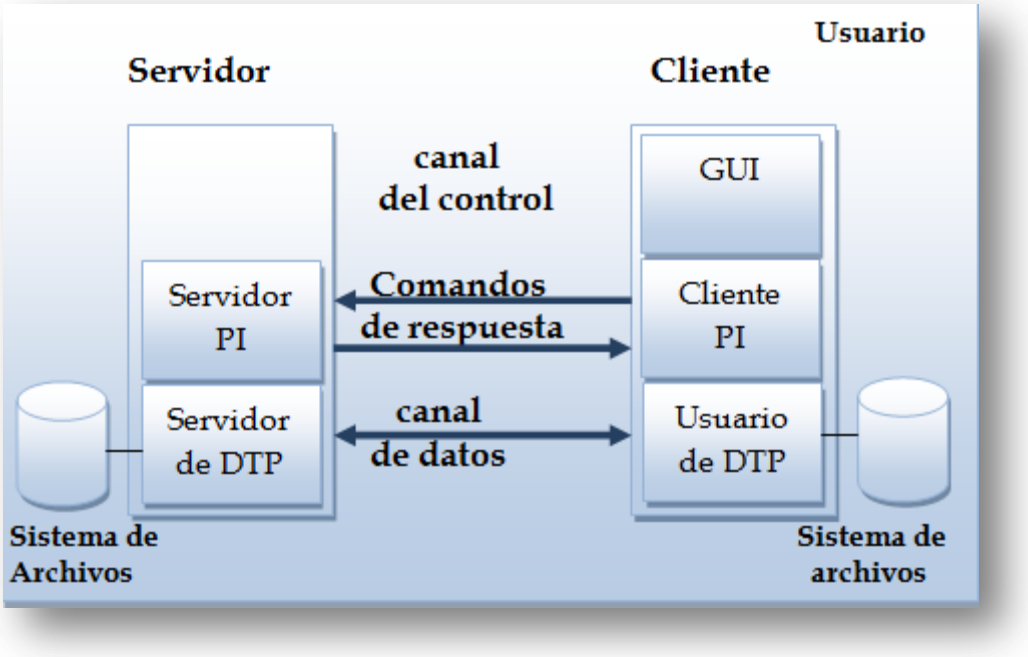
Es un protocolo de la capa de aplicación utilizado para compartir archivos de manera eficaz a través de la red TCP/IP además de que permite gestionar la manera en que se transfieren independientemente del Sistema Operativo.

[9] http://es.kioskea.net/contents/internet/telnet.php3?part=2
http://www.scribd.com/doc/20289794/Telnet
http://www.rfc-es.org/rfc/rfc0854-es.txt

2.3.2.2 Uso y Funcionamiento.

Es muy utilizado, trabaja en un entorno Cliente/Servidor, presenta mecanismos de autentificación por parte del cliente puesto que utiliza TCP, aunque no maneja ningún tipo de encriptación. Manipula generalmente los puertos 20 o 21 dependiendo de las necesidades. Según la aplicación cliente utilizada puede ser de modo gráfico y modo consola. Para ello es necesario un equipo con la aplicación FTP Server que contenga las debidas configuraciones acerca de los permisos y el FTP cliente instalado en el equipo que queremos que acceda de manera remota a ese servidor para subir o descargar los archivos.

Figura 2.14Modelo de Transmisión FTP



* DTP (Proceso de transferencia de datos)
* PI (Intérprete de protocolo) diferente en el cliente y el servidor:

Fuente: http://rockybal.iespana.es/ftp.html

Tipos de Acceso por parte del Cliente

- **Acceso autorizado** Brinda privilegios de acceso al usuario hacia los archivos del servidor previa la autentificación del mismo mediante un login y contraseña que permita identificarlo.

- **Acceso Anónimo.-** Permite el acceso a los usuarios sin ningún tipo de autentificación pero de igual manera sin privilegios hacia los archivos del servidor, solamente el permiso de descarga.

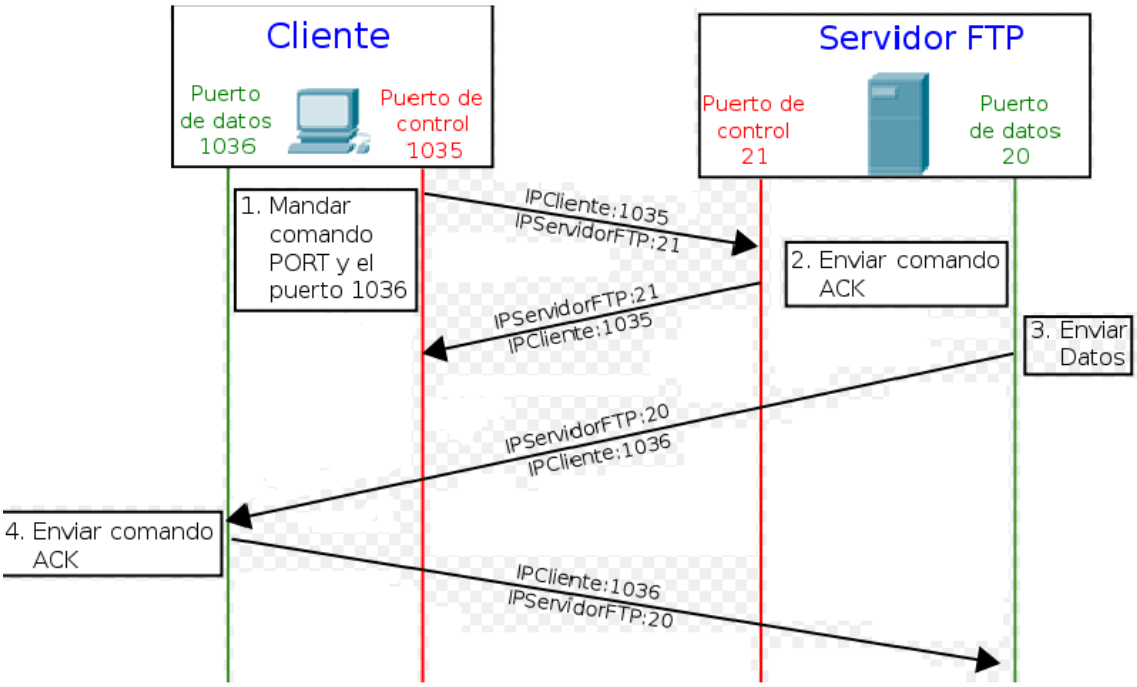
- **Acceso de Invitado.-** Una combinación de las anteriores, se realiza la autentificación del usuario pero con ciertas restricciones al momento de acceder a archivos.

Por del puerto número 20 se trasmiten los datos y por el 21 las órdenes de control entre el cliente y servidor.

Modos de acceso: pueden ser activo o pasivo:

- **Modo Activo.-** Utiliza el comando PORT. El cliente inicia la conexión hacia el servidor utilizando un número de puerto registrado aleatorio y habilita el siguiente puerto para escuchar al servidor que se comunica a través del puerto 20. Facilita la administración del firewall del servidor.

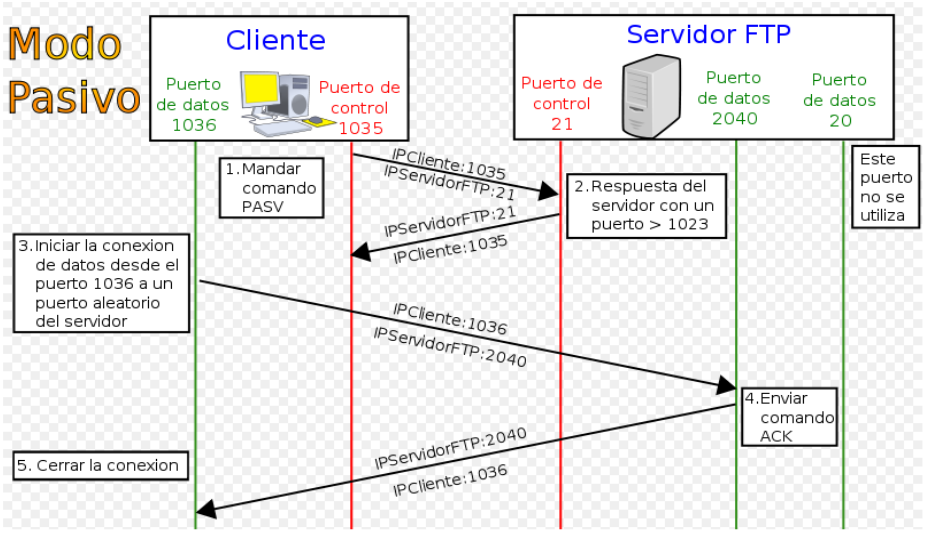
Figura 2.14 Modo de Acceso Activo del protocolo FTP.



Fuente: http://es.wikipedia.org/wiki/Archivo:Activo.svg

Modo Pasivo.- Utiliza el comando PASV. El cliente inicia la conexión y el servidor proporciona un nuevo puerto registrado aleatorio, el cliente se conecta a ese puerto y descarga la información requerida.

Figura 2.15 Modo de Acceso Pasivo del protocolo FTP.



Fuente: http://es.wikipedia.org/wiki/Archivo:Pasivo.svg

Permite una conexión bidireccional, subir y bajar archivos de gran tamaño simultáneamente y brinda mayor seguridad por parte del cliente al no dejar puertos en estado de escuchar

2.3.3 Protocolo De Transferencia De Hipertexto (Http)

2.3.3.1 Descripción

Es el protocolo de Capa de Aplicación que permite la transmisión de cualquier documento en hipertexto de manera sencilla dentro de la Internet, es así como se pueden visualizar las páginas web por lo que es el más utilizado por la World Wide Web.

Utiliza el protocolo TCP y el puerto por defecto es el 80, una variación de éste es el HTTPS que permite mayor seguridad mediante la encriptación de datos y autentificación de usuarios.

2.3.3.2 Uso y Funcionamiento

En una conexión a internet, ingresamos en un browser la dirección web que permite acceder al documento con el que se desea trabajar de la siguiente manera:

http://direccionIP:numero de puerto/path

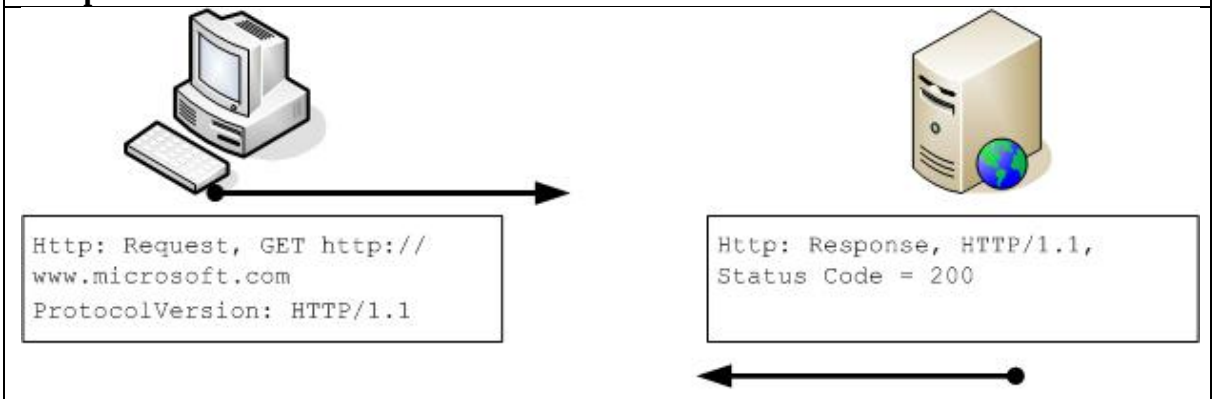
Dónde,

"dirección" =>es el nombre del dominio de internet o dirección ip

"numero" => de puerto si no se coloca usa por defecto el 80

"path "=>recurso a acceder

Componentes HTTP



HTTP Versión

Método=> Se trata de la acción que el cliente solicita al servidor (por ejemplo, GET y POST).

Código de estado: es el código que describe lo que sucedió durante esta transacción en particular (por ejemplo, 200, 301 y 407).

Razón: es un complemento al campo anterior (por ejemplo, está bien, NO OK).

Headers: los contenidos de la cabecera (cabecera) dependerá de la versión del protocolo HTTP en uso. Por ejemplo, o protocolo HTTP/1.1., tiene algunos campos específicos para esta versión.

Body: algunos contienen un cuerpo de mensaje de texto, que a su vez son los datos en sí. Sin embargo, algunos otros tipos de mensaje contiene ningún cuerpo.

Fuente: http://blogs.technet.com/b/latam/archive/2007/09/10/utilizando-o-network-monitor-3-para-entender-o-tr-fego-http.aspx

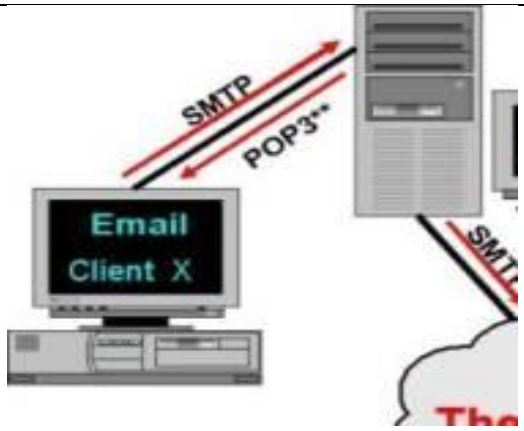
Trabaja en un entorno Cliente/Servidor, en la que el cliente mediante una dirección URL accede al documento que desea utilizar. El proceso general del protocolo se realiza mediante una solicitud http y una respuesta http. La petición la realiza mediante un comando GET, POST, etc., que procesa la sintaxis de petición mientras que el servidor devuelve una respuesta mediante un código de estado

2.3.4 Protocolo de Oficina de Correo Post Office Protocolo Versión (Pop3)

2.3.4.1 Descripción

Permite la recepción del correo, es un software de Agente Usuario de Correo (MUA) que ofrece la debida interfaz para leer y escribir los mensajes desde el buzón, en esta versión presenta la ventaja de no requerir conexión continua a internet salvo al descargar los mensajes.

Proceso de Recepción de Correo Electrónico en el que intervienen el protocolo POP3.



2.3.4.2 Uso y Funcionamiento

Utiliza el puerto 110 en el servidor y se debe contar con una cuenta que permita la identificación del usuario para que al conectarse el cliente POP obtenga información de sus mensajes y solicitar la descarga de alguno de ellos.

Al iniciarse la conexión se procede a la autorización mediante la verificación de los datos, una vez aprobado procede a ejecutar las peticiones por parte del cliente las mismas que serán actualizadas de ser necesario para finalmente cerrar la sesión.

2.3.5 Protocolo simple de transmisión de correo (SMTP).

Fuente:
http://www.racsa.co.cr/consejos_navegacion/proteccion/spam/index_clip_image004.jpg

2.3.5.1 Descripción.

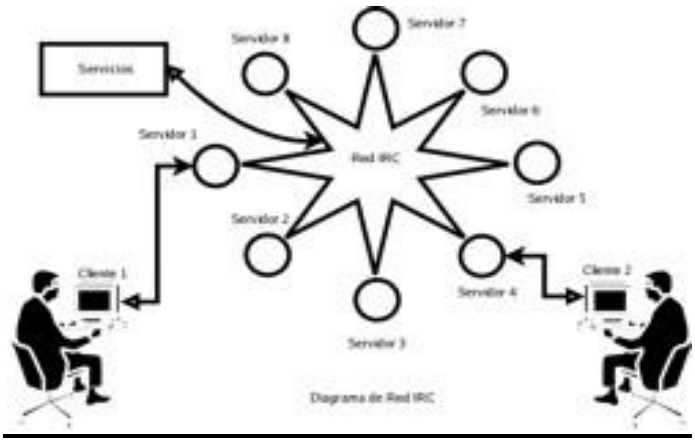
Este protocolo define los formatos que permitan el intercambio de correo electrónico entre computadores por lo tanto funciona como un Agente de Transporte (MTA), se encarga de la parte de envío de correo electrónico desde el origen al destino.

2.3.5.2 Uso y Funcionamiento

Utiliza TCP y el puerto 25, por lo que, lo primero que hace es establecer una conexión para que una vez que el servidor esté listo para recibir e-mails, el cliente especifique las direcciones origen y destino para enviar el mensaje.

2.3.6 Protocolo IRC (Internet Relay Chat)

Diagrama De Red IRC



Fuente: http://www.malavida.com/blog/b/167/irc-conversacion-en-internet-con-cientos-de-personas

2.3.6.1 Descripción

Este protocolo permite el intercambio de mensajes de texto en tiempo real, similar a la mensajería instantánea con la diferencia que cualquier usuario puede intercambiar información aunque nunca antes lo hayan hecho entre sí mismos.

2.3.6.2 Uso y Funcionamiento

Utiliza el puerto 6667, es necesario que cada cliente se identifique con un nombre único (Nick) para poder conectarse, cada comunicación se realiza mediante canales donde todas las personas que pertenecen a ese canal se podrán comunicar entre ellos y participar en tantos canales como puedan. Es de fácil implementación y no muy seguro.

Conclusiones del Capítulo.

A lo largo del desarrollo de este capítulo hemos logrado adquirir ciertos conocimientos acerca del funcionamiento de los protocolos en cada una de las capas del modelo TCP/ IP y su importancia dentro de una comunicación de red,

Las aplicaciones de Internet que se destacan en la última capa así como los otros protocolos de las anteriores serán mencionados continuamente, por lo que es necesario tenerlos presentes de aquí en adelante.

En el siguiente capítulo, se estudiarán puntos más acordes al tema de tesis planteado, como son las herramientas y protocolos utilizados en la actualidad para el análisis y control de ancho de banda. Sin más que decir a continuación el Capítulo 3.

CAPÍTULO 3

Objetivos:

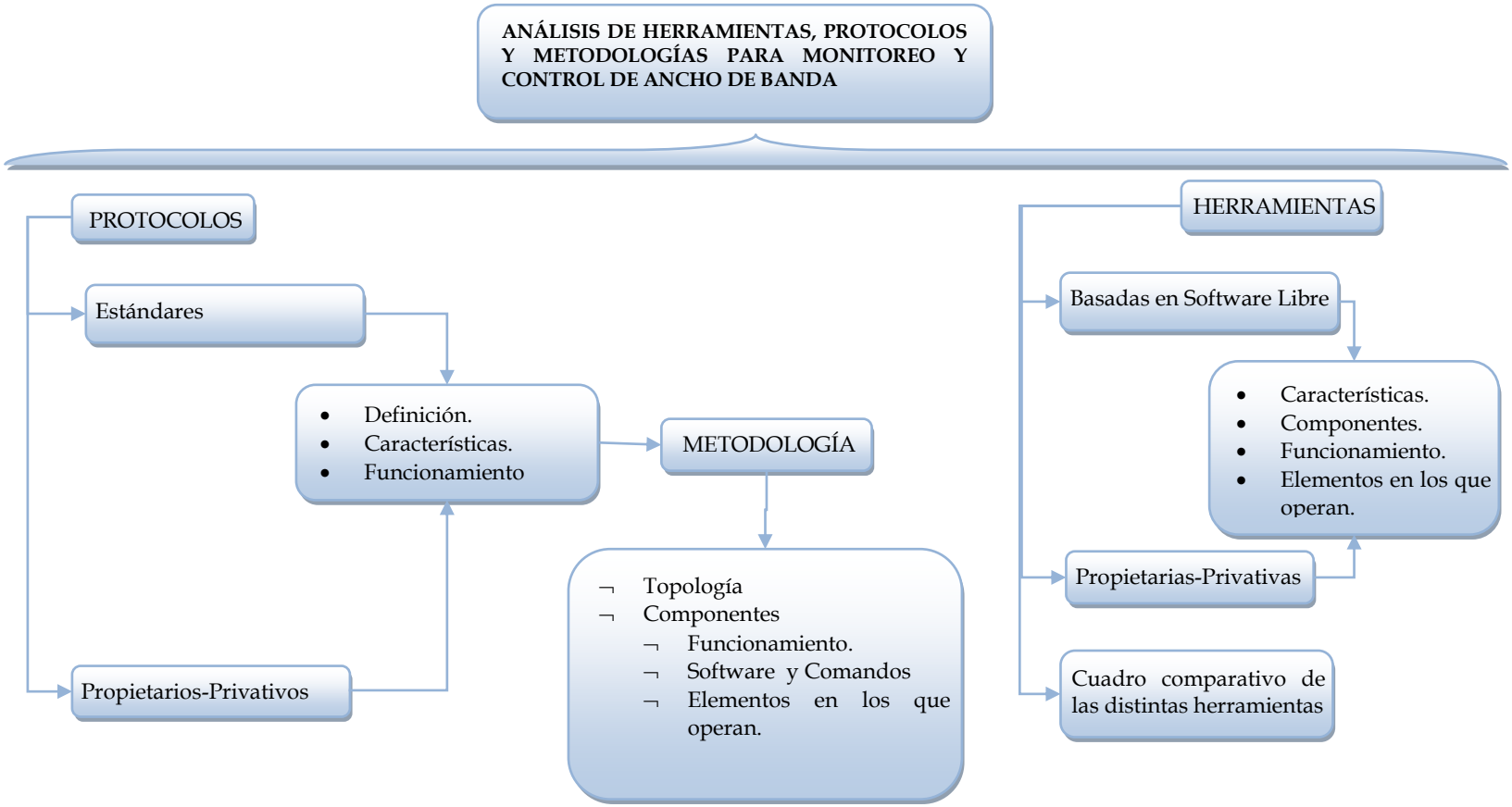
Objetivo General:

- Analizar herramientas, protocolos y metodologías para el Monitoreo y control de ancho de Banda

Objetivos Específicos:

- Analizar y estudiar protocolos que nos ayuden al monitoreo de red por aplicación.
- Considerar las metodologías que utilizan los diferentes protocolos de monitoreo
- Establecer un cuadro comparativo sobre herramientas de monitoreo orientadas a software libre y propietarios privativos.

Esquema (Mapa Conceptual):


ANÁLISIS DE HERRAMIENTAS, PROTOCOLOS Y METODOLOGÍAS PARA MONITOREO Y CONTROL DE ANCHO DE BANDA
PROTOCOLOS
Estándares
Definición.
Características.
Funcionamiento
METODOLOGÍA
Topología
Componentes
Funcionamiento.
Software y Comandos
Elementos en los que operan.
Propietarios-Privativos
HERRAMIENTAS
Basadas en Software Libre
Características.
Componentes.
Funcionamiento.
Elementos en los que operan.
Propietarias-Privativas
Cuadro comparativo de las distintas herramientas

ANÁLISIS DE HERRAMIENTAS, PROTOCOLOS Y METODOLOGÍAS PARA MONITOREO Y CONTROL DE ANCHO DE BANDA

Introducción.

Como lo mencionamos anteriormente, éste capítulo presentará un análisis acerca de las herramientas y protocolos de gestión de red con el objetivo de ayudarnos en la identificación de lo necesario para el desarrollo de nuestro sistema de monitoreo.

Entre los protocolos se destacan SNMP, Netflow, IPFix, entre otros. Comenzaremos con un estudio de las MIB **(Manager Information Base)** que son nombradas muy a menudo en este tema.

3.1. MIB (Manager Information Base).- Base de Datos de Información de Administración

Definición:

> La MIB es una base de datos completa y bien definida con una estructura en árbol adecuada para manejar diversos grupos de objetos con identificadores exclusivos para cada objeto.[10]

A través de la MIB se logra acceder a la información acerca de hardware, estadísticas de rendimiento, etc., dicha información está contenida en la memoria interna de los dispositivos de red y se utiliza para una gestión adecuada.

Versiones MIB

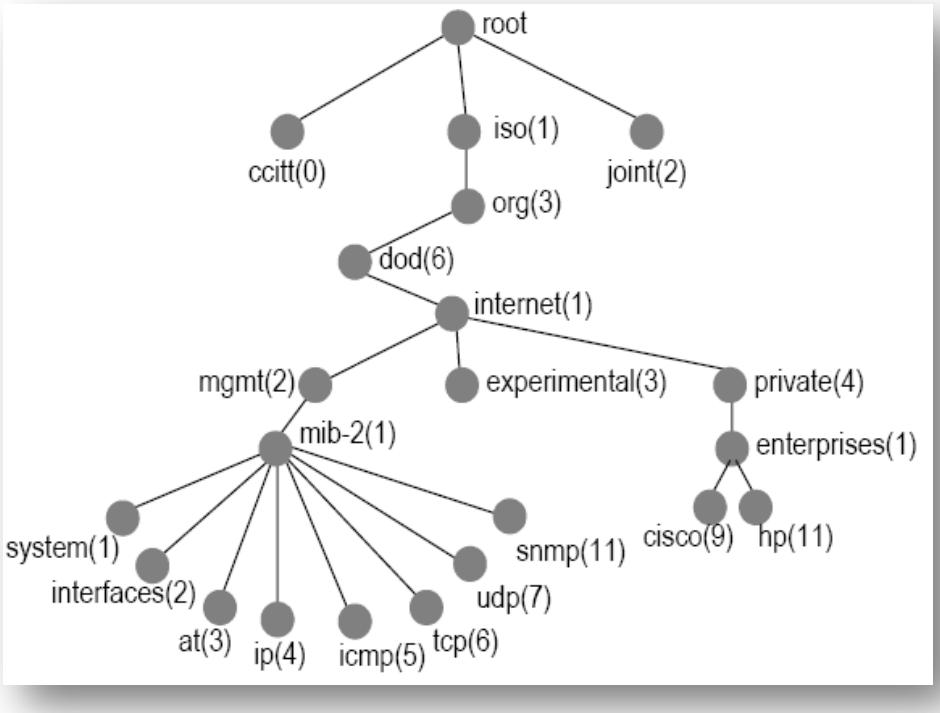
Existen MIB-I y MIB-II, en este caso nos centraremos en la MIB-2 puesto que es la base de datos más completa y común en la actualidad aunque cabe recalcar que tanto fabricantes de hardware como programadores están en libertad de desarrollar MIBs

[10] http://www.coit.es/publicac/publbit/bit102/quees.htm

propietarias que contemplen descripciones especificas, obteniendo de ésta manera total autoridad de los objetos.

Estructura de la MIB-II

Figura 3.1. Estructura de la MIB-II



Fuente: http://www.javeriana.edu.co/biblos/tesis/ingenieria/Tesis190.pdf

Una MIB se basa en el formato de la estructura de gestión de la Información SMI (Structure of Management Information), en forma de árbol jerárquico global, en el que:

- Cada Nodo del árbol representa un objeto, que es identificado con un nombre o identificador del objeto (OID) que es único en cada caso y se

forma de la combinación de una serie de números enteros que vienen en los nodos del árbol separados por puntos.

Áreas.- Se definen 4 áreas en las que se pueden utilizar las MIB

- **Administración.-** Define un estándar de administración
- **Privados.-** Reservado para objetos definidos por individuos u organizaciones de forma privada.
- **Experimentales.-** Reservado para pruebas e investigación
- **Directorio.-** Actualmente no utilizado [11]

Grupos MIB- II.- A más de los 8 niveles con los que trabajaba en MIB-I, MIB-II incorpora 3 más detallados a continuación:

Tabla 3.1. Grupos MIB-II

Nivel	Grupo	Descripción
1	Systems (SYS)	Muestra información genérica del sistema gestionado.
2	Interfaces (INT)	Presenta información de las interfaces presentes en el sistema y estadísticas, también incluye objetos que describen como los dispositivos son conectados a la red.
3	Address translation (ADD TRS).	Contiene objetos apropiados para el mapeo de las direcciones de red a las direcciones físicas

[11] Tomado de: http://www.quanaxoft.com/blog/category/programacion/programacion-web/

4	Internet Protocol (IP)	Proporciona las tablas de rutas, y mantiene estadísticas sobre los datagramas IP recibidos.
5	Internet Protocol Message (ICMP)	Se almacenan contadores de paquetes ICMP entrantes, salientes y errores.
6	Transmisión Control Protocol (TCP)	Información relativa a la configuración, estadísticas y estado de protocolo
7	User Datagram Protocol (UDP)	Cuenta el número de datagramas UDP, enviados, recibidos y entregados.
8	Exterior Gateway Protocol (EGP)	Recoge información sobre el número de mensajes EGP recibidos, generados. Contiene objetos asociados con el exterior gateway protocol
9	CMOT	Describe una arquitectura de gestión de red usando los protocolos CMIS/CMIP del modelo OSI sobre la familia de protocolos de internet. Esta arquitectura proporciona un canal para que un gestor y una entidad de red remota intercambien información de control y monitorización
10	TRANSMISIÓN	Deriva de diferentes tecnologías del nivel de enlace implementado en las interfaces del sistema gestionado, información sobre los esquemas de transmisión y protocolos de acceso.
11	SNMP	Almacenan información relevante acerca de la implementación y operación del protocolo SNMP detallado en lo posterior

Fuente: 8174575-Snmp.pdf

Ejemplo de Codificación según SMI

Si se desea consultar interfaces sería: *iso.org.dod.internet.mgmt.mib_2.interfaces*

O su equivalente .*1.3.6.1.2.1.2.2.1*

Es decir, inicialmente se identifica el organismo de estandarización, ISO y dentro de éste está ORG y dentro DOD (*Departamanet of Defense*), donde la primera rama del árbol desde DOD es Internet. Así sucesivamente hasta especificar la variable (u objeto) a consultar. [12]

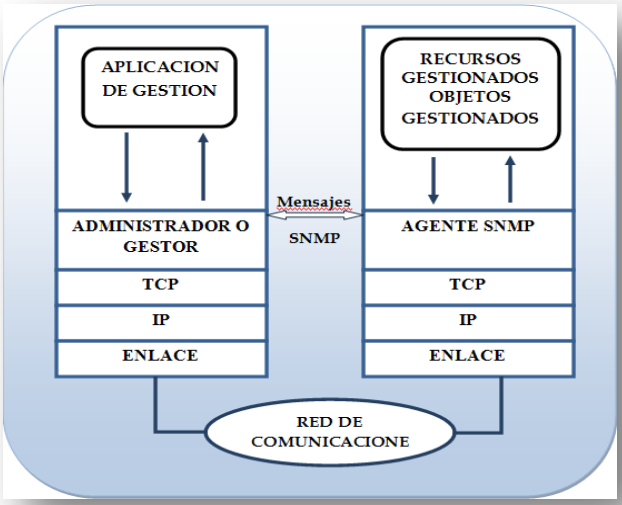
Una vez evaluadas las MIB podemos adentrarnos en lo que son los protocolos de gestión de red, como es el caso del SNMP que trabaja precisamente haciendo consultas a estas bases de datos que por lo general son pequeñas debido a las limitaciones de los dispositivos lo que hace que sea sencillo de implementar.

3.2 Protocolo SNMP

Simple Network Management Protocol (Protocolo Simple de Administración de Red).

[12] Tomado de: informatica.uv.es/it3guia/ARS/transparencias_1c/snmp-santi.ppt

Figura 3. 2. Modelo de Comunicación SNMP



Fuente: http://www.javeriana.edu.co/biblos/tesis/ingenieria/Tesis190.pdf

Definición:

"Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red."[13]

Este protocolo es de gran importancia en nuestro estudio puesto que es el estándar más utilizado en la actualidad para la administración de los dispositivos de red, es así que todos los fabricantes de estos dispositivos incluyen soporte para SNMP, lo que permite que topologías de red formadas por una gran variedad de marcas sean fácilmente gestionadas en su totalidad.

Características:

- Ocupa pocos recursos de la red
- Es sencillo de implementar

[13] "Simple Network Management Protocol" :http://es.wikipedia.org/wiki/SNMP

- Permite elegir al administrador que va a monitorizar : ancho de banda , sobrecargas en el servidor, administración de papel en la impresora, etc. [14]
- Fácil de actualizar lo que permite gran capacidad de expansión
- Genera un exceso de tráfico, volviéndolo incompatible en amplios entornos de red
- Los dispositivos administrados con SNMP, pueden enviar alertas en caso de que ocurra algún evento poco usual.

Versiones.- Existen 3 versiones de este protocolo en cada una de ellas se han realizado mejoras en cuanto a rendimiento, seguridad y confidencialidad, las más utilizada es la versión 2 ya que la 3 aunque se ha esforzado en aspectos de seguridad no ha sido acogida por las industrias como se esperaba.

Tabla 3.1. Tabla comparativa de Versiones

VERSIÓN	CARACTERÍSTICAS
SNMP versión 1 (SNMPv1).	- Autenticación basada en nombres de comunidad (*community strings*), que consiste en una lista de control de acceso sobre direcciones IP y una palabra clave.[15] - Existen sobrecargas en la transferencia de datos
SNMP versión 2 (SNMPv2c).	- Surge en el año 1997 - Mantiene la autentificación de la primera versión - Resuelve el problema sobrecargas de transferencias de datos optimizándolas (GetBulk e Informs). - Incorpora un mecanismo de recuperación de información en bloques *(bulk request)*, junto con mensajes de error más detallados. - Soluciona los problemas de monitorización remota con RMON

[14] Tomado de Tesis 210.pdf

[15] dmrPrac1aacrivasmnpcisco.pdf

SNMP versión 3 (SNMPv3).	¬ SNMPv3 = SNMPv2 + (Seguridad y administración) ¬ Es la última versión hasta la actualidad, incorpora: ¬ Integridad de los mensajes ¬ Autentificación Presenta el modelo de seguridad basado en usuario USM (*User-Based Security Model*) que proporciona los servicios de autentificación y privacidad. ¬ Encriptación

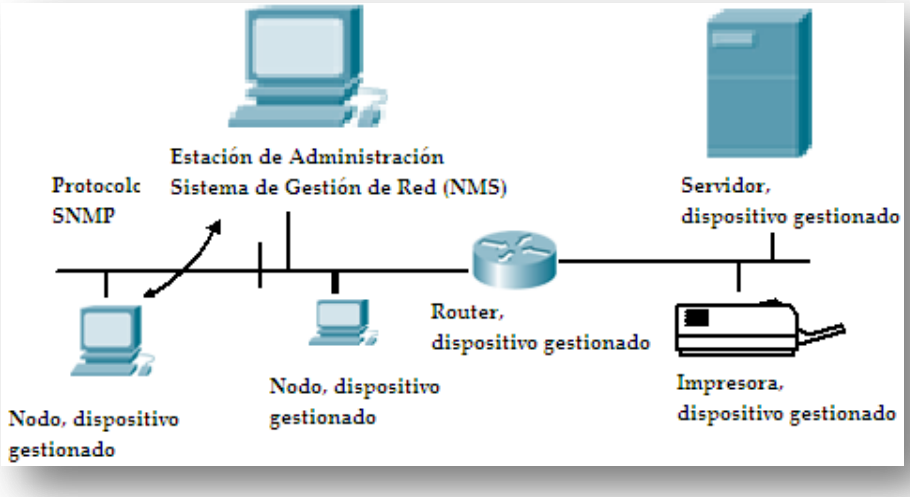
Fuente: Serrano Veronica – Llivigañay Eugenia

Además del SNMP existe otro protocolo, el **CMIS, Protocolo de administración de información común** (Common Management Information Service/Protocol) de OSI, ofrece una mejor administración muy bien planteada con mejoras en cuanto a rendimiento y seguridad que en muchos aspectos supera a SNMP, pero que debido a la complejidad y costo a nivel de Hardware y Software que este representa en su implementación no será evaluado en nuestro estudio.

Metodología SNMP

Topología.

Figura 3.3. Metodologia SNMP



Componentes que intervienen:

El modelo de SNMP se fundamenta en el uso de 3 componentes:

1. Dispositivos Gestionados (Managed Devices): Son los elementos que interviene en la red y ejecutan un *agente*, estos pueden ser:

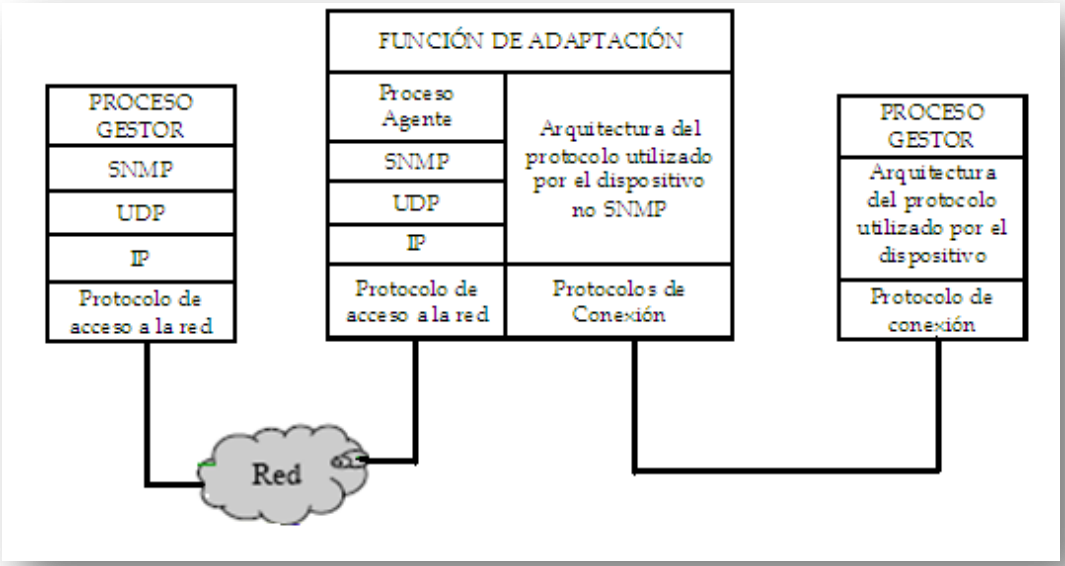
- **Dispositivos Finales:** Computadoras, estaciones de trabajo. Servidores, etc.
- **Dispositivos Intermediarios:** Routers, hubs, switches, mau, etc.
- **Otros:** Impresoras, Modems, UPS, alarmas, etc.

2. Agentes SNMP.- Son aplicaciones que recolectan la información del dispositivo desde la Base de Datos de Información de Administración (**MIB).** Estos Agentes realizan tareas tanto de consulta como de modificación a la **MIB**. Para tener una mayor conocimiento de lo que es posible analizar a través de SNMP es crucial saber a detalle el funcionamiento y a acceso a las MIBs por parte estos agentes.

Si bien hoy en día la gran mayoría de los dispositivos vienen con un Agente SNMP o en su defecto presta las condiciones para que pueda ser incorporado, en un principio no fue así, es por ello que en caso de ser necesario administrar un dispositivo sin un agente se deben utilizar los denominados *Agentes proxy* detallados a continuación:

3. Agentes Proxy.- Casi obsoletos en la actualidad**,** este agente requiere que el producto cuente con una función administradora aunque sea propietaria con la que se comunicará mediante los debidos protocolos. El agente se ubica entre el dispositivo y la red actuando como representante de uno o más dispositivos que se encuentran en el proxy.

Figura 3.4. Proxies



Fuente: http://zeus.unex.es/~victor/software/RAL/Monitorizacion/tema3.pdf

Sistema de gestión de la Red (NMS, Network-Management System).- es el equipo en el que se procesa y visualiza información que llega por parte de los agentes gracias a la ayuda del protocolo SNMP, contiene las aplicaciones que facilitan las tareas de administración de la red, puede trabajar en cualquier plataforma: Windows, GNU-Linux, Mac OS , etc.

Funcionamiento del Protocolo SNMP.- Precisamente es el encargado de habilitar la comunicación entre los agentes y gestores de Red. Como el resto de protocolos de la capa de aplicación se basa en el modelo Cliente/Servidor.

- **Operaciones:** Este protocolo trabaja con 4 operaciones básicas:

  GET para lectura**, SET** para escritura**, TRAP** para notificaciones y **GET-NEXT** para realizar recorridos jerárquicos de la MIB

- **Mensajes SNMP.-** A través de estas operaciones presenta los siguientes mensajes:

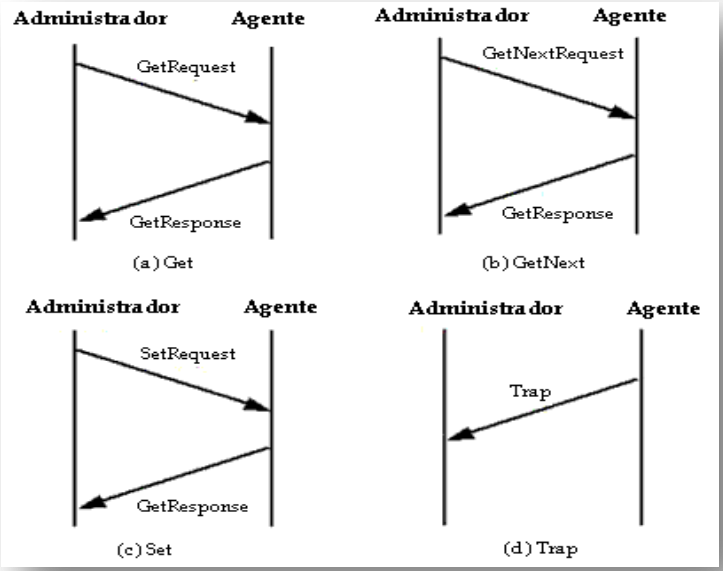
Tabla 3.2. Mensajes SNMP

¬ **GET REQUEST** ¬ Solicita (y se recoge en la contestación) el valor de un objeto o variable contenido en la MIB
¬ **GET NEXT REQUEST** ¬ Solicita el siguiente atributo de un objeto una vez se ha usado el anterior ¬ Se usa para descubrir los objetos de la MIB del dispositivo
¬ **GET BULK (Soportado a partir de la versión 2)** ¬ Lo mismo que el anterior pero más eficiente ya que en una sola petición se trae todos los valores de la tabla.
¬ **SET REQUEST (y SET NEXT REQUEST)** ¬ Solicita modificar el valor de un objeto en la MIB, deben ser tratados con sumo cuidado.
¬ **GET RESPONSE** ¬ Respuesta del agente con los valores solicitadores ante un Get o Set request
¬ **TRAP** ¬ Mensaje generado por agente para informar situaciones de alerta, son limitados para no influir en el trafico de la red.
¬ **INFORM, NOTIFICATION, REPORT (Soportado a partir de la versión 2)** ¬ Mensajes de un dispositivo administrador a otros dispositivos para intercambiar información, errores, confirmaciones, etc.

Aunque por lo general trabaja con el protocolo de transporte UDP también lo puede hacer con TCP, en ambos casos a través de los puertos 161 y 162.

En el caso de UDP, el puerto 161 se usa para las transmisiones normales mientras que el 162 lleva mensajes de tipo Trap o interrupción y es el único caso en el que el agente inicia la acción. A continuación se presenta una imagen en la que se observan este intercambio de mensajes.

Figura 3. 5. Mensajes de intercambio SNMP



Fuente: www.javeriana.edu.co/biblos/tesis/ingenieria/Tesis190.pdf

3.3 Protocolo RMON

Remote Network Monitoring (Red de Monitoreo Remoto).

Definición:

Son conocidas como sondas RMON estas permiten la recolección periódica de los datos del tráfico de red como lo realiza SNMP, además de permitir su procesamiento de datos al enviarlo a un equipo administrador

Características:

La extensión RMON permite observar y gestionar la red como un todo

La MIB asociada es 1.3.6.1.2.1.16

Es una extensión de SNMP.

Ventajas:

- ¬ Monitorización configurable de la sonda RMON
- ¬ Detección local de fallos e informe al gestor principal de los mismos
- ¬ Recolección de información para múltiples gestores (almacena la configuración que recibe en tablas).
- ¬ Disminución del consumo de recursos en la red y en la estación central de gestión.

Elementos en los que opera:

RMON se puede presentar dentro de un host, switch, router o dispositivos

Versiones:

Tabla 3.2. Tabla comparativa versión RMON

Versión	Característica principal
RMON1	Trabaja en información de capa 1 y 2.
RMON2	Trabaja en información de capa 3 y superiores

Componentes:

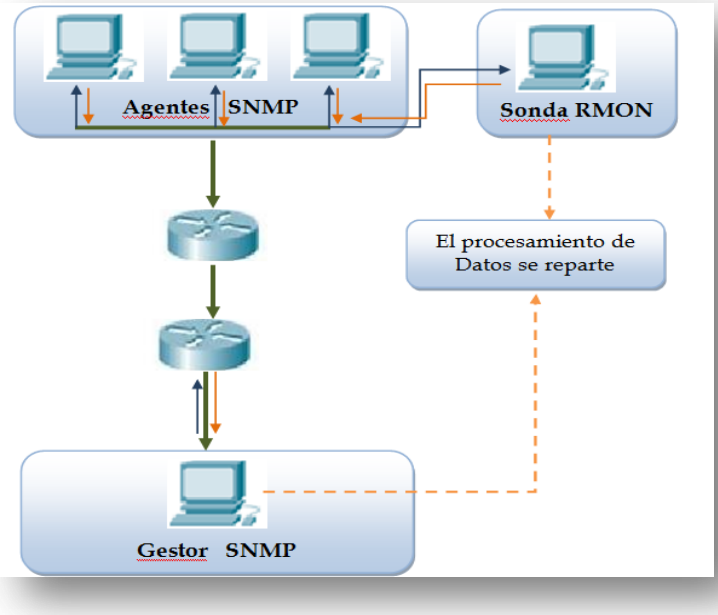
Aunque sigue el mismo estándar que SNMP, RMON está conformada por dos componentes:

Una sonda (o un agente o un monitor)

Un cliente, (Estación para la administración)

Funcionamiento de RMON:

Figura 3.6. Gestión de la Red con RMON

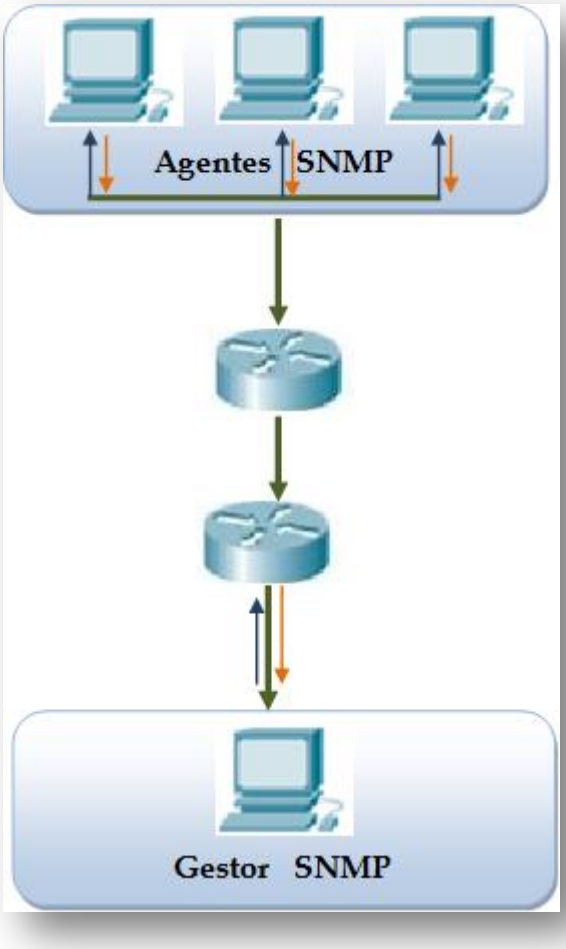


Fuente: *www.bibliociencias.cu/gsdl/collect/eventos/index/assoc/...dir/doc.ppt*

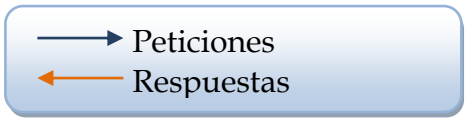
Explicacion:

1. El gestor configura la sonda RMON empleando SNMP
2. La sonda recibe la informacion de configuración, recoge datos y los Procesa
3. Las sondas envian estadisticas elaboradas al gestor

Figura 3.7. Gestión de la Red sin RMON



Fuente: *www.bibliociencias.cu/gsdl/collect/eventos/index/assoc/...dir/doc.ppt*

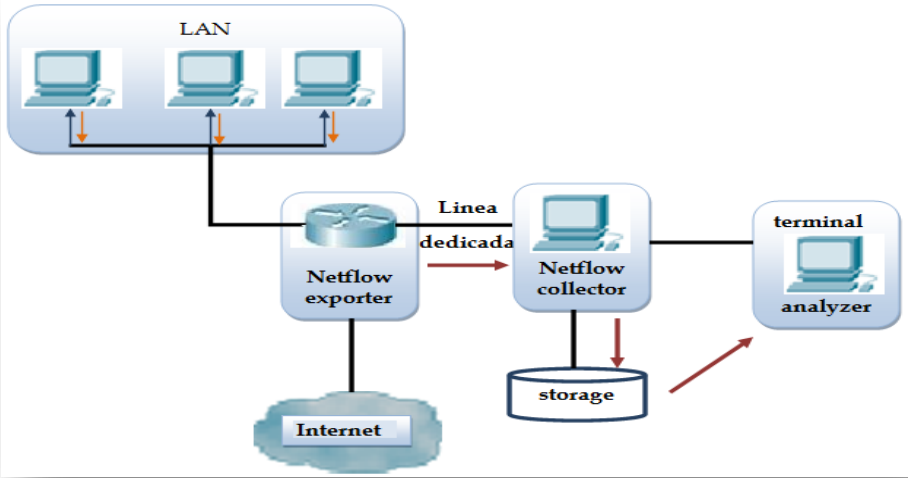


Explicacion:

1. El gestor realiza las peticiones
2. Las peticiones llegan a la red destino
3. Los agentes responden
4. La respuesta se encamina al gestor
5. Las respuestas llegan al gestor y son Procesadas.

3.4 Protocolo Netflow

Figura 3.8. Arquitectura de Netflow



Fuente: http://en.wikipedia.org/wiki/Netflow

Definición:

Para poder definir a Netflow partimos del concepto de Flujo quien se define como *una secuencia unidireccional de paquetes con algunas propiedades comunes que pasan a través de los dispositivos de red*[16].

Netflow es un protocolo de red que en un principio fue desarrollado por CISCO Systems quien funciona en el IOS del equipo permitiendo así recolectar los datos del tráfico de red IP.

Características:

- Esta estructura tiene soporte en las siguientes plataformas como IOS, Juniper, Linux, FreeBSD y OpenBSD.

[16] http://www.ietf.org/rfc/rfc3954.txt

- Permite la generación de registros Netflow a quienes se les exporta en paquetes desde el router y son recolectados por un colector Netflow.
- *Responde las preguntas quién, qué, dónde y cómo basado en el tráfico IP*[17]
- *No requiere instalación de sondas basadas en hardware, que pueden ser onerosas para su adquisición y mantenimiento, pueden producir fallas en la red y, si se instalan en línea con el flujo de datos, retrasar el tráfico de la red.*[18]
- Da una información detallada de cómo se comporta la RED.
- Realiza monitorización de las aplicaciones que están utilizando puertos dinámicos.
- Por su alto consumo de recursos del CPU su análisis se basa en el muestreo lo que ocasiona imprecisión en los registros de los flujos.
- Tiene un *flow cache* en donde se contienen los datos sobre los flujos que se encuentren activos.
- Cada flujo está representado por un *flow record*, en la hay campos de información.
- *Flow record* es actualizado cuando los paquetes que están en el flujo son conmutados

Versiones:

Tabla 3.3. Tabla comparativa versión de Netflow

Versión	Comentario
V1	Primer intento
V5	La mayoría de la versión usada v6
V6	Información de la encapsulación

[17] http://lacnic.net/documentos/lacnicx/Intro_Netflow.pdf

[18] http://www.google.es/url?sa=t&source=web&cd=20&ved=0CE0QFjAJOAo&url=http%3A%2F%2Fwww.arbornetworks.com%2Fes%2Fdocman%2Fpeakflow-x-data-sheet-espa-ol%2Fdownload.html&ei=D25MTNSGBcP58AakrOE-&usg=AFQjCNHpt-3Vk4SAepPx4o1OjoksGgeiCA

V7	Cambie la información
V8	Varias formas de la agregación
V9	Plantilla basada, permitiendo muchas combinaciones
IPFIX	A la v10; El IETF estandarizó Netflow 9 con los campos de la empresa y la otra entrada de la comunidad

Fuente: http://www.worldlingo.com/ma/enwiki/es/Netflow

Funcionamiento:

La tecnología NetFlow se refiere a como un router o switch realiza la exportación de muestras del tráfico al generar registros de NetFlow que pasa por el mismo quienes son exportados vía datagramas UDP a un dispositivo o máquina quien se encarga de recolectarla.

Con excepción de la Capa de Aplicación, desde la capa 2 – 4 se examina parámetros de las muestras del tráfico como son:

- Dirección IP origen y destino
- Protocolo de capa4
- Puerto de origen y destino
- TOS byte (Type of Service)
- Interfaz de entrada al equipo de red

Una vez que los datos son exportados, a esta información se le suma la cantidad de bytes asociados que son guardados en el NetFlow cache, para ser procesada mediante la generación de reportes para los Administradores.

Características:

- El router o switch son los encargados de informar del tráfico de red
- Es escalable debido a que no depende del tipo de interfaces.
- Brinda facilidades para añadir más interfaces.

Desventajas:

- ¬ Da un análisis menos detallados
- ¬ Es dependiente de la electrónica de red ya que necesita soporte NetFlow

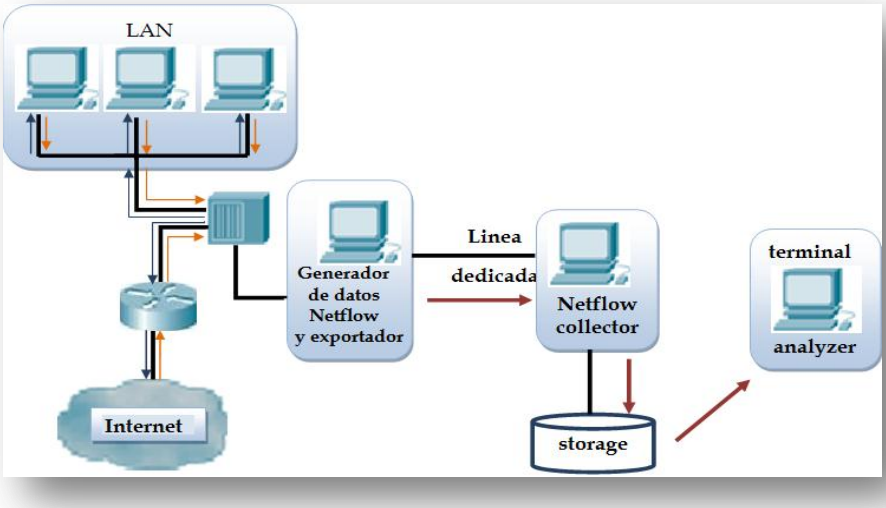
Elementos en los que opera:

- ¬ Netflow puede operar tanto en routers o switchs que son los encargados de exportan las estadísticas del tráfico de red.

Metodología NETFLOW

Topologías de Netflow:

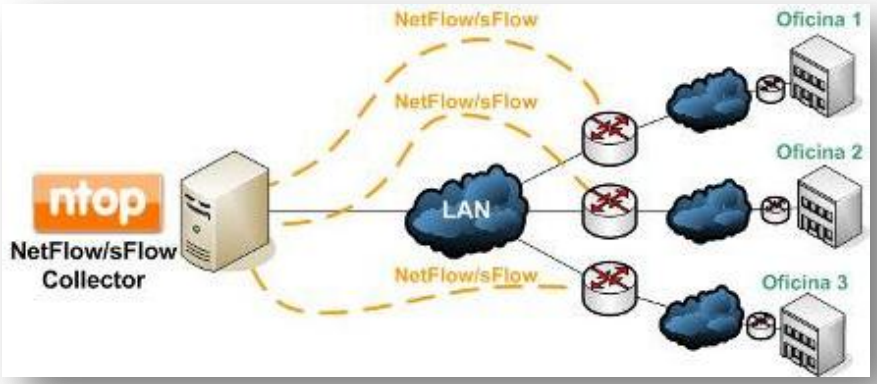
Figura 3.9. Topología cuando el router es un dispositivo que no soporta Netflow



Explicación:

En esta topología se utiliza un hub para transmitir todo el tráfico que se escucha en la Red y mediante un servidor GNU que contendrá una sonda para generar datos Netflow y exporte los datos a un colector para ser enviados a una Base de Datos que serán sustraídos por otro software que se encargara de analizar los datos obtenidos.

Figura 3.10. Como colector NetFlow/sFLow

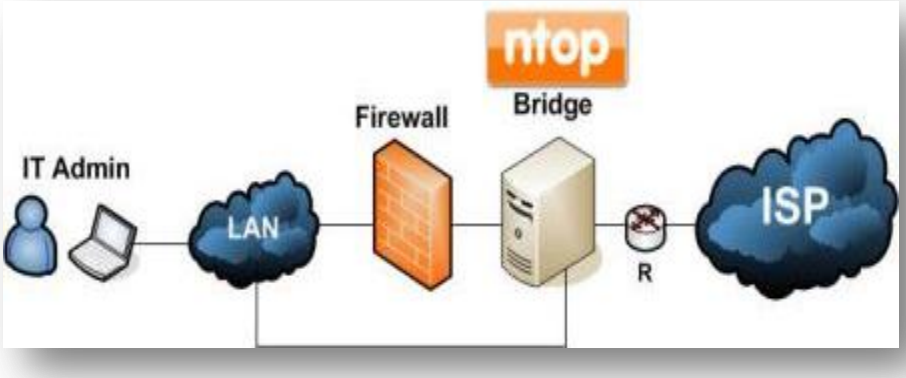


Fuente: http://www.ntop.org/news.php

Explicación:

En esta topología se observa que **ntop** funciona en una LAN, como colector NetFlow y sFlow para analizar el tráfico de red que fluye a través de los enrutadores quienes se encargan de enviar periódicamente los datos a dichos colectores.

Figura 3.11. Como bridge a la salida de Internet o de cualquier canal de comunicaciones.



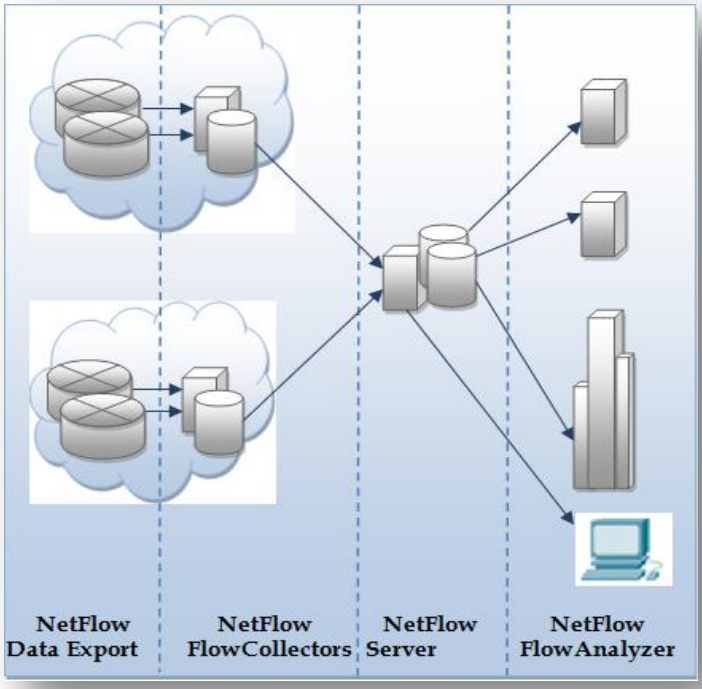
Fuente: http://www.ntop.org/news.php

Explicación:

En el ntop puede colocarse un bridge y no afectara en su funcionamiento debido a que es transparente tanto para el "Firewall" como para el router la existencia de ntop, siendo así una forma en la que se captura el tráfico entrante y saliente que se da en el medio.

Componentes:

Figura 3.12. Componentes

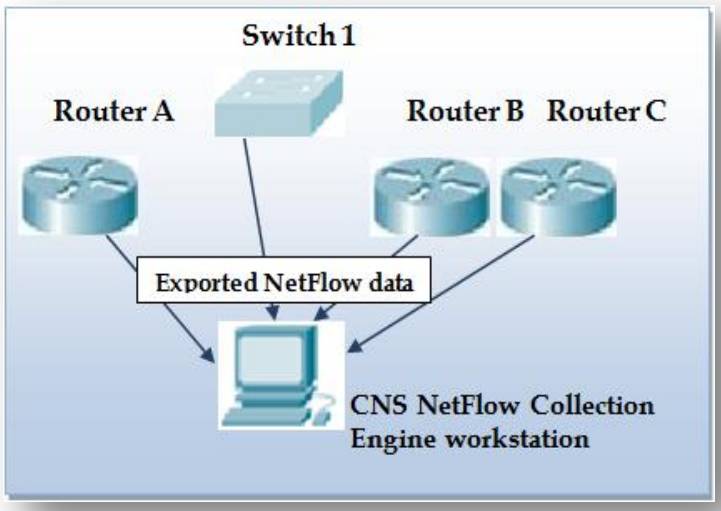


Fuente: http://www.bibliociencias.cu/gsdl/collect/eventos/index/assoc/HASH010e.dir/doc.pdf

- **Exportador (Router o Switch)**

La exportación del tráfico de red permite que estos sean recolectados y procesados.

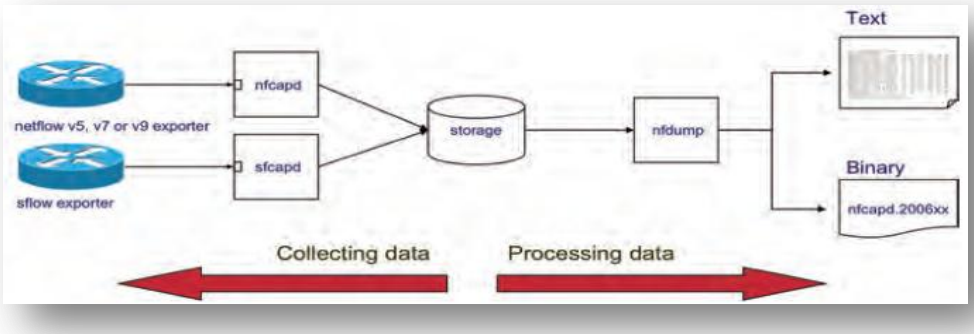
Figura 3.13. Exportador



Fuente: Netflow.pdf

- Colector
- Oye el tráfico por el puerto UDP
- Guarda o reenvía el flujo a otros colectores
- Analizador
- Es una herramienta que permite Filtrar, muestrear y analiza graficas de los datos

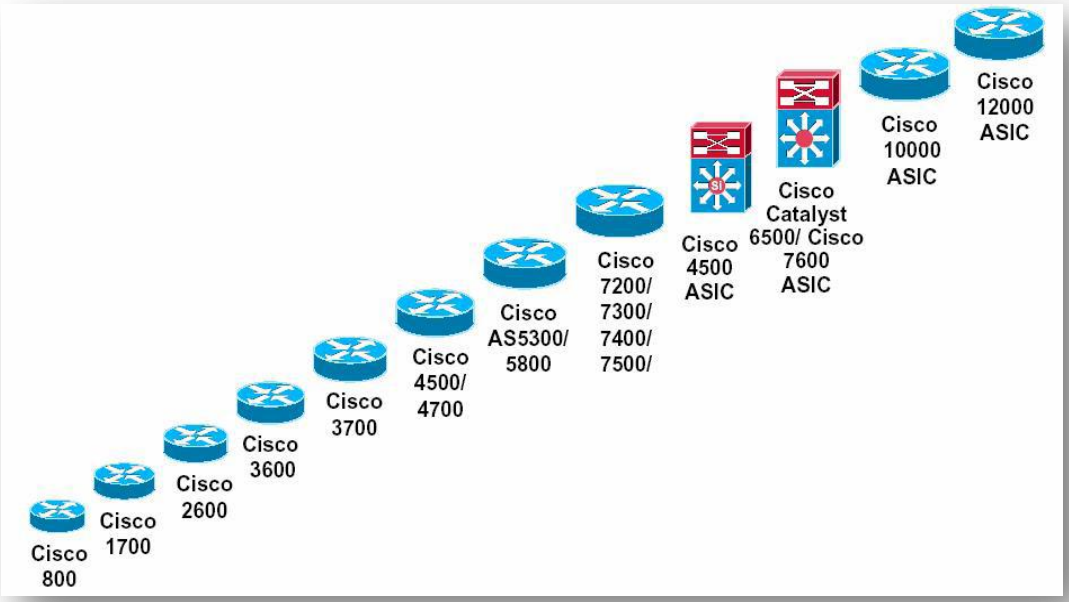
Figura 3.14. Arquitectura de Monitorización y Análisis basada en el uso de NFDUMP/NFSEN



Fuente: enfoque1.pdf

Dispositivos que lo soportan:

Figura 3.15. Dispositivos que soportan Netflow



Fuente: enfoque1.pdf

3.5 Protocolo IPFIX

Internet Protocol Flow Information Export (**Exportación de la información del flujo del Protocolo Internet**).

Glosario

IPPM: Internet Protocol Performance Metrics, constituye el marco de referencia en el cual tanto proveedores como clientes pueden, gracias a un conjunto de métricas comunes, llegar a establecer acuerdos de calidad de servicio y verificar el correcto cumplimiento de los mismos.

SCTP: Stream Control Transmission Protocol (SCTP) es un protocolo de comunicación de capa de transporte que surge en el año 2000, provee confiabilidad, control de flujo y secuenciación como TCP y opcionalmente permite el envío de mensajes fuera de orden similar al envío de datagramas UDP

Definición:

Define un procedimiento estándar en la obtención de información referente a los flujos establecidos en conexiones basadas en TCP/IP[19]

IPFIX está basado en la versión 9 de NetFlow aprobada en el año 2006, cuya finalidad es el ahorro de ciclos de CPU mediante el almacenamiento en memoria acerca de la correspondencia entre el flujo y su interfaz de salida para que en posteriores paquetes pertenecientes a ese flujo no es sea necesario recurrir a consultas en tablas de encaminamiento.

Se ha visto la necesidad de estudiar este protocolo debido a que es el estándar de medición que están adoptando los dispositivos de red actualmente y para el futuro.

Características

¬ IPFIX no es compatible con versiones anteriores a la versión 9 de Netflow

¬ Permite implementar herramientas efectivas que cumpla con las métricas definidas en IPPM, ancho de banda efectivo, tiempo de respuesta, etc.

[19] http://jungla.dit.upm.es/~jlopez/publicaciones/telecomid04lopezber.pdf

¬ Los procesos de recolección de información no influyen en el tráfico normal de datos que se producen en la red

¬ Constituye un modelo bien estructurado que hace que sea fácilmente extensivo

Metodología:

Componentes que intervienen:

Similar a la topología Netflow:

"Un proceso de medición (**metering**) colecta paquetes de datos en un punto de observación, opcionalmente estos son filtrados y agregan información acerca de los paquetes, usando el **protocolo IPFIX**, un **exportador** (exporter), envía esta información a la **colector** (collector). El exportador y colector pueden recibir datos desde muchos exportadores " [20]

Funcionamiento del protocolo IPFIX

El protocolo toma la información del flujo IP y crea una plantilla en formato binario, genérica, extensible que permita su almacenamiento como datos la transfiere a un colector de exportación para en lo posterior analizar y procesar dicha información en dispositivos externos a la red.

[20] Tomado de: Tesis Ana Belén Castro Romero , Andi del Cisne Estrella Escudero, "2.4.3 IPFIX"

http://dspace.espoch.edu.ec/bitstream/123456789/98/1/18t00375.pdf

IPFIX puede trabajar conjuntamente con los protocolos de transporte UDP, TCP o SCTP .

Tabla 3.4. Cuadro comparativo de herramientas

Herramientas de monitoreo de red

Plataforma	Nombre	Características	Elementos en los que operan	Protocolos que soportan
Unix/ Windows	MRTG	MRTG es una herramienta que grafica datos. ¬ Mide la carga de tráfico sobre las interfaces de los dispositivos. (Es posible hacer otro tipo de mediciones) ¬ Recolecta información de los dispositivos de red cada cierto tiempo ¬ Puede Graficar los datos almacenados en la RRD.	Todos los dispositivos de red disponibles	SNMP
Windows/ Linux/Unix	CACTI	Herramienta de colección y visualización de tráfico ¬ Ofrece tráficos similares a MRTG ¬ Más sencillo de configurar (via web) ¬ Aprovecha el poder de las RRDtool. ¬ Para instalaciones LAN, así como también para redes complejas con cientos de dispositivos.	Todos los dispositivos de red disponibles	SNMP
LINUX	NAGIOS	¬ Se encuentra en la capacidad de alertar a su equipo técnico sobre el problema	Operas en todos los elementos de	SNMP

		¬ *monitorización de servicios de red (SMTP, POP3, HTTP)* ¬ *monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos)* ¬ *independencia de sistemas operativos* ¬ *posibilidad de monitorización remota mediante túneles SSL cifrados ó SSH* ¬ *La posibilidad de programar plugins específicos para nuevos sistemas*.[21] ¬ *Informa automática e instantáneamente 24 horas al día, 365 días al año* ¬ *Disponible interfaz web para consulta del estado de los recursos y servidores* [22]	red disponibles	
UNIX / WINDOWS	NTOP	*Obtiene información y estado del tráfico de la red* *Ntop puede ser visto como un agente de RMON* *Posee una interfaz web basada en HTTP* *Su configuración limitada y la administración es a través de la interfaz web* *El uso de CPU y memoria es reducido* [23] *RRD para almacenar persistentemente estadísticas de tráfico*[24]	Dispositivos que soporten Netflow	Recolector/emisor NetFlow/sFlow

[21] http://es.wikipedia.org/wiki/Nagios

[22] http://www.ua.es/es/servicios/si/documentacion/presentaciones/monitorizacion.pdf
[23] http://www.ntop.org/overview.html

[24] http://es.wikipedia.org/wiki/Ntop

LINUX FREEBSD	IP FLOW METER	*Medidor de flujo IP (IPFM).* *Es una herramienta de análisis de ancho de banda, que mide la cantidad de ancho de banda hosts especificados uso en su enlace a Internet.* *Funciona las 24 horas del día los 365 días del año* *Está escrito con libpcap*[25]	Todos los dispositivos de red disponibles	SNMP
Propietario privativo				
WINDOWS/ LINUX	Nnetflow Analyzer	NetFlow Analyzer es un software (para Windows y Linux), no necesita ningún dispositivo y puede utilizarse para: ¬ Control del ancho de banda de la red con informes instantáneos ¬ Análisis del tráfico de la red ¬ Informes programados y perfiles de alerta	Dispositivos que soporten Netflow	NETFLOW
WINDOWS	OBSERVER	Herramienta para el Análisis y Monitoreo de redes ¬ Ofrece información de control en tiempo real. ¬ Dispara automáticamente una serie de eventos de alerta para tomar decisiones a tiempo**.** ¬ Rastrea múltiples dispositivos SNMP, y la información. ¬ Permite monitorear o predecir tendencias de toda la red	Todos los dispositivos de red disponibles	NETFLOW, SNMP, RMON

[25] http://robert.cheramy.net/ipfm

WINDOWS	GFI NETWORK SERVER MONITOR ™	¬ Consta de un servicio de supervisión de red y un interface de administración separado. ¬ No se necesita instalar software agente en los equipos que desea monitorizar. ¬ Alta fiabilidad y escalabilidad para vigilar redes grandes y pequeñas. ¬ Asegura que un Servicio funcione ¬ Toma Acciones Correctivas Automáticamente ¬ Notificación de Alertas mediante Correo, Buscapersonas o SMS	Todos los dispositivos de red disponibles	SNMP
Comandos				
UNIX: Linux, Solaris, BSD, Mac OS X, HP-UX y AIX	TCPDUMP	¬ *Trabaja con líneas de comandos para analizar el tráfico que circula por la red.* ¬ *Permite al usuario capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado* ¬ *Es necesario tener los privilegios del root para utilizar tcpdump.* ¬ *El usuario puede aplicar varios filtros para que sea más depurada la salida.* [26]	*SNMP*[27]	Operas en todos los dispositivos de red disponibles

[26] http://es.wikipedia.org/wiki/Tcpdump

[27] http://www.pablin.com.ar/computer/info/varios/snmp.htm

Conclusión del Capítulo

La culminación de este capítulo ha sido de gran importancia para definir tanto la topología de red como la de monitoreo que utilizaremos en nuestro Sistema.

Desde ya, hemos decido trabajar con una topología basada en Netflow, puesto que gracias a las características que presenta nos permitirá obtener la información necesaria en las estadísticas de monitoreo que deseamos generar, con reportes más útiles y detallados.

CAPÍTULO 4

Objetivos:

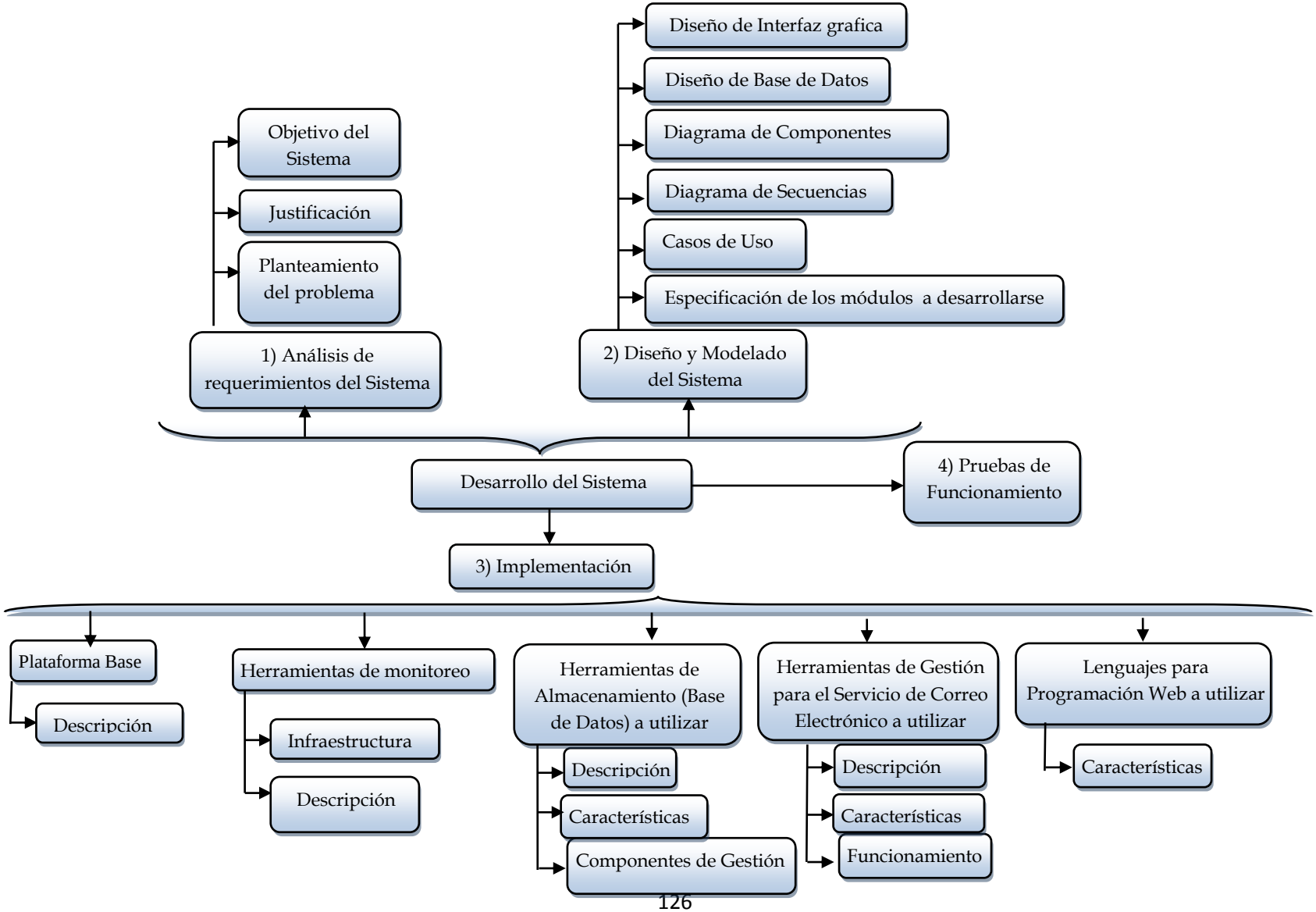
Objetivo General:

- Implementar un Sistema de Monitoreo

Objetivos Específicos:

- Realizar un análisis de los requerimientos para la implementación del Sistema
- Crear diseños y modelos que representen a nuestro sistema
- Analizar las características más sobresalientes de las herramientas utilizadas en nuestro Sistema
- Realizar respectivas pruebas para verificar el correcto funcionamiento del mismo.

Esquema (Mapa Conceptual)


Diseño de Interfaz grafica
Diseño de Base de Datos
Diagrama de Componentes
Diagrama de Secuencias
Casos de Uso
Especificación de los módulos a desarrollarse
Objetivo del Sistema
Justificación
Planteamiento del problema
1) Análisis de requerimientos del Sistema
2) Diseño y Modelado del Sistema
Desarrollo del Sistema
4) Pruebas de Funcionamiento
3) Implementación
Plataforma Base
Descripción
Herramientas de monitoreo
Infraestructura
Descripción
Herramientas de Almacenamiento (Base de Datos) a utilizar
Descripción
Características
Componentes de Gestión
Herramientas de Gestión para el Servicio de Correo Electrónico a utilizar
Descripción
Características
Funcionamiento
Lenguajes para Programación Web a utilizar
Características

DESARROLLO DEL SISTEMA

Introducción

A llegado la hora de definir nuestro Sistema de Monitoreo, es por ello que a continuación se evalúan todos los puntos necesarios para su desarrollo, pondremos en práctica los estudios realizados en los anteriores capítulos con la finalidad de cumplir con lo previsto dentro del alcance planteado y evaluado en éste capítulo.

4.1 Análisis de Requerimientos del Sistema

4.1.1 Planteamiento del Problema

El monitoreo de tráfico de Internet en la mediana y pequeña empresa requiere de herramientas de fácil gestión y bajo costo, que permitan obtener información útil y detallada acerca las aplicaciones que se ejecutan dentro de la Internet para de ésta manera gestionar eficazmente su red.

4.1.2 Justificación:

Las herramientas de monitoreo de tráfico de Internet analizadas en su mayoría no cuentan con la suficiente documentación, los procesos de instalación, configuración y administración se realizan por separado mediante la manipulación de distintos archivos repartidos en el Sistema Operativo, a esto se le suma lo tedioso y complejo que puede llegar a ser la configuración de los mismos. Por otra parte gran cantidad de ellas se basa en SNMP lo limita el análisis del tráfico

El costo que representa una herramienta de éste tipo mediante la adquisición de dispositivos especializados resulta demasiado elevado al tratarse de una empresa en crecimiento a la cual se enfoca nuestro proyecto.

Además el estudio nos ayudó a conocer que existen otras soluciones que dan soporte en el área de monitoreo del tráfico de Internet por aplicación; sin embargo presentan como principal inconveniente su costo ya que son privativas y las que no, requieren un conocimiento avanzado tanto del protocolo Netflow, como de gestión de redes para su configuración.

Son todos los inconvenientes citados los que dieron origen al desarrollo de éste "Sistema de Monitoreo" que esperamos concluya exitosamente.

Alcance:

Para nuestro proyecto hemos visto la necesidad de crear un sistema que integre los procesos tanto de instalación, configuración y gestión basado en una distribución GNU-Linux.

Para la consecución y elaboración del mismo nos basaremos en herramientas libres que trabajen con la estructura que utiliza el protocolo Netflow debido a que permite obtener mayor información para el análisis del tráfico de Internet, por ende se descartan herramientas aplicadas sobre el protocolo SNMP que analiza el tráfico de una manera más general.

Para la administración del Sistema se implementará un entorno vía web que resulte amigable hacia el usuario, adjunto al Sistema se planea la elaboración de un portal en línea que contenga los enlaces de descarga tanto del sistema de monitoreo, como su respectiva documentación, además de una imagen ISO que incluya un demo del sistema funcionando.

4.1.3 Objetivos del Sistema.

General:

Implementar un sistema de libre distribución, para monitorizar el tráfico de Internet por aplicación, que sea de fácil instalación, configuración y administración.

Específicos:

- Analizar las posibles topologías en la que es factible utilizar el sistema de monitoreo.
- Buscar herramientas que permitan generar flujo Netflow para el análisis del tráfico de Internet por Aplicación.
- Estudiar programas multiplataforma que faciliten el desarrollo del Sistema web.
- Hacer que el sistema sea amigable para el usuario, siendo de fácil instalación, configuración y administración.
- Permitir la generación de reportes pertenecientes a un tiempo determinado.
- Plantear un problema real para el cual funcionara nuestro demo.
- Crear un demo que permita observar el funcionamiento del sistema mediante la implementación de un Live DVD sobre el sistema operativo Debian.

4.2 Diseño y Modelado Del Sistema

Introducción:

Con la finalidad de representar de una manera clara lo que se pretende lograr con el desarrollo del sistema, se procederá a la especificación de cada uno de los módulos mediante la elaboración del los respectivos diagramas y prototipo de interfaz web que interactuará directamente con el usuario.

Entre los diagramas que intervendrán para el diseño y modelado de nuestro proyecto están:

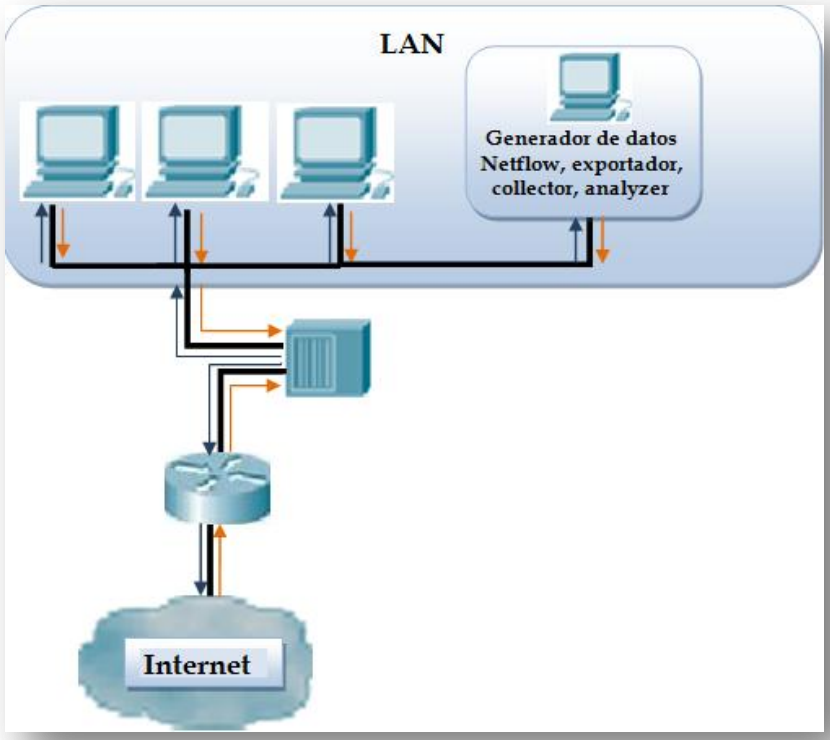
- **Diagramas de Casos de Uso:** Permitirán describir el comportamiento de nuestro sistema con los usuarios y otros sistemas.
- **Diagrama de Secuencias:** Requerido para representar la comunicación entre los objetos a través del tiempo, en un escenario presentado en los casos de uso.
- **Diagramas de Componentes:** Para representar cada uno de los componentes de nuestro sistema y sus dependencias.
- **Diagramas de Base de Datos:** Para especificar la información necesaria para nuestro trabajo y que es preciso almacenar.

4.2.1.1.1 Descripción de Topología de Red a utilizarse

Para que nuestro sistema funcione correctamente nos basamos en dos topologías:

Topología 1

Grafica 4.1. Topología 1



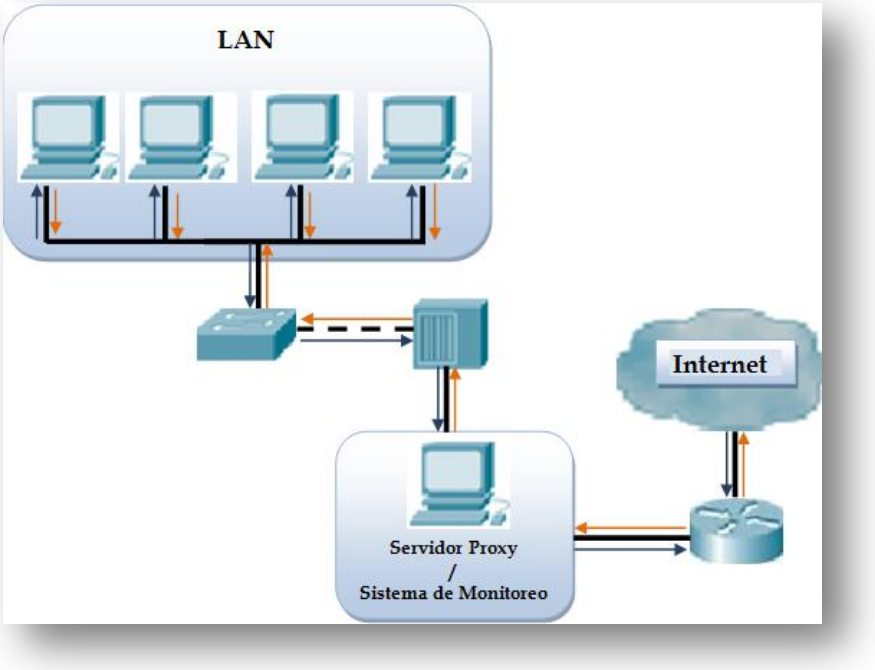
A continuación enumeraremos los elementos que intervienen en esta topología con una breve explicación de la función que cumplen:

- **Protocolo.-** Dependiendo del soporte que disponga el dispositivo que emite los datos de red que van a ser analizados y procesados en lo posterior en este caso es NetFlow
- **Estación de Administración.-** En éste equipo va a estar ejecutándose el sistema de monitoreo, que incluye los componentes: Exportador, Colector y Analizador
- **Nodo.-** Son cada uno de los terminales que realizan peticiones hacia Internet.
- **HUB.-** Al ser un repetidor multipuerto**,** este dispositivo permitirá que el tráfico que pasa por el Router sea escuchado por el equipo de administración que contiene el sistema.
- **Router.-** Es el dispositivo que permitirá el acceso a internet por parte de los nodos.

- **Internet.**

Topología 2

Grafica 4.2. Topología 2



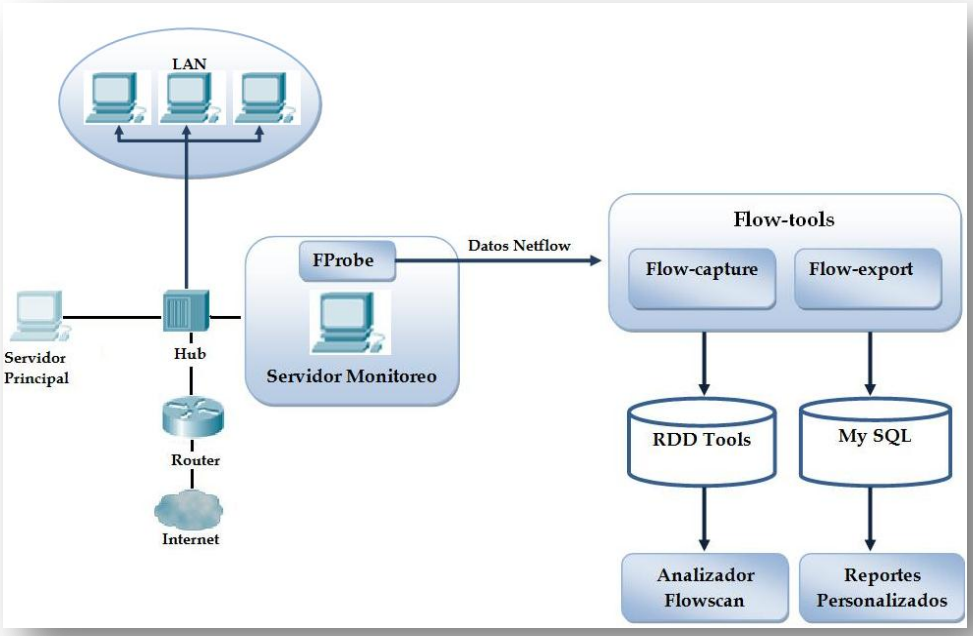
- **Proxy.-** Es un servidor que permite que los demás ordenadores tengan acceso al Internet por medio de él, este tiene una única dirección IP que sale hacia la Internet.
- **Switch.-** es un dispositivo de interconexión de redes que trabaja a nivel de la capa 2, el mismo que pasa los datos de acuerdo con la dirección MAC.
- **Hub.**
- **LAN.-** Red de Área Local Una LAN, permite conectar a varios ordenadores dentro de un área pequeña, estos pueden tener diferentes topologías.
- **Internet.**

Además este sistemas puede ser instalado desde una maquina virtual que tenga conexión a Internet, pero que cumpla una de las dos topologías anteriormente mencionadas.

4.2.2 Arquitectura del Sistema:

Nuestro sistema de Monitoreo se basa en la arquitectura que se muestra a continuación:

Grafica 4.3. Arquitectura del Sistema



El FProbe es una sonda que captura todo el flujo de datos que ingresa por una interfaz determinada.

Para procesar los datos se utiliza la herramienta **Flow-capture** en la que colocamos el tiempo y la versión del paquete NetFlow, en base a estas especificaciones generará archivos que serán almacenados dentro del disco.

Por otra parte para herramienta **flow-export** permitirá almacenar los flujos que se encuentran dentro del disco en una base de datos MySQL con lo que se procederá a realizar los respectivos reportes personalizados.

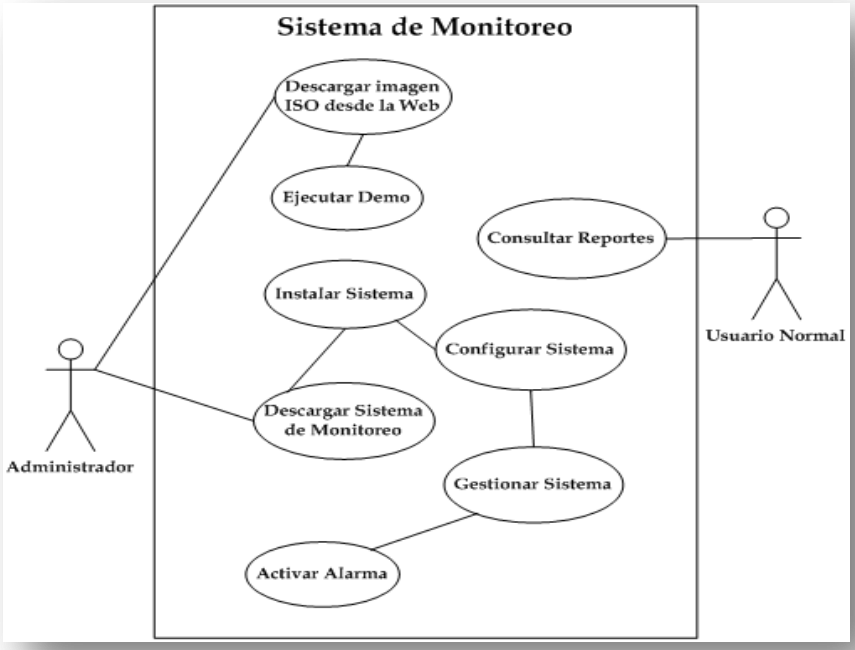
4.2.3 Especificación de Módulos a desarrollar

A continuación se presenta un caso de uso general del Sistema frente a un usuario administrador y uno normal que son los dos tipos de usuarios identificados para el manejo de nuestro proyecto.

El Administrador será el responsable de todo el Sistema de Monitoreo por ende de la configuración de todos y cada uno de los módulos que lo conforman, incluyendo el de poder crear nuevos usuarios, el segundo tipo de usuario denominado Usuario Normal será creado por el Administrador con permisos simplemente al módulo de Gestión del Sistema y a puntos específicos del mismo como por ejemplo la consulta de Reportes.

De aquí partiremos para en lo posterior analizar a detalle los entornos y comportamientos durante la ejecución de cada módulo respectivamente.

Caso de Uso:

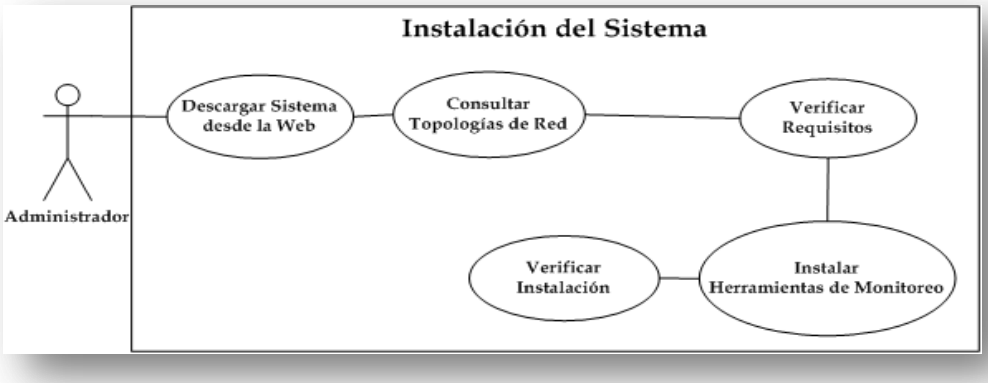


1. **Módulo de Descarga del Software de Monitoreo de Red:** Consta de la construcción de un sitio web que presente la documentación del Sistema de Monitoreo, así como las opciones de descarga del Software, la misma que puede darse de dos maneras: descarga de la Imagen ISO que incluirá el demo del Sistema y la descarga del Sistema de Monitoreo en sí para su instalación.

   Caso de Uso:

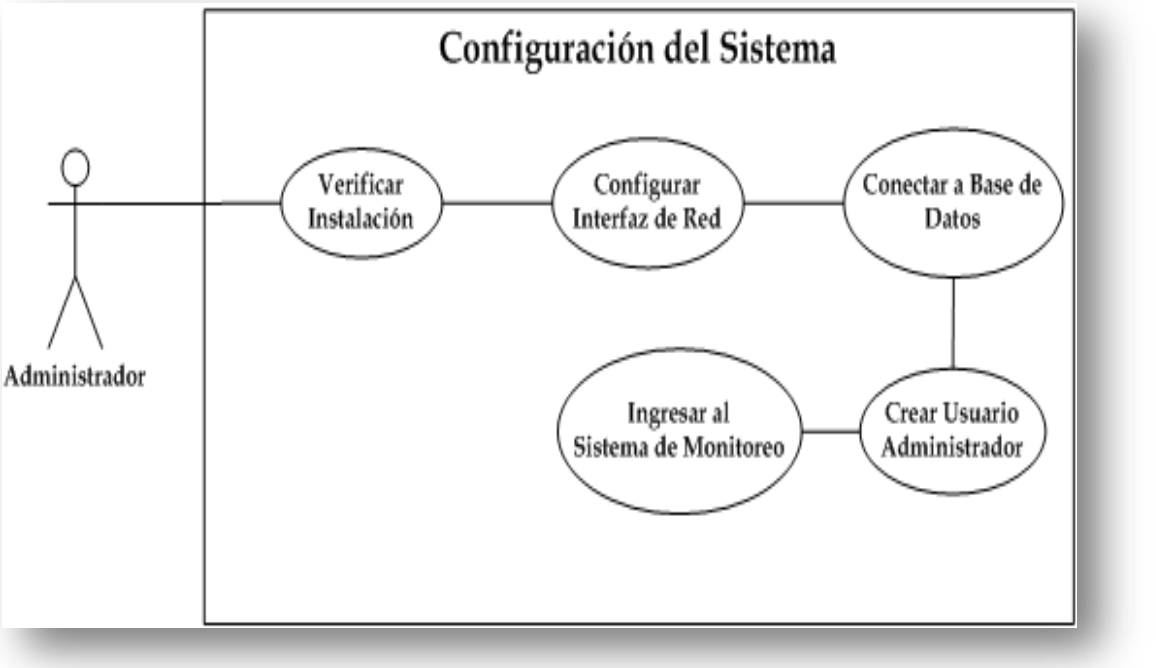
2. **Módulo de Instalación:** Este módulo será el encargado de realizar la verificación de requisitos previos para el funcionamiento de nuestro Sistema, así como la instalación de las debidas herramientas de monitoreo para que finalmente la instalación de nuestro software sea exitoso.

   Caso de Uso:



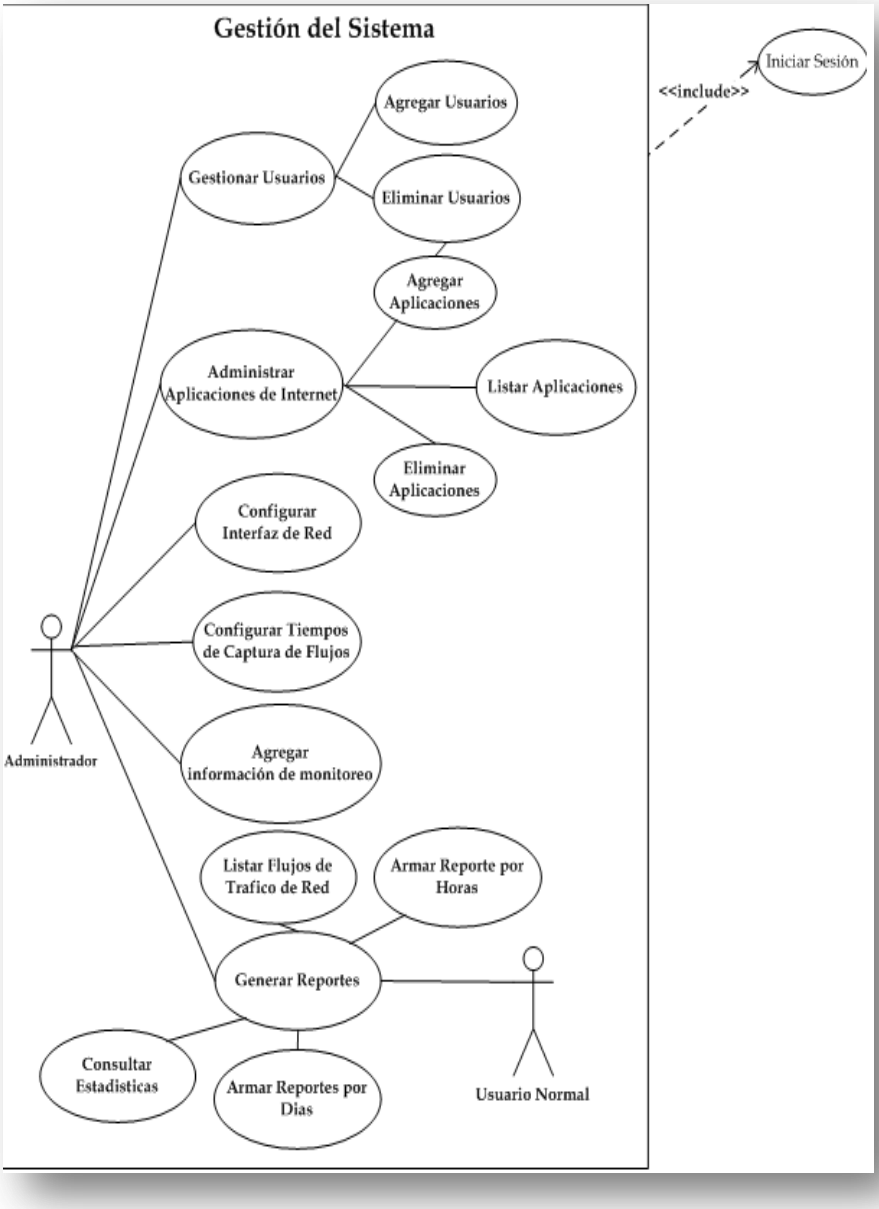
3. **Módulo de Configuración:** Registrará las configuraciones previas al funcionamiento del Sistema, lo que incluye una verificación de la instalación correcta de las Herramientas de Monitoreo, identificación de interfaz de red por la que se desea capturar el tráfico, creación de Base de Datos que almacene los flujos de tráfico generados de Internet, creación de usuario administrador para finalmente ingresar al modulo de gestión de nuestro Sistema.

Caso de Uso:



4. **Módulo de Gestión del Sistema:** Permite la administración del Sistema para lo cual incluye componentes para la creación y listado de usuarios, creación, listado y eliminación de aplicaciones, registro de interfaz de red, tiempos de captura de tráfico, elección de protocolos y direcciones IP a monitorizar además de la generación de reportes de varios tipos.

Caso de Uso:

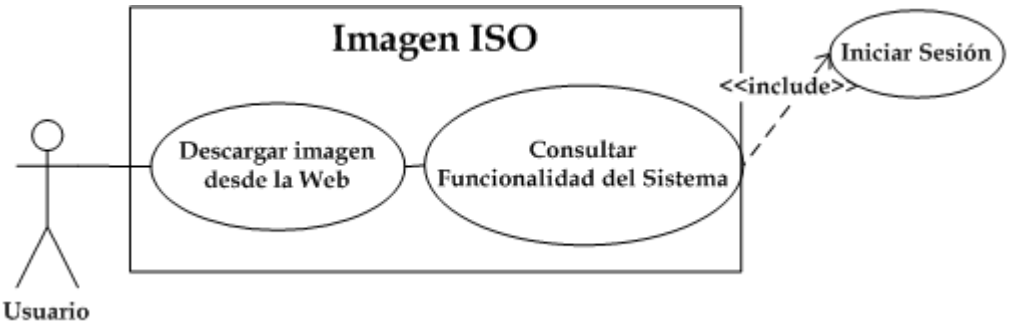


5. **Módulo de Alarmas:** Permite consultar requisitos y configuraciones necesarias del servidor de correo electrónico para activar la alarma. Una vez activada se encarga de enviar un reporte al correo electrónico del administrador de red con información acerca usuario que más ancho de banda a consumido a lo largo de la jornada de trabajo.

   Caso de Uso:

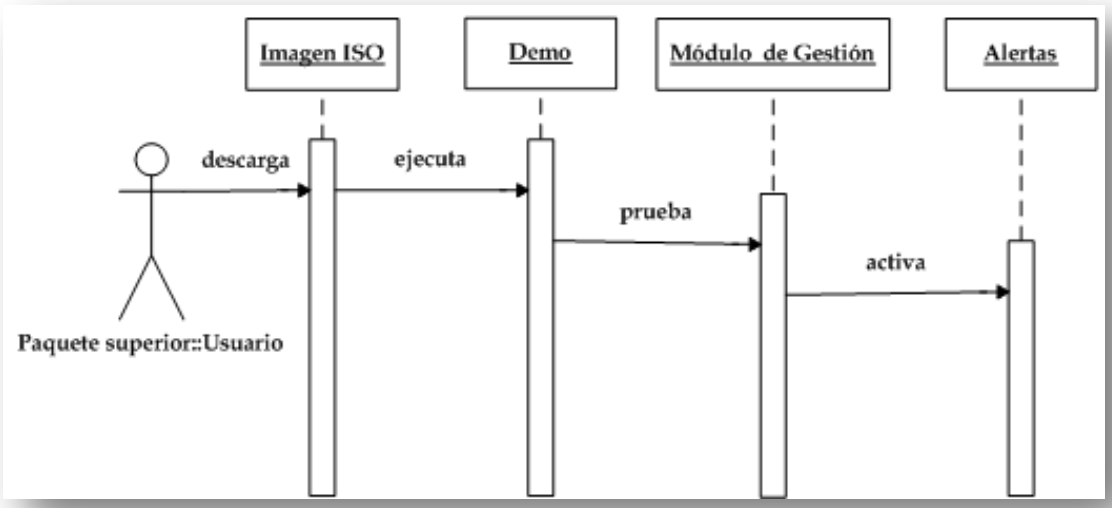
6. **Módulo de Creación de Imagen ISO:** Brinda al usuario la oportunidad de probar el Sistema de Monitoreo sin previa instalación ni configuración del mismo, puesto que incluye un demo con todos los prerrequisitos para su funcionamiento.

   Caso de Uso:

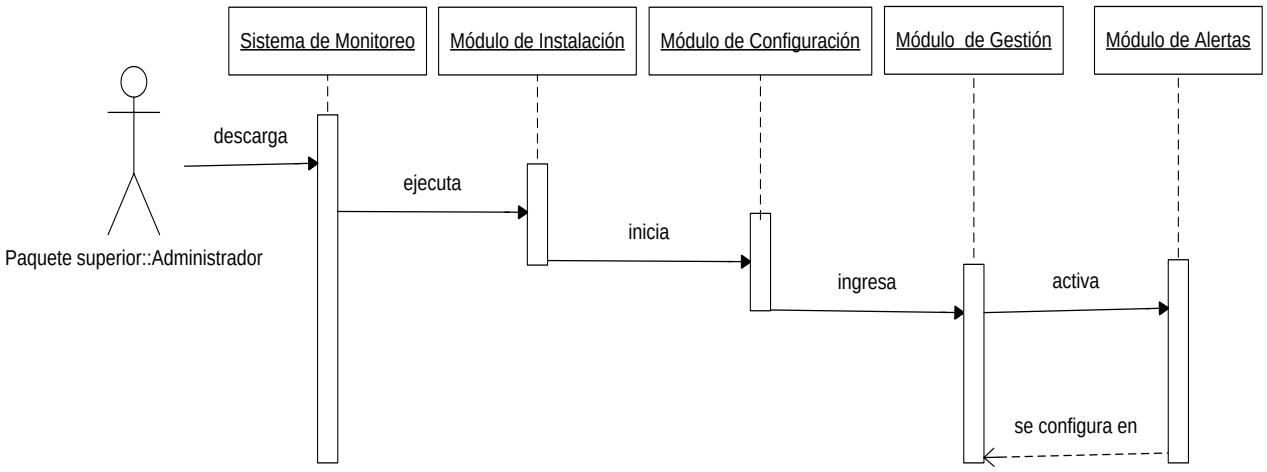


4.2.4 Diagramas de Secuencia.

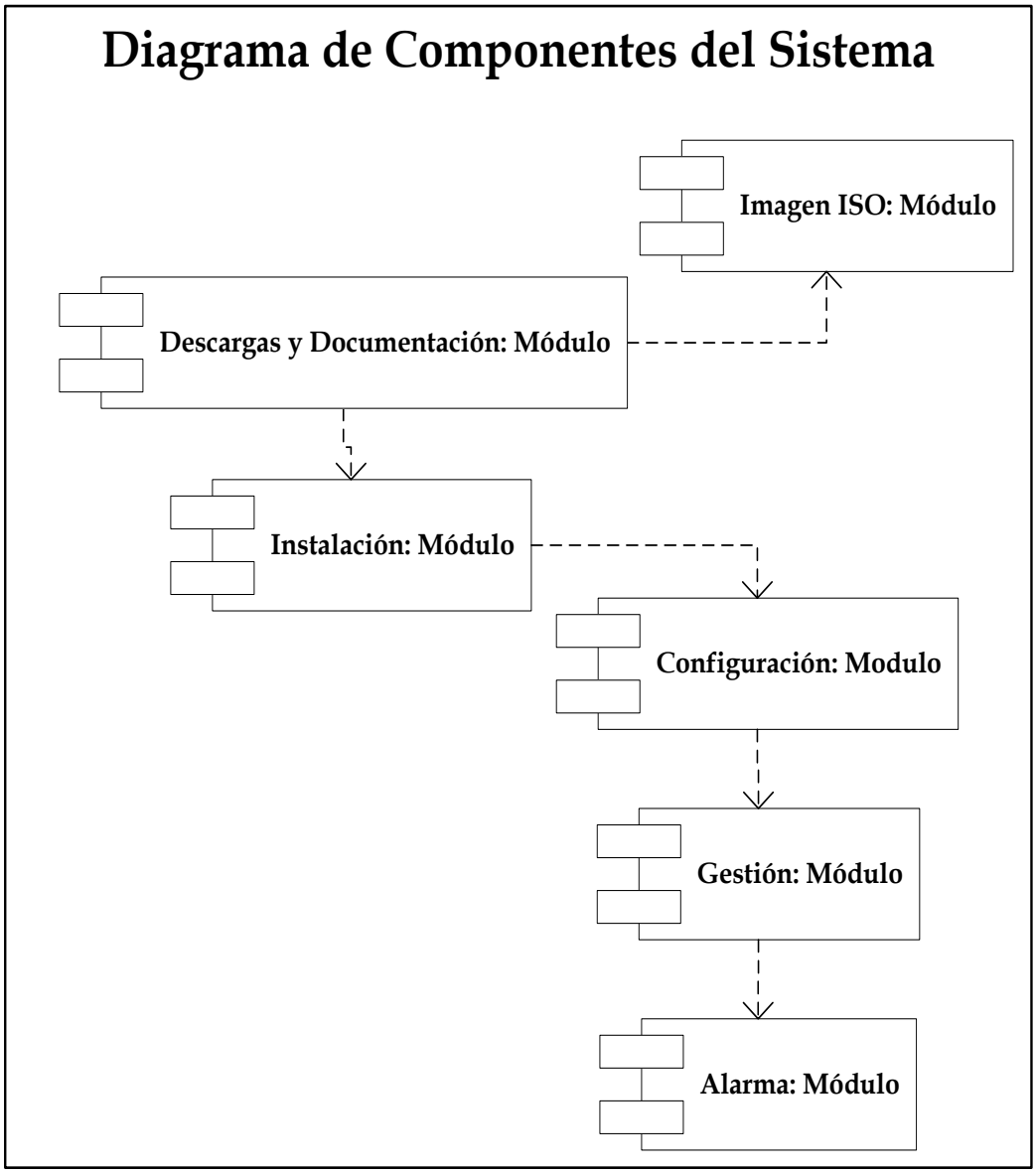
Demo:



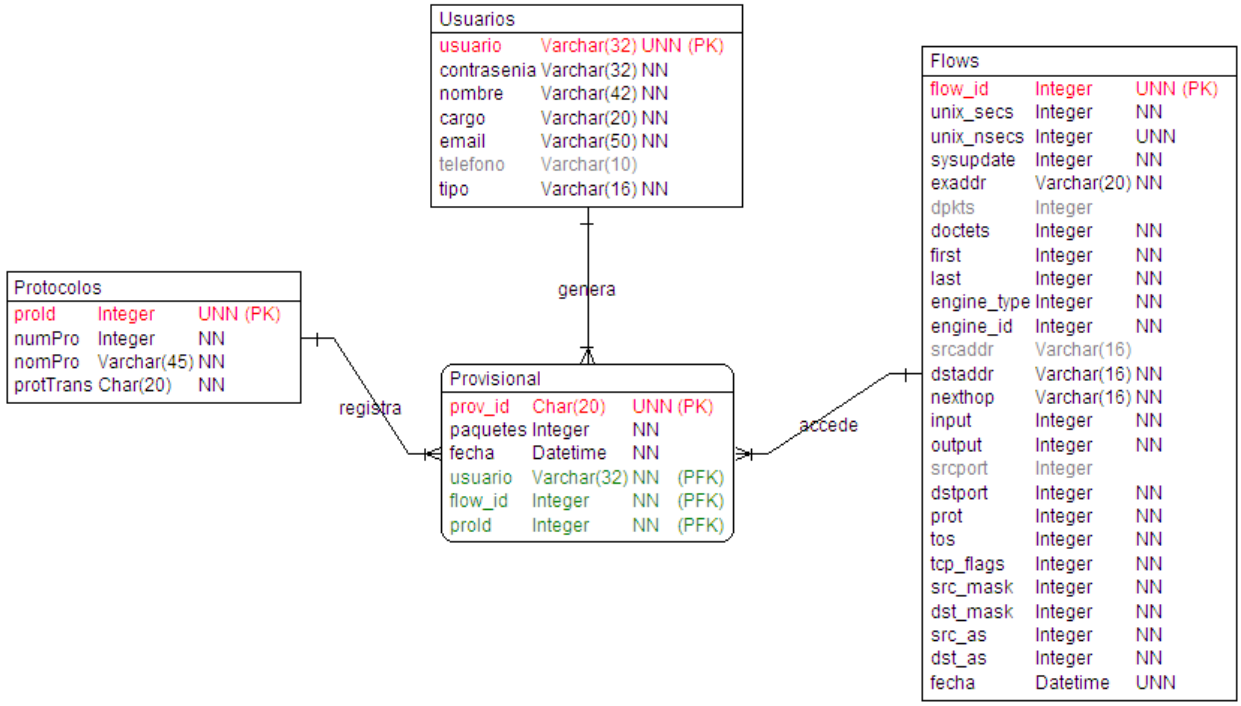
Sistema de Monitoreo:



4.2.5 Diagrama de Componentes:

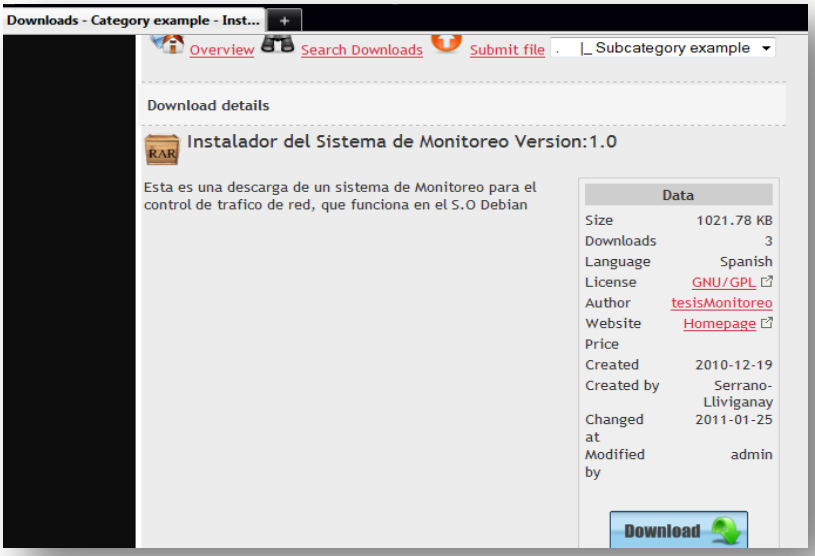


4.2.6 Diagrama Base de Datos (Entidad – Relación)

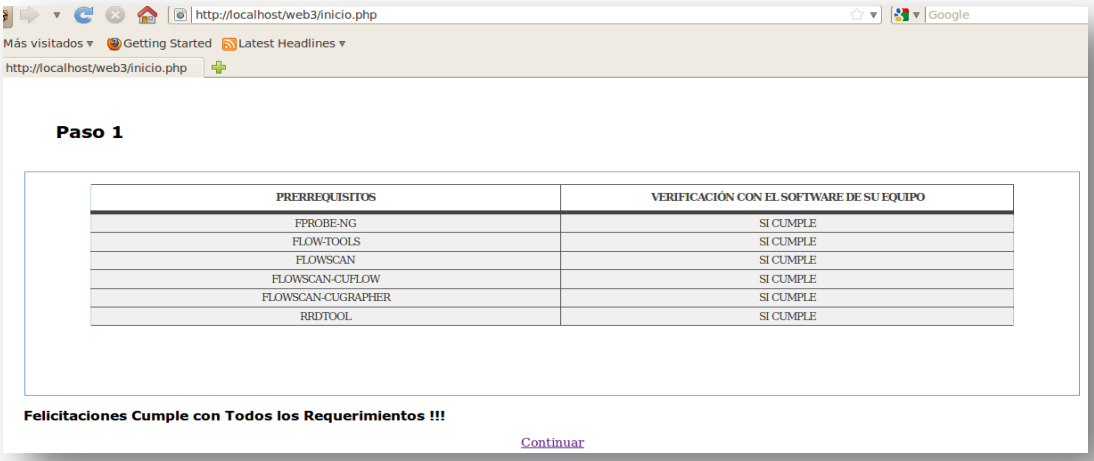


4.2.7 Diseño de Interfaces de Usuario.

Página de Descargas y Documentación



Página de Verificación de Requerimientos

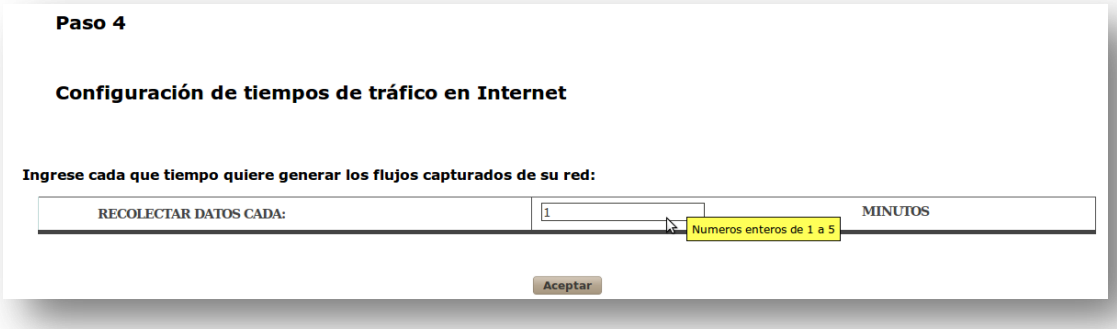


Página de Creación de Usuario Administrador

Página de Inicio al Sistema.

Pagina de Creación de Aplicaciones de Internet

Página de Configuración de Tiempos de Captura.



Página de Reportes por Horas

4.3 Descripción de Herramientas de Monitoreo:

Para la utilización de estas herramientas nos basamos en que se trabajara con flujos de datos Netflow versión 5, así como se definió los tiempos de muestreo y la interfaz por la que escuchara dichos flujos.

Fprobe

Es una herramienta que recoge datos del tráfico de red y lo emite como flujos Netflow hacia un colector especificado.[28]

Flow-capture

Recibe y almacena las exportaciones del flujo NetFlow en el disco. Los archivos del flujo son guardados en directorios de trabajo y pueden ser almacenados en niveles adicionales del directorio como por ejemplo nuestra estará almacenada dentro de */var/lib/pqnetflow/*.

[28] http://fprobe.sourceforge.net/

Los archives activos creados por el flow-capture comienzan con **tmp.** Los archivos que ya están completos comienzan con **ft**.[29]

Flow-tools

Es una colección de programas que se utilizan para recoger, transmitir, procesar y generar informes a partir de los datos Netflow. Esta cuenta con un API para el desarrollo de aplicaciones personalizada en las versiones 1, 5, 6 de Netflow.[30]

Flow-export

Exporta Flujos de archivos flow-tools a otros formatos. Actualmente soporta formatos ASCII y cflowd. La salida ASCII se puede utilizar con Perl u otros lenguajes script. [31]

4.3.2 Herramientas de Almacenamiento

Para el desarrollo de la presente tesis hemos optado por trabajar con la Base de Datos:

My SQL

Descripción:

Es un sistema de gestión de base de datos relacional multihilo y multiusuario.[32]

Características:

- Posee licencia GNU GPL para utilizarlo en desarrollos no comerciales
- Es multiplataforma trabaja en Linux, Windows, PHP y Joomla.

[29] http://linux.die.net/man/1/flow-capture
[30] http://www.splintered.net/sw/flow-tools/docs/flow-tools.html
[31] http://www.sanog.org/resources/sanog6/gaurab-sanog6-flow-tools.pdf
[32] http://es.wikipedia.org/wiki/MySQL

- Es utilizado en aplicaciones Web.

Componentes de Gestión:

Nuestro sistema utilizo esta herramienta para:

- Creación de la base de datos y tablas a partir de un script.
- Creación de la tabla usuarios del Sistema e inserción de los mismos.
- Control de ingreso al Sistema mediante el manejo de Sesiones
- Creación e inserción de la tabla flows, la misma que contiene los flujos Netflow.
- Exportación de los flujos Netflow mediante la utilización de la instrucción flow-export
- Creación e inserción de la tabla serviciosCU la misma que corresponde a los puertos de las aplicaciones que utilizaron los usuarios monitorizados.
- Creación y eliminación de una tabla Provisional que contendrá los paquetes consumidos por diversos puertos pertenecientes aun periodo de tiempo determinado.
- Permite exportar la tabla provisional a una archivo .csv
- Se pueden realizar consultas a las diferentes tablas requeridas por el sistema
- Obtener reportes personalizados por el usuario.
- Se gestiona fácilmente desde lenguajes como PHP y Joomla para desarrollo de páginas web.

4.3.3 Herramientas de Gestión para el Servicio de Correo

Postfix

Descripción:

Es un Agente de Transporte de Correo (MTA) de software libre / código abierto, un programa informático para el enrutamiento y envío de correo electrónico.[33]

Características:

- Es una alternativa rápida, fácil de administrar y segura.34
- Trabaja en distribuciones Linux.
- Es de fácil implementación
- Se trabajara con una cuenta Gmail para el envío de los mails.

Funcionamiento:

Nuestro sistema contará con postfix para el envío de un correo electrónico con los reportes del usuario que mayor consumo realizo durante el día, el envío se lo realizara a una hora determinada (5 de la tarde).

4.3.4 Lenguajes de programación Web a utilizar

PHP

Descripción:

Es un lenguaje de programación interpretado y diseñado originalmente para la creación de páginas web dinámicas[35].

[33] http://es.wikipedia.org/wiki/Postfix

[34] http://es.wikipedia.org/wiki/Postfix

[35] http://es.wikipedia.org/wiki/PHP

Características:

- ¬ Es un lenguaje multiplataforma (Window-Linux).
- ¬ Soporte para mysql
- ¬ Soporte para scripts .sh (Linux)

Funcionamiento:

- ¬ Nuestro sistema se baso en dicho programa para la creación del entorno web.
- ¬ Manejo de hojas de estilo
- ¬ Lectura y Escritura de Archivos
- ¬ Muestra de reportes gráficos mediante la implementación de paquetes adicionales como lo es PChart
- ¬ Exportación de flujos
- ¬ Fusión con código JavaScript para recoger y validar datos de formularios HTML.
- ¬ Manejo de Ajax.
- ¬ Manejo de sesiones para el ingreso del usuario al Sistema

JOOMLA

Descripción:

Es un sistema de gestión de contenidos, y entre sus principales virtudes está la de permitir editar el contenido de un sitio web de manera sencilla. Es una aplicación de código abierto programada mayoritariamente en PHP bajo una licencia GPL. Este administrador de contenidos puede trabajar en Internet o

intranets y requiere de una base de datos MySQL, así como, preferiblemente, de un servidor HTTP Apache[36].

Características:

- Mejorar el rendimiento web
- Versiones imprimibles de páginas[37]
- Creación de artículos
- Subida y descargada de archivos

Funcionamiento:

- Contendrá un enlace para descargar el Sistema de Monitoreo y Manuales del Sistema
- Contiene información sobre requerimientos, instalación, configuración y administración

4.3.5 Plataforma Base a utilizar

Distribución Debian Lenny 5.0

Descripción:

Es un sistema operativo libre que tiene un conjunto de programas básicos y utilidades que permiten el funcionamiento de una computadora. Debian utiliza

[36] http://es.wikipedia.org/wiki/Joomla!

[37] http://es.wikipedia.org/wiki/Joomla!

el núcleo Linux (el corazón del sistema operativo), pero la mayor parte de las herramientas básicas vienen del Proyecto GNU; de ahí el nombre GNU/Linux[38].

Características:

- Cuenta con una página de soporte y descargas
- La disponibilidad en varias arquitecturas. (i386, amd64, PowerPC, etc.).
- Una amplia colección de software disponible. La versión 5.0 viene con más de ≈ 23.000 paquetes.
- Un grupo de herramientas para facilitar el proceso de instalación y actualización del software (APT, Aptitude, Dpkg, Synaptic, Dselect, etc.) Todas ellas obtienen información de donde descargar software desde /etc/apt/sources.list, que contiene los repositorios.
- No tiene marcado ningún entorno gráfico en especial, puediéndose no instalar ninguno, o instalar, ya sean: GNOME, KDE, Xfce, LXDE, Enlightenment u otro.[39]

Funcionamiento:

Se escogió esta distribución por las siguientes consideraciones:

- Es considerado uno de los S.O. más estables
- Posee mayor documentación para esta distribución.
- Existe un mayor soporte en paquetes y sus dependencias.

[38] http://www.debian.org/index.es.html

[39] http://es.wikipedia.org/wiki/Debian_GNU/Linux

- Trabaja con paquetes estables (por ejemplo trabaja con Php 5.2 que no tiene problemas de compatibilidad con la librería pChart como en Php5.3)

4.4 Pruebas de Funcionamiento.

Para el desarrollo de este punto hemos visto la necesidad de seguir un formato que permita documentar los resultados de las pruebas realizadas a lo largo de la implementación de nuestro proyecto, dicho formato se basa en el documento que se presenta en la tesis "Estudio de las Metodologías de desarrollo de Software Libre y su aplicación en un caso práctico". (Andrés Argudo,William Astudillo, 2010).

SISTEMA DE MONITOREO DE RED

DOCUMENTO DE PRUEBAS DEL SISTEMA

Fecha de elaboración: 19 Diciembre del 2010

Responsables: Eugenia Llivigañay, Verónica Serrano.

Versión: 1.0

1. Definición de la misión de las Pruebas

Verificar que el funcionamiento de cada uno de los módulos descritos en el proyecto "Sistema de Monitoreo de Tráfico de Red", se cumpla a cabalidad con la aplicación oportuna de pruebas que representen entornos reales en los que actuará el sistema, con el objetivo de detectar posibles falencias, controlarlas y eliminarlas.

2. Evaluación del Sistema

Ejecutar el sistema una vez que se ha comprobado el módulo de instalación.

Descripción: Se procederá a poner a prueba el script de instalación del sistema con los requisitos previos a la instalación completos para verificar la instalación adecuada de las herramientas de monitoreo.

Resultado Obtenido: El sistema verificó los requisitos del equipo e instalo las herramientas de monitoreo satisfactoriamente.

```
tesis:/var/www/instaladorComandos# sh ejecuta.sh
Des:1 http://http.us.debian.org lenny Release.gpg [1033B]
Des:2 http://http.us.debian.org lenny/main Translation-es [562kB]
Des:3 http://backports.debian.org lenny-backports Release.gpg [835B]
Ign http://backports.debian.org lenny-backports/main Translation-es
Des:4 http://ftp.us.debian.org stable Release.gpg [1033B]
Des:5 http://ftp.us.debian.org stable/main Translation-es [562kB]
Ign http://www.geekconnection.org debian/ Release.gpg
Ign http://www.geekconnection.org debian/ Translation-es
Des:6 http://security.debian.org lenny/updates Release.gpg [835B]
Ign http://security.debian.org lenny/updates/main Translation-es
Ign http://security.debian.org lenny/updates/contrib Translation-es
Ign http://backports.debian.org lenny-backports/contrib Translation-es
Ign http://backports.debian.org lenny-backports/non-free Translation-es
Des:7 http://backports.debian.org lenny-backports Release [74,3kB]
Ign http://www.geekconnection.org debian/ Release
Des:8 http://security.debian.org stable/updates Release.gpg [835B]
Ign http://security.debian.org stable/updates/main Translation-es
Ign http://security.debian.org stable/updates/contrib Translation-es
Ign http://security.debian.org stable/updates/non-free Translation-es
Des:9 http://security.debian.org lenny/updates Release [40,8kB]
6% [9 Release 1187/40,8kB 2%] [Esperando las cabeceras] [2 Translation-es 25700
```

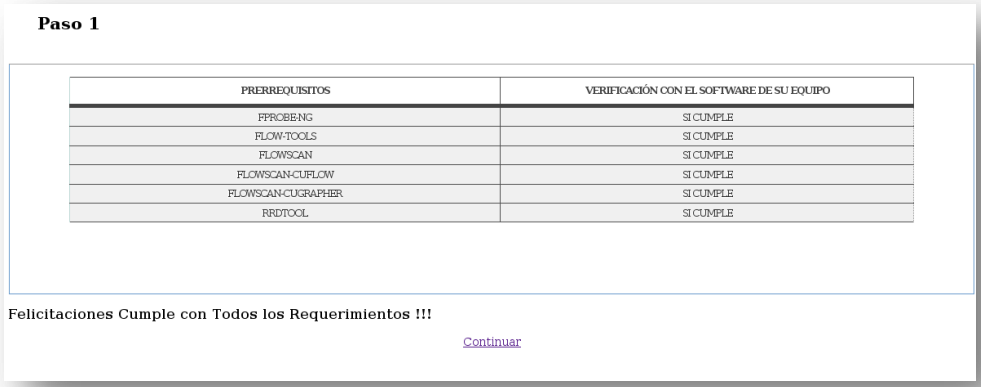
Resultado Esperado: El sistema debe presentar el resultado de las verificaciones de los requisitos y de cumplirlos instalar las herramientas de monitorización con un mensaje de aviso de verificación de instalación correcta.

Estado de la prueba: Superada

Ejecutar el Sistema a partir del módulo de instalación sin cumplir con los requisitos previos al script de instalación.
Descripción: En esta prueba se procederá a modificar los requisitos previos de manera que el equipo no cumpla con alguno de ellos.
Resultado Obtenido: El sistema verifico de manera correcta el incumplimiento de requisitos.
Resultado Esperado: El sistema no continuar ejecutándose mostrando la falta de requisitos para la instalación de las herramientas de monitoreo.
Estado de la prueba: Superada

Verificar la instalación de las Herramientas de Monitorización posterior a su instalación.
Descripción: Se comprobará que la instalación de las herramientas de monitoreo hayan sido registradas de manera correcta por el equipo.
Resultado Obtenido: El sistema presenta la página de verificación con todas las herramientas debidamente instaladas.

Resultado Esperado: El sistema debe permitir continuar con el módulo de configuración una vez superada la verificación.



Estado de la prueba: Superada

Módulo Configuración: Conexión a la Base de Datos como administrador.

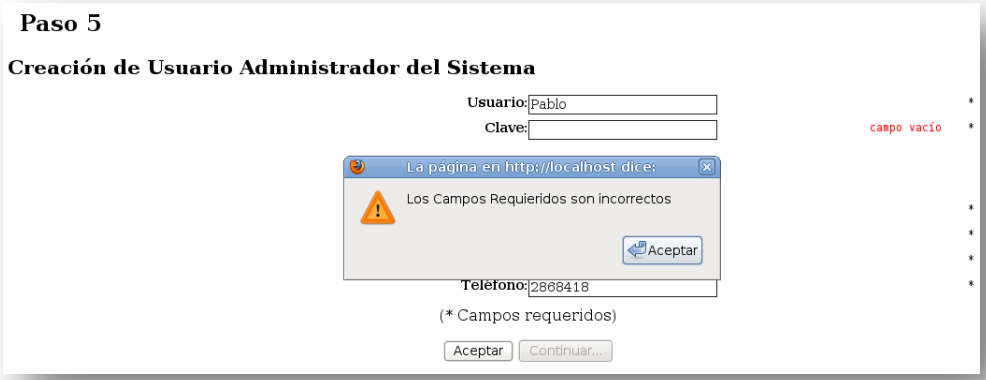
Descripción: Se procederá a tratar de continuar con el proceso de configuración mediante el ingreso erróneo de los datos de conexión a la base de datos.

Resultado Obtenido: Presenta un mensaje de conexión Errónea al Servidor y la posibilidad de reintentar

Resultado Esperado: El usuario no debe poder continuar con el proceso de configuración del sistema.
Estado de la prueba: Superada

Módulo de Configuración: Validación de formulario para la creación del usuario administrador.
Descripción: Se intentará acceder mediante la digitalización errónea de los datos solicitados en el formulario de creación del usuario.

Resultado Obtenido: El sistema muestra mensajes de validación de cada uno de los campos registrados de manera incorrecta y no permite la grabación de información de este usuario.



Resultado Esperado: El usuario no debe poder registrarse hasta que ingrese de manera correcta cada uno de los campos solicitados.

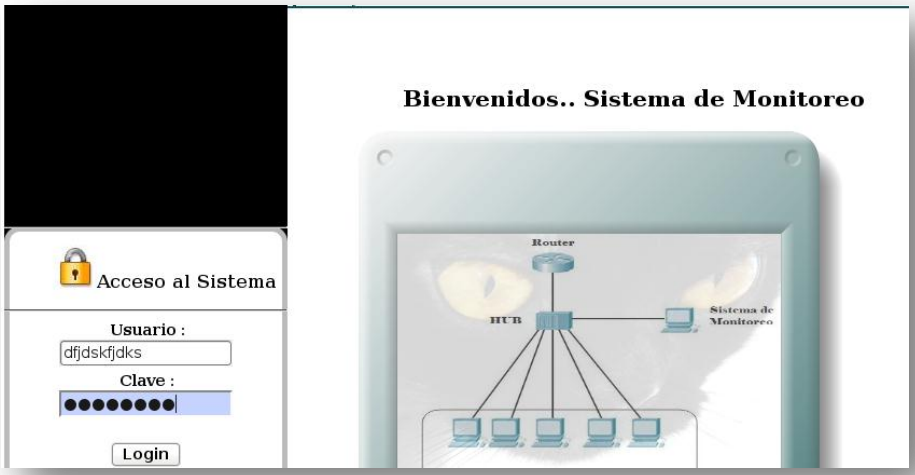
Estado de la prueba: Superada

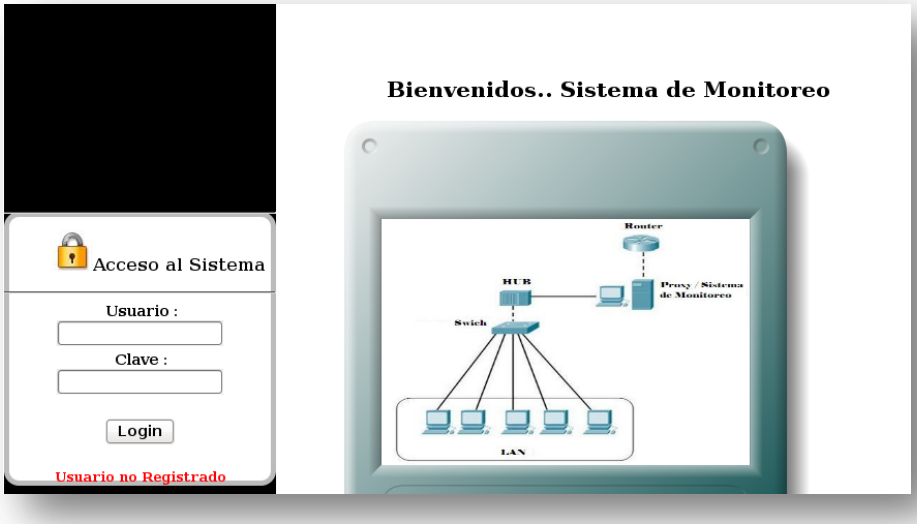
Módulo de Gestión: Autentificar el inicio de sesión al Sistema de Gestión de Monitoreo para un usuario no registrado en la Base de Datos.

Descripción: Se comprobará el comportamiento del sistema al tratar ingresar

al módulo de gestión con un usuario y clave erróneos.

Resultado Obtenido: El sistema presenta un mensaje de usuario no registrado y no permite el acceso al módulo de gestión no presentó el contenido de la pagina redirigiendo al usuario a la página de autentificación.

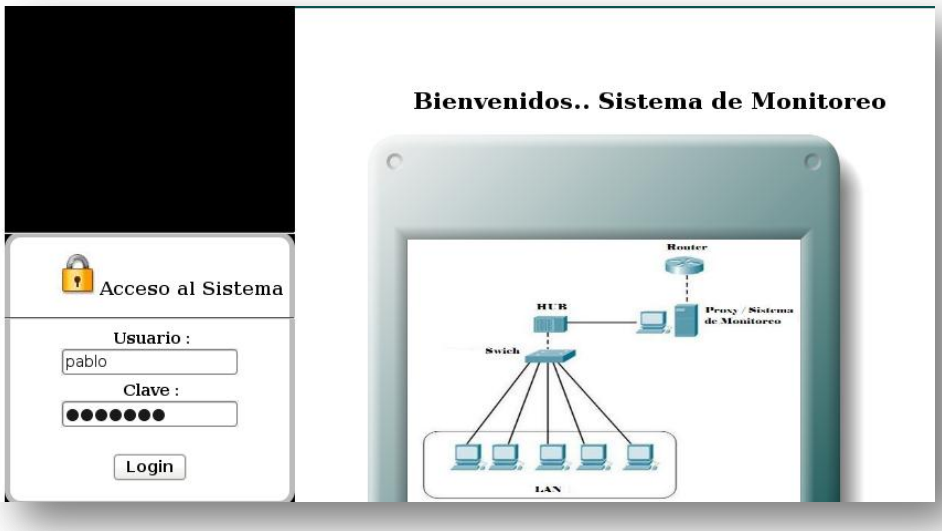




Resultado Esperado: El usuario debe ingresar datos de usuario y clave correctos.

Estado de la prueba: Superada

Invocar a una de las páginas de gestión sin iniciar sesión.
Descripción: Se comprobará el comportamiento del sistema al tratar de acceder directamente a los módulos y clases de la aplicación sin antes autenticarse.
Resultado Obtenido: El sistema no presentó el contenido de la pagina redirigiendo al usuario a la página de autentificación.
Resultado Esperado: El usuario no debe tener acceso al contenido de la página obligándolo a autentificarse.

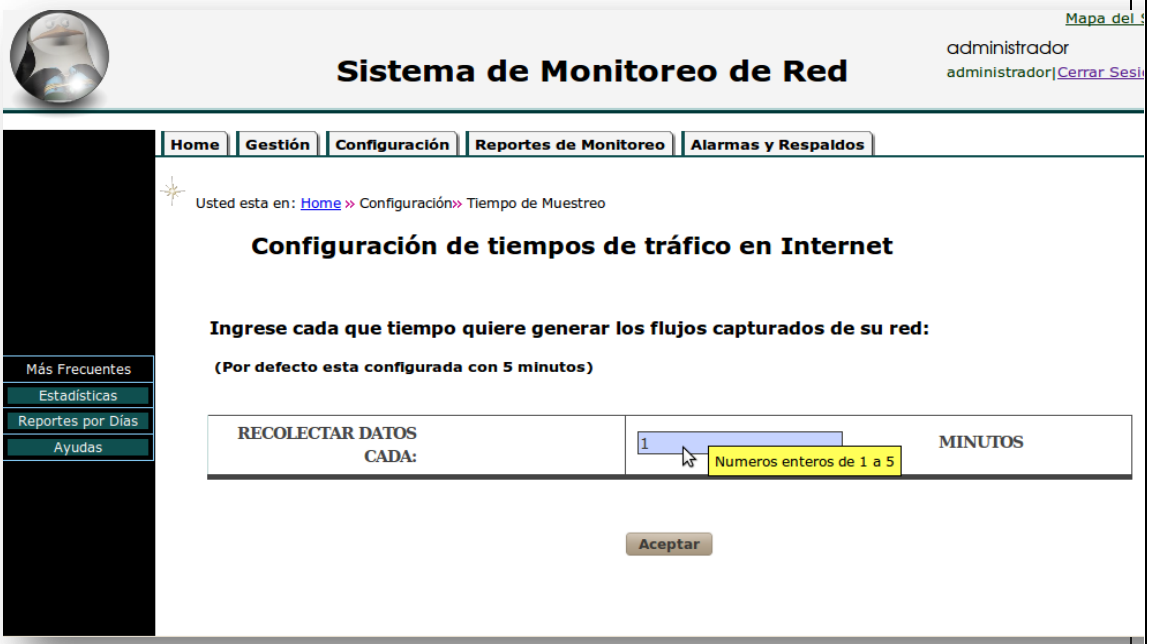


Estado de la prueba: Superada

Validar que en el ingreso de números puertos del Ingreso de Aplicaciones de Internet se permitan solo números

Descripción: La prueba consiste en ingresar caracteres que no sean números al campo de ingreso de aplicaciones de internet.

Resultado Obtenido: El sistema no responde cuando se digitan caracteres diferentes de los números.



Resultado Esperado: El campo del número de puerto la aplicación debe permitir solo el ingreso de números.

Estado de la prueba: Superada

Validar que el campo de ingreso de Tiempos de Captura de Tráfico permita valores dentro del rango especificado

Descripción: Para esta prueba se procedió a ingresar el tiempo de captura de tráfico en un rango mayor a 5 minutos.

Resultado Obtenido: Muestra un mensaje de tiempo no permitido y no permite continuar.

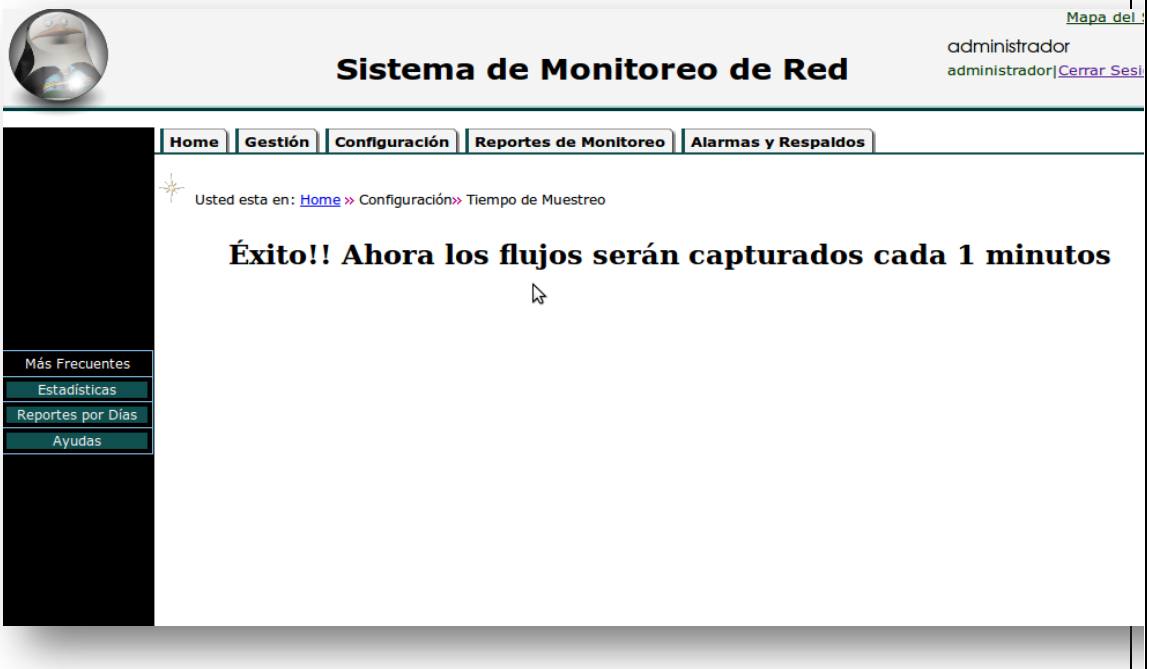
Resultado Esperado: El sistema debe mostrar mensaje de error y no permitir guardar los cambios.

Estado de la prueba: Superada.

Validar que los Tiempos de Captura de Tráfico hayan sido cambiados satisfactoriamente.

Descripción: Para esta prueba se procedió a ingresar el tiempo de captura de tráfico en un rango de 1 a 5 minutos para verificar que los archivos de configuración necesarios han sido cambiados.

Resultado Obtenido: Se muestra una mensaje de cambio de tiempos de captura exitoso pero al verificar los archivos de configuración han sido reemplazados con el tiempo ingresado de manera incorrecta:



Resultado Esperado: El sistema debe mostrar mensaje exitoso y realizar el debido reemplazo de valores en los archivos de configuración.

Estado de la prueba: Superada

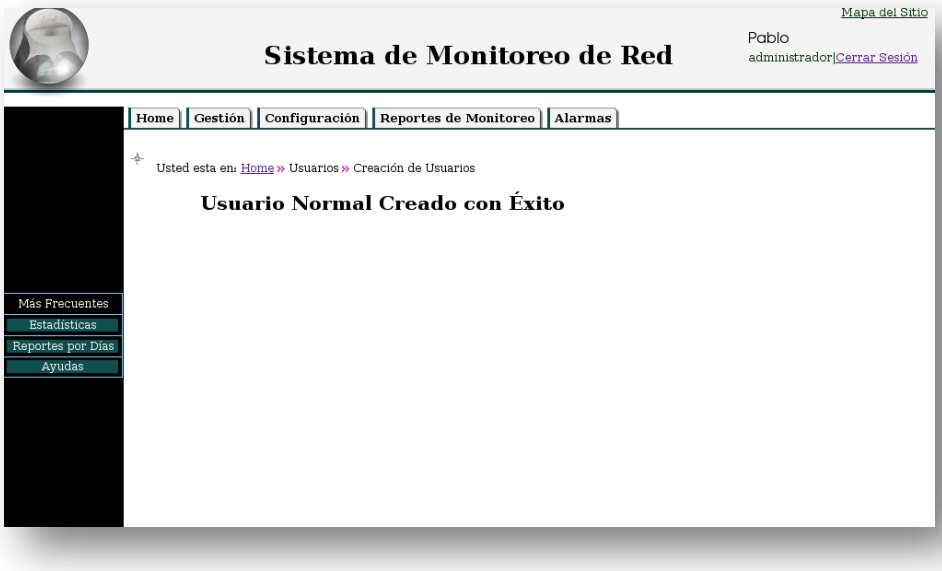
Observaciones: Hicimos un nuevo método que reemplace de manera correcta el tiempo

en todos los archivos de configuración requeridos.

Módulo de Configuración: Validar que los usuarios hayan sido agregados de manera correcta.

Descripción: La prueba consiste en agregar un usuario desde el módulo de agregación de usuarios.

Resultado Obtenido: Se tiene un mensaje de aviso de usuario creado con éxito.



Resultado Esperado: El sistema registra el nuevo usuario.

Estado de la prueba: Superada

Módulo de Configuración: Verificar que las aplicaciones hayan sido eliminadas de manera correcta.

Descripción: La prueba consiste en eliminar una de las aplicaciones de Internet que hayan sido agregadas.

Resultado Obtenido: Se tiene un mensaje de aviso de aplicación eliminada exitosamente.

Resultado Esperado: El sistema debe eliminar de la base de datos la aplicación especificada por el usuario.

Estado de la prueba: Superada

Módulo de Configuración: Validación de Reportes

Descripción: En esta prueba se procedió a realizar un reporte con una selección de datos que no produzcan ningún tipo de información.

Resultado Obtenido: El sistema presenta un mensaje sin resultados de los reportes.

Resultado Esperado: El sistema no debe presentar ningún reporte y dar aviso que la consulta no contiene la información necesaria.

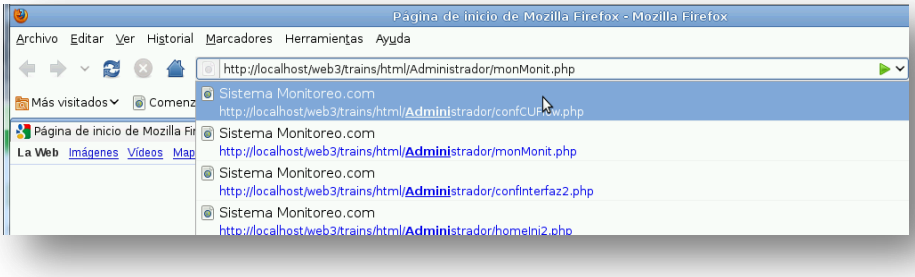
Estado de la prueba: Superada

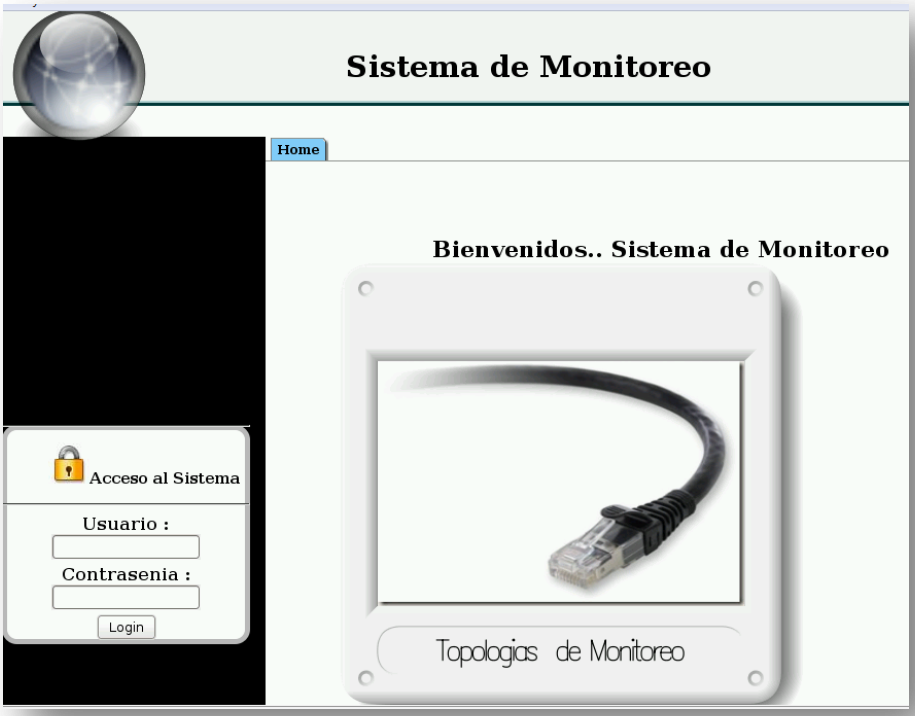
Invocar a una de las páginas de gestión sin iniciar sesión.

Descripción: Se comprobará el comportamiento del sistema al tratar de acceder directamente a los módulos y clases de la aplicación sin antes autenticarse.

Resultado Obtenido: El sistema no presentó el contenido de la pagina redirigiendo al usuario a la página de autentificación.

Resultado Esperado: El usuario no debe tener acceso al contenido de la página obligándolo a autentificarse.





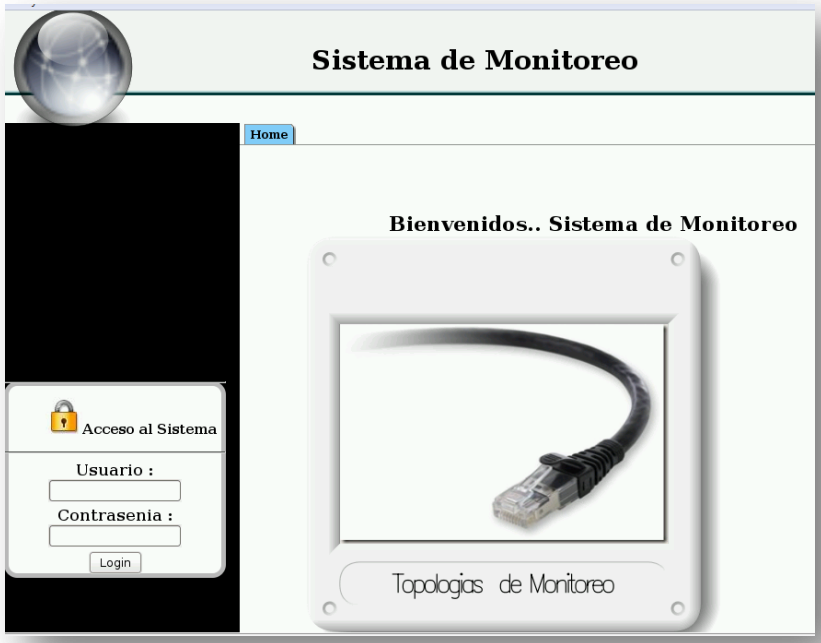
Estado de la prueba: Superada

Configurar Módulo de Activación de Alarmas.

Descripción: Se comprobará que una vez configuradas y aprobadas las pruebas de prerrequisitos de activación de alarma llegue un mensaje de correo electrónico al administrador del Sistema con un informe del usuario que mas ancho de banda a consumido.

Resultado Obtenido: El sistema presenta el mensaje de alarma activada y al revisar el correo se recibe un correo con la siguiente información:

Resultado Esperado: El usuario no debe tener acceso al contenido de la página obligándolo a autentificarse.



Estado de la prueba: Superada

Módulo Imagen ISO: Ejecutar Demo automáticamente
Descripción: Se comprobará el comportamiento del la imagen generada al iniciar al sistema Debian.
Resultado Obtenido: Una vez ejecutada la imagen desde la unidad de DvD el sistema presento automáticamente el navegador web con el sistema de monitoreo precargado.
Resultado Esperado: Al ejecutarse la imagen del sistema ISO salta automáticamente el navegador firefox con el demo cargado.
Estado de la prueba: Superada

Conclusión del Capítulo

Durante el desarrollo de éste capítulo se ha tratado de cumplir con las especificaciones denotadas en el alcance, es por ello que en la implementación del Sistema nos hemos basado en los respectivos diagramas y diseños elaborados antes de comenzar, aunque claro siempre hay detalles que no logran ser cubiertos en su totalidad.

CAPÍTULO 5

Objetivos:

Objetivo General:

¬ Crear una Imagen .ISO empleando una Distribución GNU-Linux

Objetivos Específicos:

- ¬ Establecer una distribución base en la cual va a funcionar nuestro sistema de monitoreo
- ¬ Analizar las diferentes herramientas que nos permitirán crear una Imagen ISO para nuestra distribución Debian.
- ¬ Crear una imagen .ISO de nuestro Sistema que funcionara como demo.

DESARROLLO DE IMAGEN CON DISTRIBUCIÓN GNU-LINUX

Introducción

El presente capítulo ha sido creado con la finalidad de determinar las razones y características fundamentales para la creación de nuestra imagen .ISO.

Además se realizara un manual de usuarios en el que se explicara paso a paso el manejo del sistema con el objetivo de que el usuario comprenda el manejo del mismo.

5.1 Establecer la distribución base a utilizar.

La distribución base a utilizar para la creación de nuestra Imagen ISO es la última versión estable de Debían hasta la fecha: "Debian Lenny 5.0 ", para procesadores i386 que es el más común entre los equipos que disponemos, se lo puede descargar directamente desde la página web http://www.es.debian.org/CD/torrent-cd/.

El motivo de ésta elección es que todo nuestro sistema de monitoreo fue desarrollado en esta versión, precisamente por las características que posee frente a otras distribuciones GNU/LINUX las mismas que fueron evaluadas en un punto anterior de este mismo documento. Además, al ser nuestra imagen ISO la que contenga el demo del Sistema de Monitoreo hemos decidido utilizar la distribución gráfica de Debían de modo que se lo pueda presentar ejecutándose desde la misma máquina.

5.2 Herramientas de Creación de Imagen ISO.

Para la creación de la imagen se presentaron varias opciones entre las que tenemos:

Live-helper

Descripción:

Es una herramienta de creación de Live CD Debian, se trata de un cd estándar similar a los instaladores que permite arrancar un ordenador pero a diferencia de los instaladores su finalidad es dar una utilización totalmente funcional al ordenador sin necesidad de tocar en absoluto la configuración original del sistema instalado en el ordenador.[40]

Características:

- Detecta la mayoría del hardware del ordenador.
- Permite la personalización del Live CD mediante la agregación de software
- Al modificar las opciones de arranque de Grub, se puede escoger si se arranca desde el Live CD o del instalador.

Funcionamiento:

Al realizar las pruebas para obtener un Live-CD , notamos que este tiene un problema de incompatibilidad con la distribución Debian Lenny en la cual hemos venido desarrollando nuestro sistema.

Reconstructor

Definición:

Es una herramienta que permite personalizar y crear una distribución GNU-Linux de Ubuntu y Debian.[41]

Características:

La personalización del sistema incluye:

[40] http://www.esdebian.org/wiki/live-helper

[41] https://projects.lumentica.com/projects/reconstructor/wiki

- Arranque del logotipo de la imagen, fondos de escritorio, aplicaciones, etc.
- Requiere de un navegador moderno (Firefox, Chrome, etc), con Java Script activado. Pero es recomendable si utiliza Internet Explorer.

Funcionamiento:

Al momento de utilizar esta herramienta requiere que usted se registre y cancele un valor de $5 dólares mensuales para su utilización mediante

Para la elaboración de la imagen **iso** de nuestro Live DVD basado en Debian Lenny 5.0 se escogió la siguiente herramienta:

Remastersys

Definición:

Es capaz de realizar copias de seguridad o crear una copia distribuible de un Ubuntu o Debian.

Características:

Funciona con los siguientes paquetes previamente instalados como son: squashfs-módulos para el kernel y módulos o aufs o módulos unionfs.

Funcionamiento:

- Se colocan los repositorios necesarios para remastersys.
- Una vez verificado que se cumplan todos los requerimientos, instalado y configurado el Sistema de monitoreo, se procede a instalar los paquetes squashfs, aufs y unionfs para proseguir con la instalación del remastersys.
- Se realizara una copia respaldo de todo el sistema operativo, con la línea ***Remastersys backup***

- Se obtiene la imagen .iso, un Live-DVD que funcionara como demo para el usuario.

5.3 Customizar la distribución según necesidades del sistema.

Con el fin de obtener los resultados esperados, para la generación de ésta imagen se ha visto la necesidad de realizar las siguientes acciones:

- Desinstalar aplicaciones que no influyan en la ejecución del Sistema de Monitoreo, con el fin de hacer más liviana nuestra distribución.
- Instalar todas las Aplicaciones y Herramientas de Monitoreo que son requisitos para el funcionamiento del proyecto.
- Permitir el ingreso del usuario directamente sin previo inicio de sesión con login y contraseña.
- Elaborar un demo acerca de la funcionalidad del Sistema de Monitoreo y cargarlo a la distribución
- Ejecutar automáticamente el navegador Web con el demo del Sistema de Monitoreo incluido por defecto, inmediatamente después del inicio de debían.

Todas las tareas anteriormente mencionadas han sido consideradas durante la creación de la imagen ISO y de esta manera se ha logrado obtener una distribución personalizada de acuerdo a nuestras necesidades, de un tamaño aproximado de 1GB.

5.4 Elaboración de Demo para la imagen ISO de la Distribución.

Una manera de presentar todas las funcionalidades del sistema al usuario sin que éste tenga que instalar directamente en su equipo es precisamente la elaboración de un demo, el mismo que viene incluido en la imagen ISO y presenta las siguientes características:

- Mensajes de cómo ingresar al sistema, posterior a la fase de verificación de requisitos e instalación de herramientas de monitoreo puesto que en esta imagen ya están incluidos.

- Muestra de manera clara y precisa la topología de red utilizada para la generación de tráfico de Internet.

- Contiene datos reales de flujos de tráfico adquiridos con dicha Topología.

- Permite la evaluación de cada uno de los módulos de gestión del Sistema de manera de ejemplo y con ciertas limitaciones, los mismos que incluyen: gestión de usuarios, aplicaciones de internet, reportes por horas, fechas, estadísticos, etc.

5.5 Asignación de Nombre de la Imagen

La imagen ISO generada a partir de la distribución GNU-Linux Debian que incluye el demo de nuestro proyecto se denominará TesisMonitoreoRed.iso, puesto que consideramos que es un nombre lo suficientemente descriptivo de lo que contiene.

Conclusión del Capítulo:

Se ha obtenido una imagen ISO basada en la distribución GNU-Linux Debian en la que incorporamos el demo de nuestro Sistema de Monitoreo por lo que damos por concluido que se cumplido satisfactoriamente con los objetivos éste el último capítulo de nuestra tesis.

Conclusiones:

El proyecto de Tesis presentado en éste documento nos ha brindado la oportunidad de crear un "Sistema de Monitoreo de Red" , en el que han intervenido un sin número de procesos a lo largo de su implementación, algunos de ellos han representado todo un reto para nosotras puesto que se han llegado a manipular gran cantidad de archivos de configuración del Sistema Operativo que en nuestro caso fue Debian 5.0 en su versión, estable del que podemos decir, fue la mejor decisión que pudimos tomar al momento de inclinarnos hacia una distribución GNU-Linux ya que soportó y superó la mayoría de pruebas a las que fue sometido.

- Debido a la escasa documentación de las herramientas de monitoreo, específicamente las basadas en Software Libre que fueron las utilizadas por obvias razones, nos resultó bastante compleja la etapa de configuración de muchas de ellas e inclusive tuvimos que cambiar constantemente de distribuciones GNU-Linux.

- Nos ha permitido manipular múltiples topologías de red con sus respectivos componentes, las mismas que fueron necesarias para probar la correcta generación de flujos de tráfico de la Internet.

- Se han configurado múltiples servicios de Debian relacionados al campo de redes que han resultado muy útiles tanto dentro del proyecto como fuera de él.

- Si bien muchas de las configuraciones han requerido un tiempo considerable empezando desde la parte investigativa debemos reconocer que han resultado bastante interesantes.

- La culminación del proyecto nos ha tomado más tiempo que el previsto en un inicio, comenzando desde la escasa información pasando por la necesidad que tuvimos de primero instruirnos en un lenguaje de programación que sabemos que toma su tiempo y finalmente los arreglos que siempre generan retrasos.

Afortunadamente, hemos conseguido cumplir con el alcance que nos planteamos al inicio y aunque nos ha resultado extenso estamos conformes ya que ha contribuido en la obtención de nuevos conocimientos en un sin número de configuraciones y métodos de investigación que estamos seguras nos serán de gran ayuda en lo posterior.

Recomendaciones:

Una de las recomendaciones que podemos citar dentro de nuestro proyecto es que antes de utilizar el sistema lea detenidamente la documentación que se presenta en el portal de descarga del mismo y de tener la posibilidad, previa a la instalación ejecutar el demo que a más de adentrarnos en el funcionamiento del Sistema de Monitoreo nos permite evaluar otras características propias del Sistema Operativo.

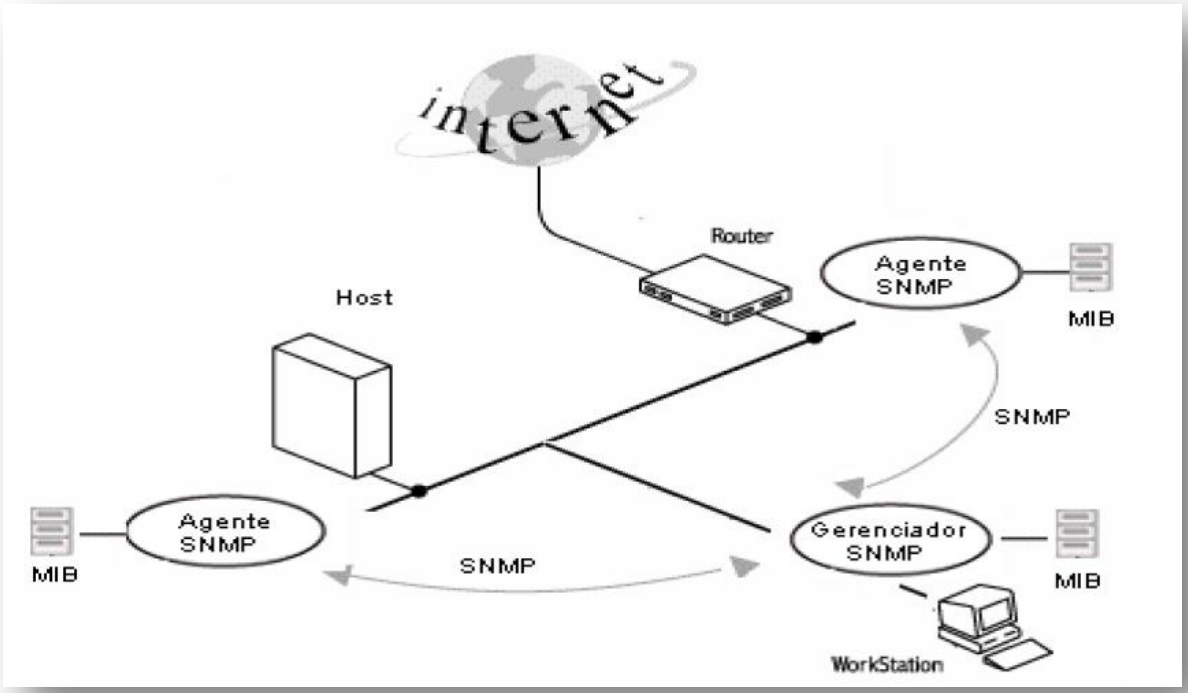
Otra de las recomendaciones guiada especialmente para los generadores de Software Libre es hacernos a la idea que lo libre no tiene que ser complicado ni tampoco serio, puesto que en lo personal preferimos el manejo de interfaces amigables cuando se trata de configuraciones y demás manipulaciones dentro de cualquier aplicación.

La mayor recomendación que podemos brindar por experiencia propia es la utilización de una distribución GNU-Linux "Debian" como Sistema Operativo, y por supuesto aplicaciones basadas en Software Libre pero a más de esto retribuir lo recibido mediante la generación de aplicaciones fieles a ésta filosofía, ya que muchas de las personas nos aprovechamos de éstas aplicaciones simplemente para lucrarnos con ellas y no seguimos su filosofía que se basa en la contribución de conocimientos que aporten a la sociedad. La libertad que se obtiene con manejo del Software Libre es realmente extraordinaria en comparación con el que es que es de carácter propietario privativo, es por ello que impulsamos a la contribución para avance del mismo, esperando que éste proyecto sea la muestra de ello.

ANEXOS

ANEXO 1

MIB: Un Escenario [42]



[42] http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf

ANEXO 2

Rendimiento de Netflow[43]

- Aproximado de Utilización de CPU por números de flujos activos

Números de flujos activos en la cache	Utilización de CPU adicional
10000	< 4%
45000	< 12%
65000	< 16%

- La Reducción significativa de la Utilización del CPU con Netflow se logra mediante:
  - *Sampled Netflow*
  - Optimización de los tiempos
  - Una arquitectura distribuida

- Tener una exportación doble no tiene un impacto relevante en la utilización del CPU

[43] http://www.bibliociencias.cu/gsdl/collect/eventos/index/assoc/HASH010e.dir/doc.pdf

ANEXO 3

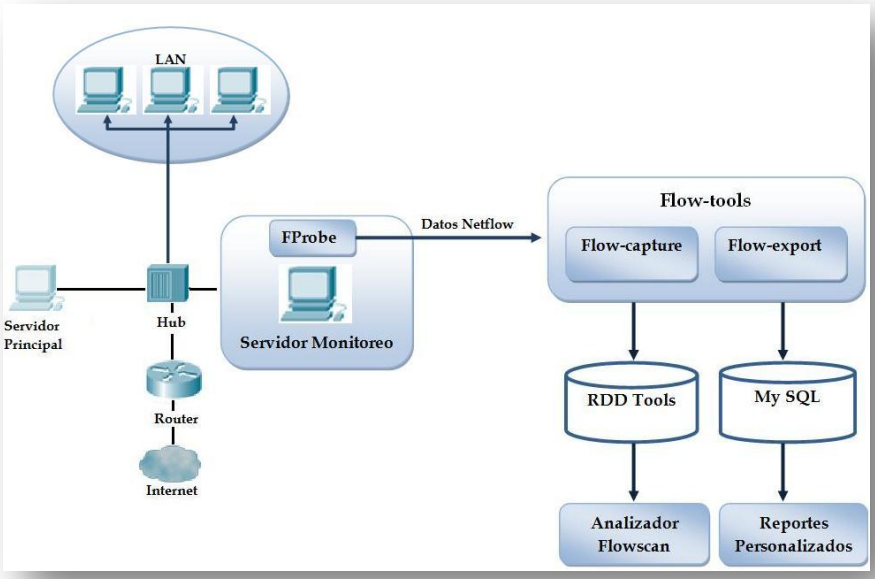
Manual del Usuario

Arquitectura del Sistema:

El FProbe es una sonda que captura todo el flujo de datos que ingresa por una interfaz determinada.

Para procesar los datos se utiliza la herramienta Flow-Capture en el que colocamos el tiempo y la versión del paquete Netflow que va a recibir y lo almacena en archivos dentro del disco.

El Flowscan cuenta con el modulo del CUFlow que permite analizar el trafico de toda la red por aplicaciones, mediante la creación de archivos .rdd, por otra parte para poder realizar los reportes personalizados utilizamos la herramienta Flow-Export que permitirá almacenar los flujos que se encuentran dentro del disco en una base de datos MySQL



Prerrequisitos del Sistema:

1. La plataforma a ser utilizada es Debian Lenny
2. Debe contar con conexión a Internet, para que pueda instalar en línea los paquetes con todas sus dependencias.

3. Para poder instalar los siguientes Prerrequisitos así como los componentes del sistema usted debe añadir los siguientes repositorios a la lista de repositorios así:
   Digite en consola:

```
echo "deb http://security.debian.org/ lenny/updates main contrib" >> /etc/apt/sources.list
echo "deb-src http://security.debian.org/ lenny/updates main contrib" >> /etc/apt/sources.list
echo "deb http://volatile.debian.org/debian-volatile lenny/volatile main contrib" >> /etc/apt/sources.list
echo "deb http://http.us.debian.org/debian/ lenny main contrib" >> /etc/apt/sources.list
echo "deb-src http://http.us.debian.org/debian/ lenny main contrib" >> /etc/apt/sources.list
echo "deb http://http.us.debian.org/debian/ lenny-proposed-updates contrib main" >> /etc/apt/sources.list
echo "deb-src http://http.us.debian.org/debian/ lenny-proposed-updates contrib main" >> /etc/apt/sources.list
echo "deb-src http://volatile.debian.org/debian-volatile lenny/volatile main contrib" >> /etc/apt/sources.list
echo "deb http://ftp.us.debian.org/debian/ stable main contrib non-free" >> /etc/apt/sources.list
echo "deb-src http://ftp.us.debian.org/debian/ stable main contrib non-free" >> /etc/apt/sources.list
echo "deb http://security.debian.org/ stable/updates main contrib non-free" >> /etc/apt/sources.list
echo "deb-src http://security.debian.org/ stable/updates main contrib non-free" >> /etc/apt/sources.list
echo "deb http://backports.debian.org/debian-backports lenny-backports main contrib non-free" >> /etc/apt/sources.list
```

O puede acceder al archivo sources.list digitando:

nano /etc/apt/sources.list

y proceda a ingresar manualmente los repositorios anteriormente mencionados, como por ejemplo:

deb http://security.debian.org/ lenny/updates main contrib

guarde el archivo con **ctrl+o** y cierre con **ctrl+x.**

Prerrequisitos necesarios para el funcionamiento del sistema:

- ✓ Apache2
- ✓ Curl
- ✓ Libapache2-mod-php5
- ✓ Mysql-server

- ✓ Mysql-client
- ✓ Mysql-admin
- ✓ Perl
- ✓ Php5
- ✓ Php5-cgi
- ✓ Php5-cli
- ✓ Php5-common
- ✓ Php5-curl
- ✓ Php5-gd
- ✓ Php5-mysql
- ✓ Sun-java6-jdk
- ✓ Sun-java6-jre
- ✓ Sun-java6-bin

Para instalarlos proceda a digitar en consola lo siguiente:

```
apt-get update
apt-get install apache2 libapache2-mod-php5
apt-get install mysql-server mysql-client mysql-admin
apt-get install perl curl
apt-get install php5 php5-gd php5-cgi php5-curl php5-common
php5-cli php5-mysql
apt-get install sun-java6-jdk sun-java6-jre sun-java6-bin
```

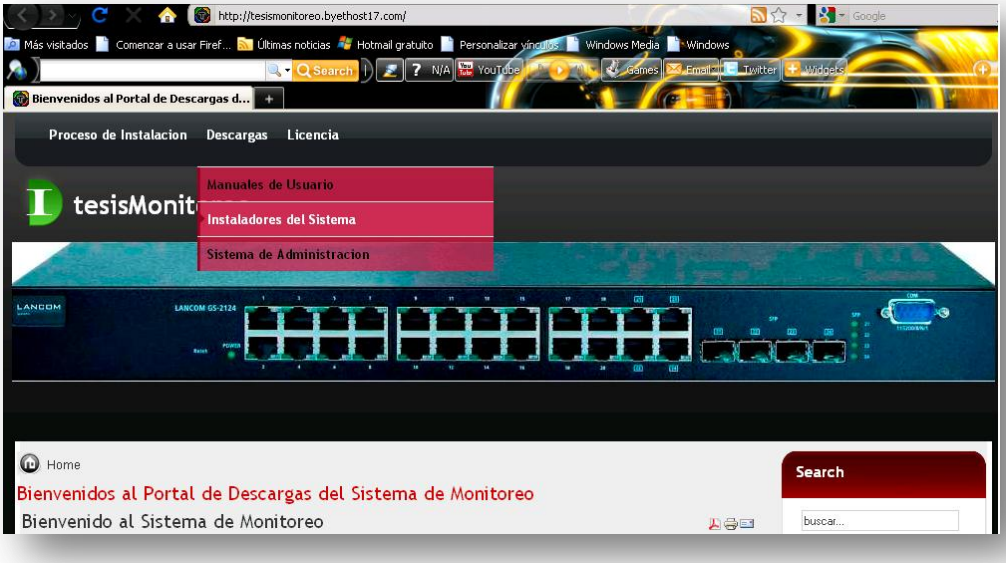
Instalación del Sistema:

Instalación del Sistema:

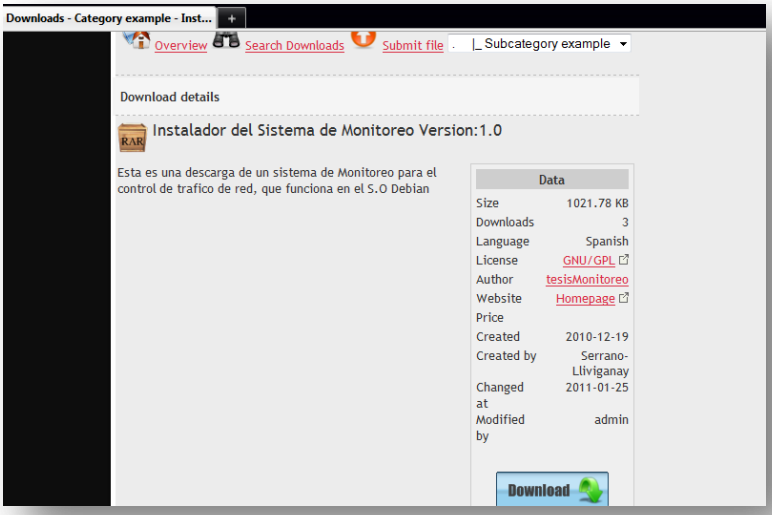
1. Descargue el Instalador desde la pagina:

   http://tesismonitoreo.byethost17.com/

   De clic en Descargas, Instaladores del Sistema.



2. De clic en el enlace Download



3. Con el archivo instaladorComandos.zip se lo descomprime y se lo coloca dentro de su Servidor en la ruta **`/var/www`**.

```
unzip /rutaOrigen/instaladorComandosFinal.zip
```

4. Digite en una terminal:

```
mv /rutaOrigen/instaladorComandos /var/www
```

5. Dentro de un terminal:

- ✓ Digite lo siguiente: **`cd /var/www/instaladorComandos`**
- ✓ Luego coloque: **`sh ejecuta.sh`**

```
tesis:/var/www/instaladorComandos# sh ejecuta.sh
Des:1 http://http.us.debian.org lenny Release.gpg [1033B]
Des:2 http://http.us.debian.org lenny/main Translation-es [562kB]
Des:3 http://backports.debian.org lenny-backports Release.gpg [835B]
Ign http://backports.debian.org lenny-backports/main Translation-es
Des:4 http://ftp.us.debian.org stable Release.gpg [1033B]
Des:5 http://ftp.us.debian.org stable/main Translation-es [562kB]
Ign http://www.geekconnection.org debian/ Release.gpg
Ign http://www.geekconnection.org debian/ Translation-es
Des:6 http://security.debian.org lenny/updates Release.gpg [835B]
Ign http://security.debian.org lenny/updates/main Translation-es
Ign http://security.debian.org lenny/updates/contrib Translation-es
Ign http://backports.debian.org lenny-backports/contrib Translation-es
Ign http://backports.debian.org lenny-backports/non-free Translation-es
Des:7 http://backports.debian.org lenny-backports Release [74,3kB]
Ign http://www.geekconnection.org debian/ Release
Des:8 http://security.debian.org stable/updates Release.gpg [835B]
Ign http://security.debian.org stable/updates/main Translation-es
Ign http://security.debian.org stable/updates/contrib Translation-es
Ign http://security.debian.org stable/updates/non-free Translation-es
Des:9 http://security.debian.org lenny/updates Release [40,8kB]
6% [9 Release 1187/40,8kB 2%] [Esperando las cabeceras] [2 Translation-es 25700
```

✓ Posteriormente coloque: **`sh inano.sh`**

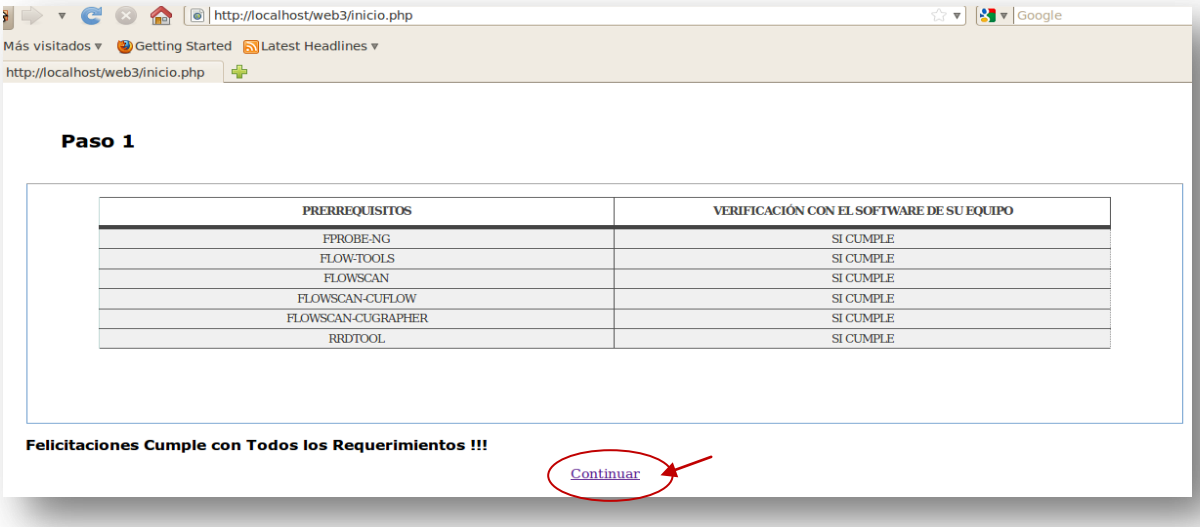
Para la ejecución del archivo ejecuta.sh usted debe tener conexión a Internet para la instalación de los programas.

Configuración del Sistema:

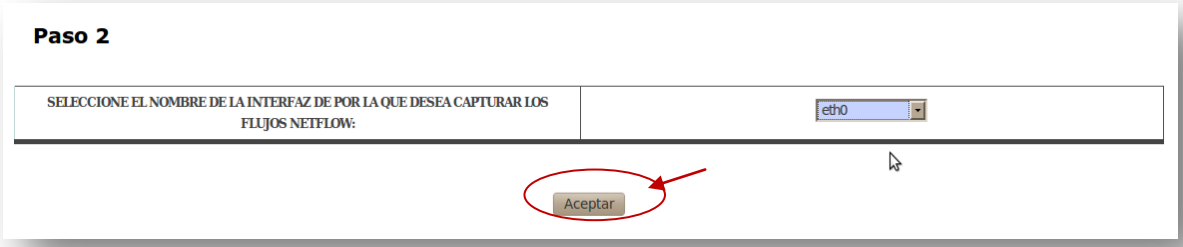
1. Ingrese desde su navegador a la siguiente dirección

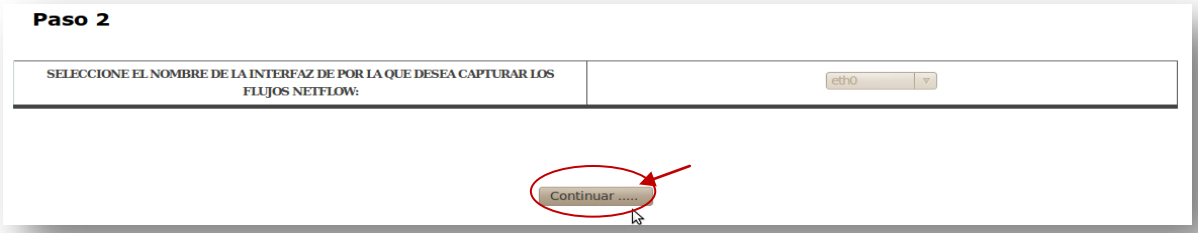
   `http://ipservidor/web3/inicio.php`

   Y presione Continuar.

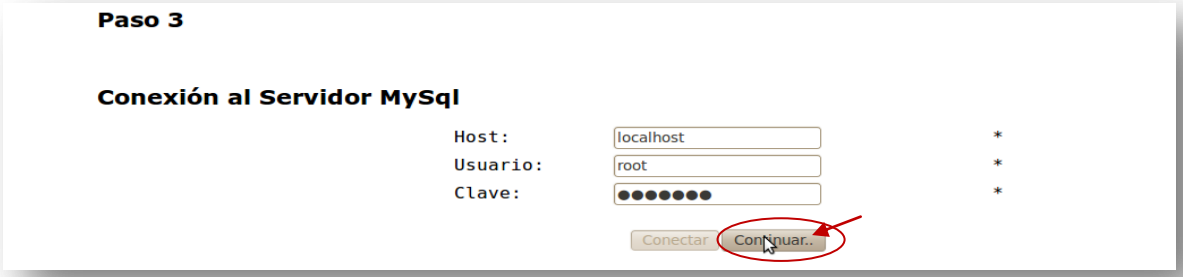


2. Ahora en el paso dos ingrese la interfaz de Red por la que desea escuchar el tráfico de Internet, presione Aceptar y Continuar.

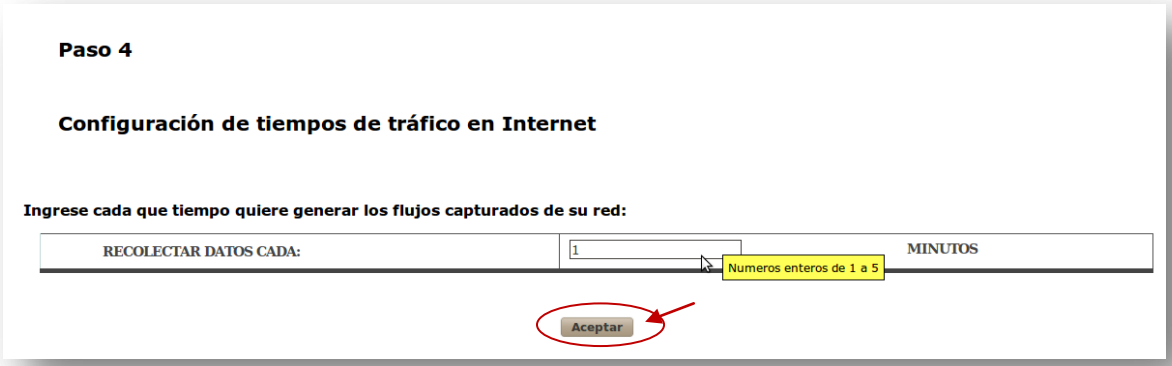


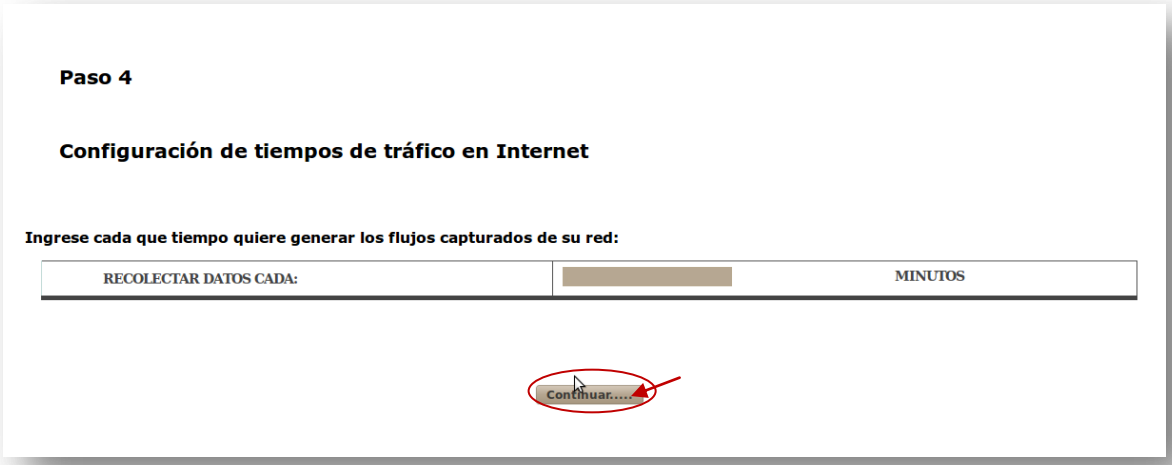


3. Apareciendo la siguiente ventana ingrese el Host, Usuario y Contraseña para conectarse a la Base de Datos del Servidor de Monitoreo. Presione Conectar y después Continuar...

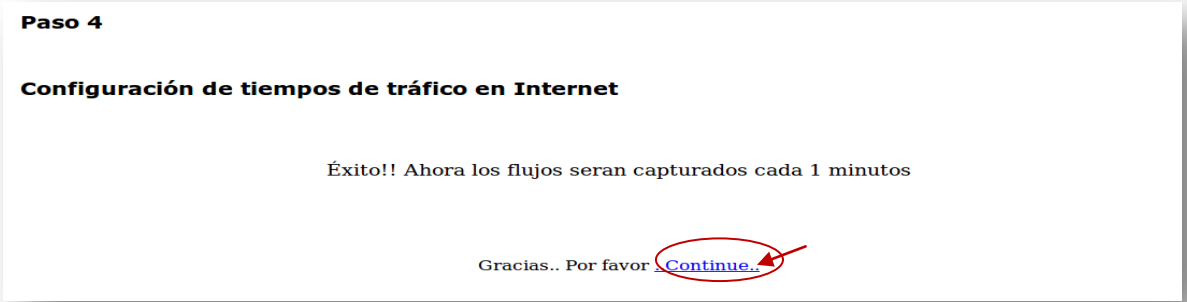


4. Proceda a ingresar los tiempos de captura de los Flujos del tráfico Netflow que pueden estar entre 1 a 5 minutos. Después pulse Aceptar y Continuar….

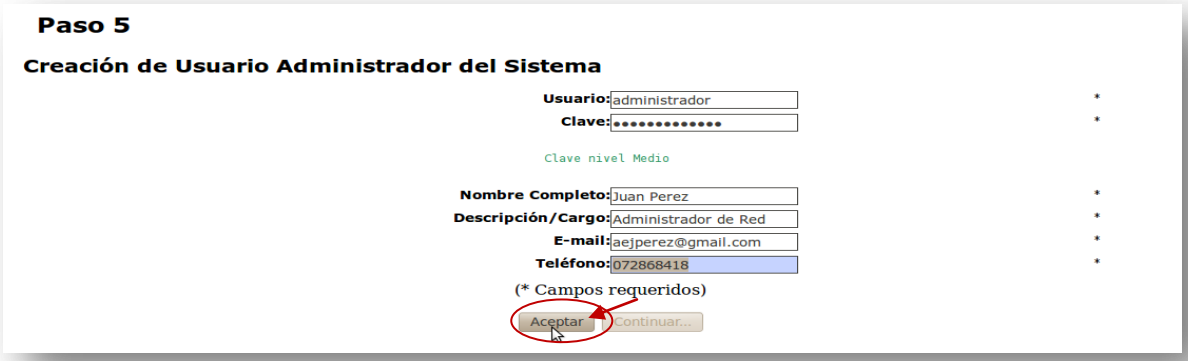


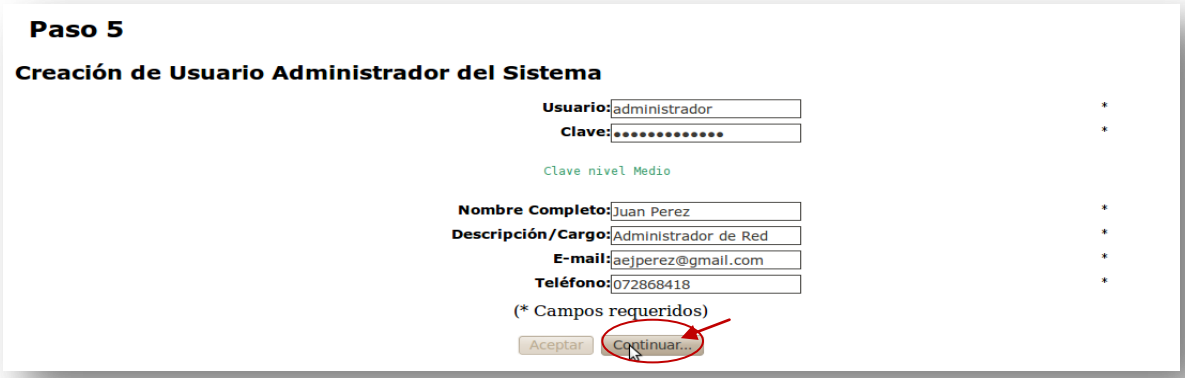


Apareciéndole una ventana de confirmación de que los tiempos fueron modificados de clic en el enlace Continuar, para proseguir con la configuración del Sistema de Monitoreo.

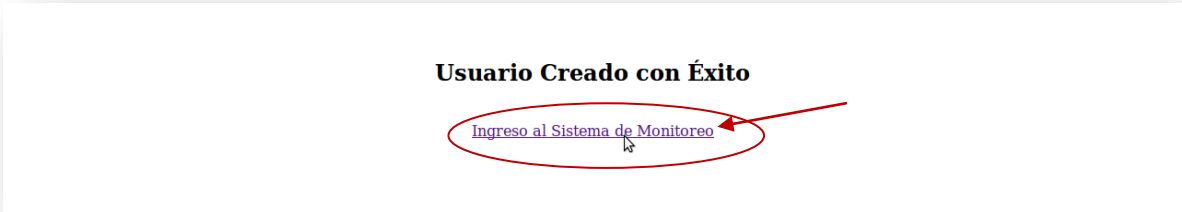


5. Luego aparecerá para la creación del primer Usuario que tendrá acceso al Sistema, ingrese los campos requeridos con * para el registro del usuario pulse Aceptar y Continuar.





6. Apareciendo la siguiente ventana que le indicara que su Usuario ha sido creado con éxito, pulse Ingreso al Sistema de Monitoreo, para acceder a la Administración del Sistema.



Administración del Sistema:

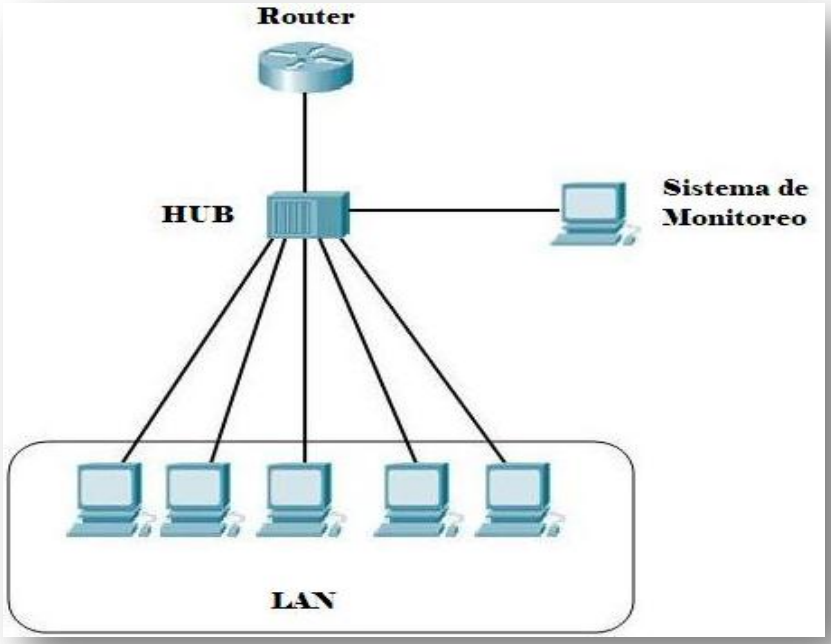
1. Dentro de un navegador web ingrese a la siguiente ruta:

   http://ipservidor/web3/trains/html

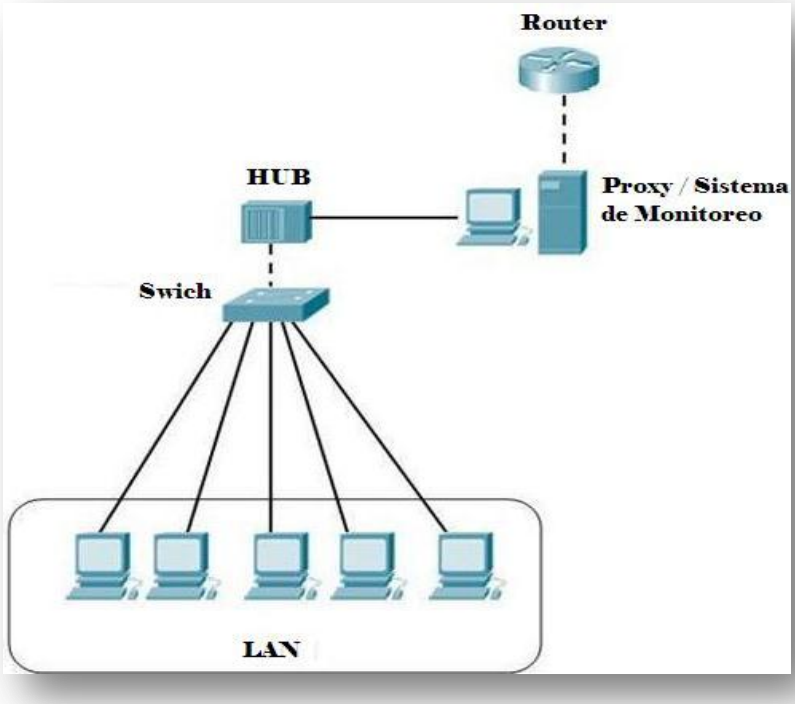
   visualizando la siguiente pantalla e ingrese su respectivo Usuario y Contraseña previamente creado, pulse LOGIN:

2. Una vez logueado al Sistema de Administración usted podrá observar la página de Inicio y en la pestaña Home usted tendrán los dos tipos de Topologías de Red con el que funciona dicho Sistema.

Topología 1

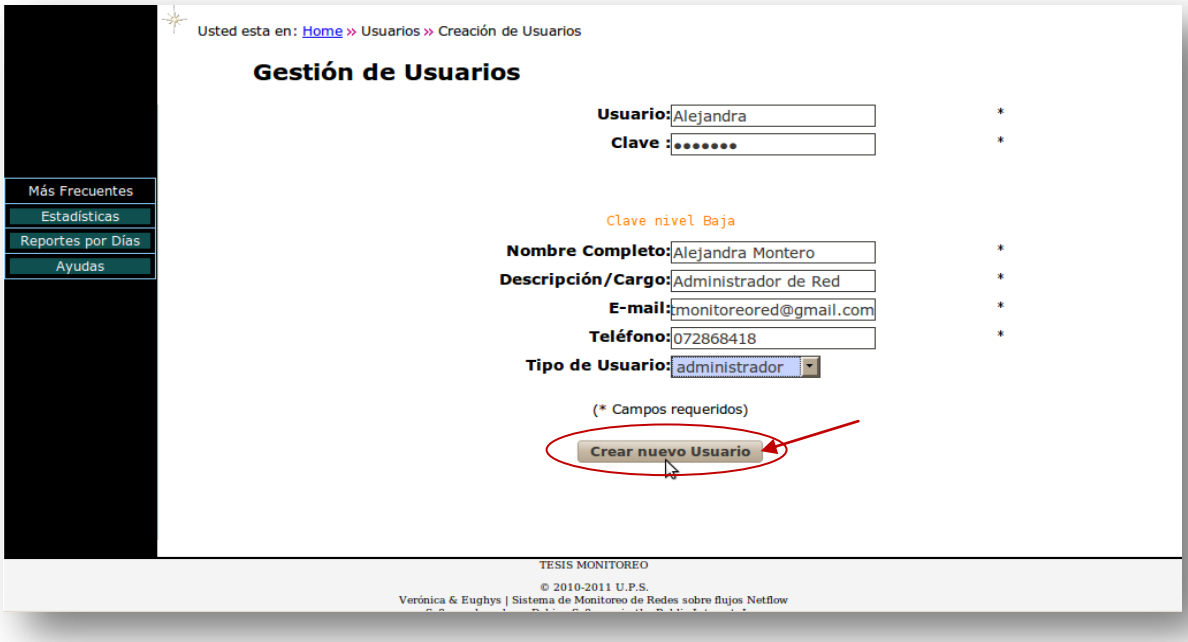


Topología 2

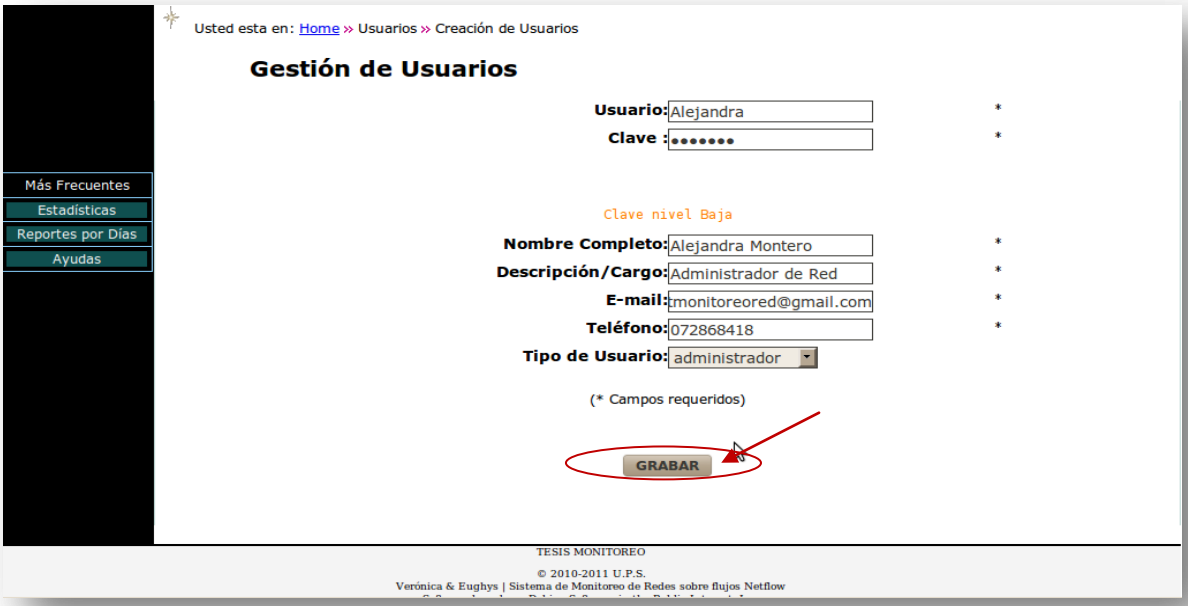


3. Ingrese en la Pestana Gestión en Crear Nuevos Usuarios para registrar uno nuevo.

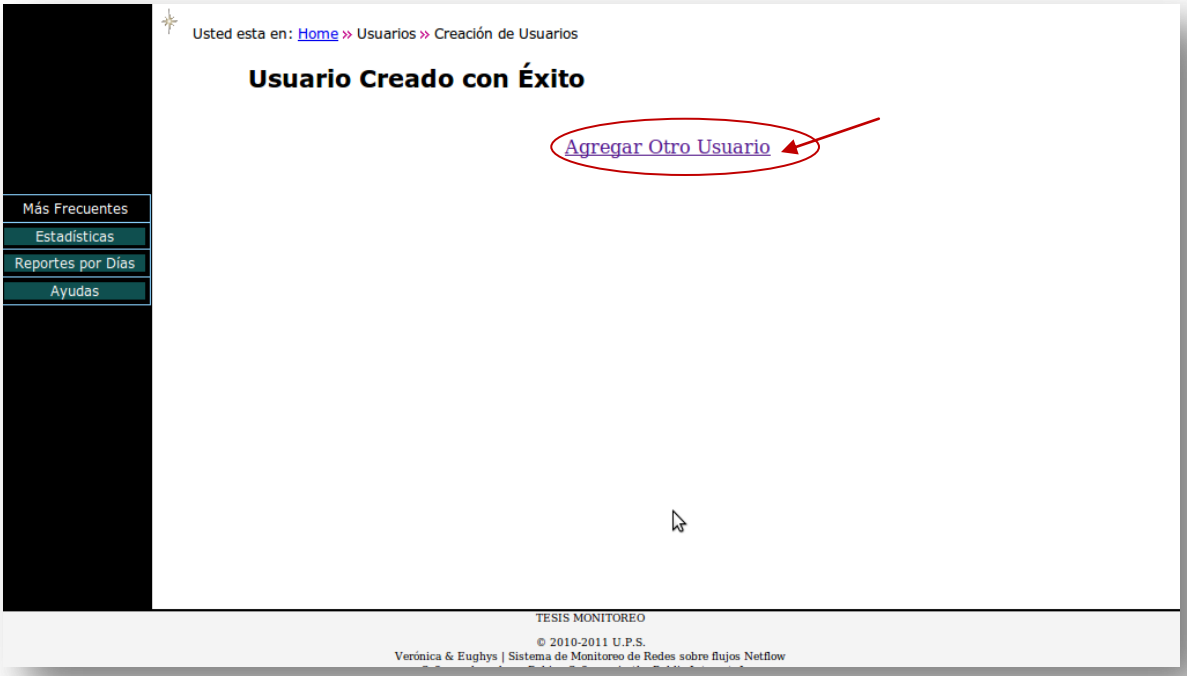
4. Le aparecerá una ventana para que registre a su nuevo usuario, donde los * representan los campos que obligatoriamente deben ser llenados y pulse Crear nuevo Usuario, para la verificación de los datos proporcionados por el Usuario.



Posteriormente pulse Grabar para registrar al nuevo Usuario.

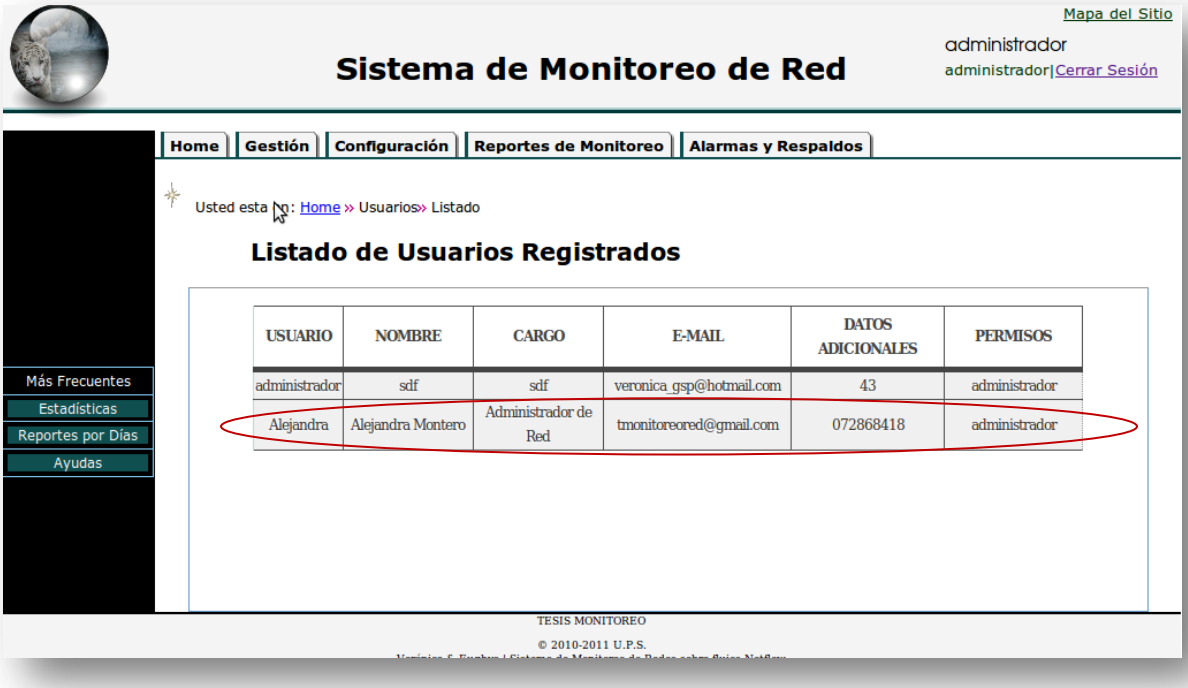


Apareciendo la siguiente ventana, que le permitirá regresar a Creación de Nuevos Usuarios en caso de que lo desee.



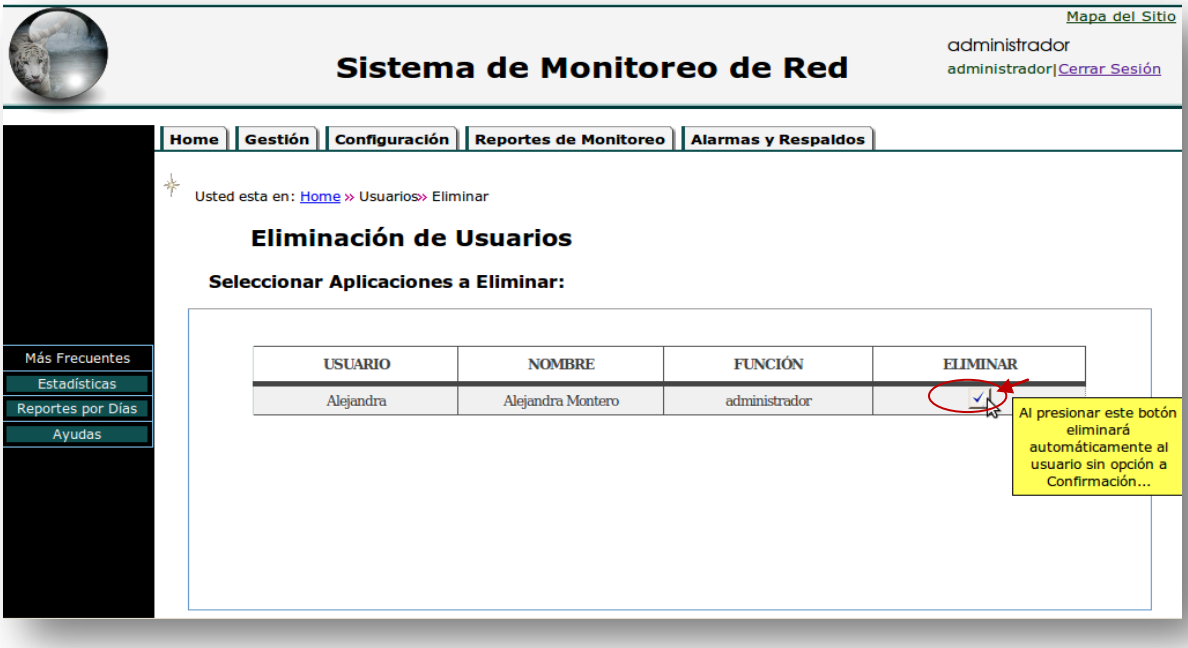
5. De clic en Gestión, Listar Usuarios Existentes para observar los usuarios que están registrados en el Sistema.

Presentándose así:



6. Al ingresar en Gestión, Eliminar Usuarios le aparecerá la ventana en la que usted podrá eliminar a los usuarios anteriormente creados.

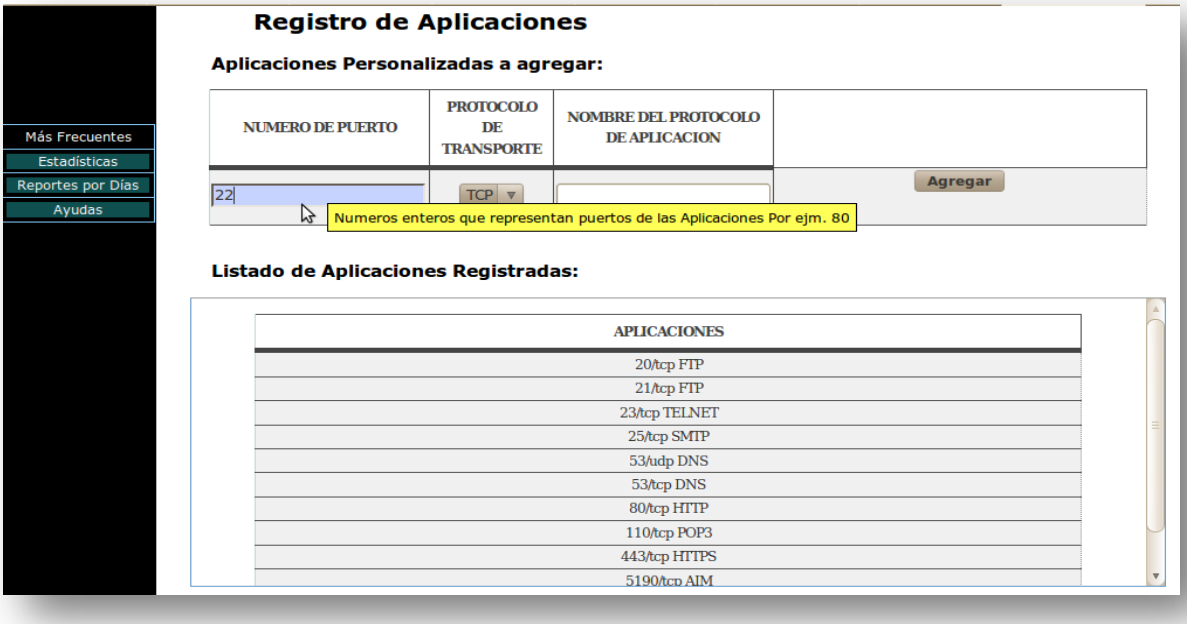
7. En esta ventana le dará la posibilidad de eliminar a los usuarios creados desde el Sistema de Monitoreo, pero siempre cuidando que no se elimine al usuario Administrador con el objetivo de que este pueda loguearse y administrar el Sistema.



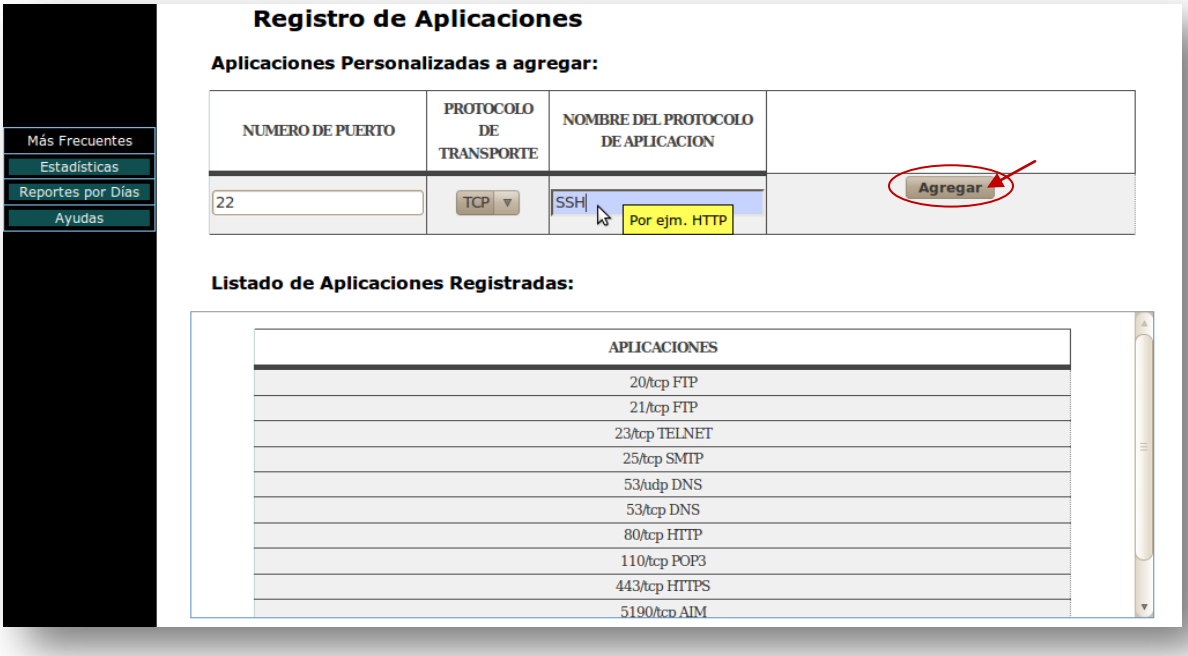
8. Apareciendo luego una ventana que le permitirá regresar a la ventana de Eliminación de Usuarios si pulsa en el enlace Eliminar otro Usuario.

9. Ahora de clic en Gestión, Ingresar Aplicaciones para Registrar los servicios a monitorizar en el Sistema.

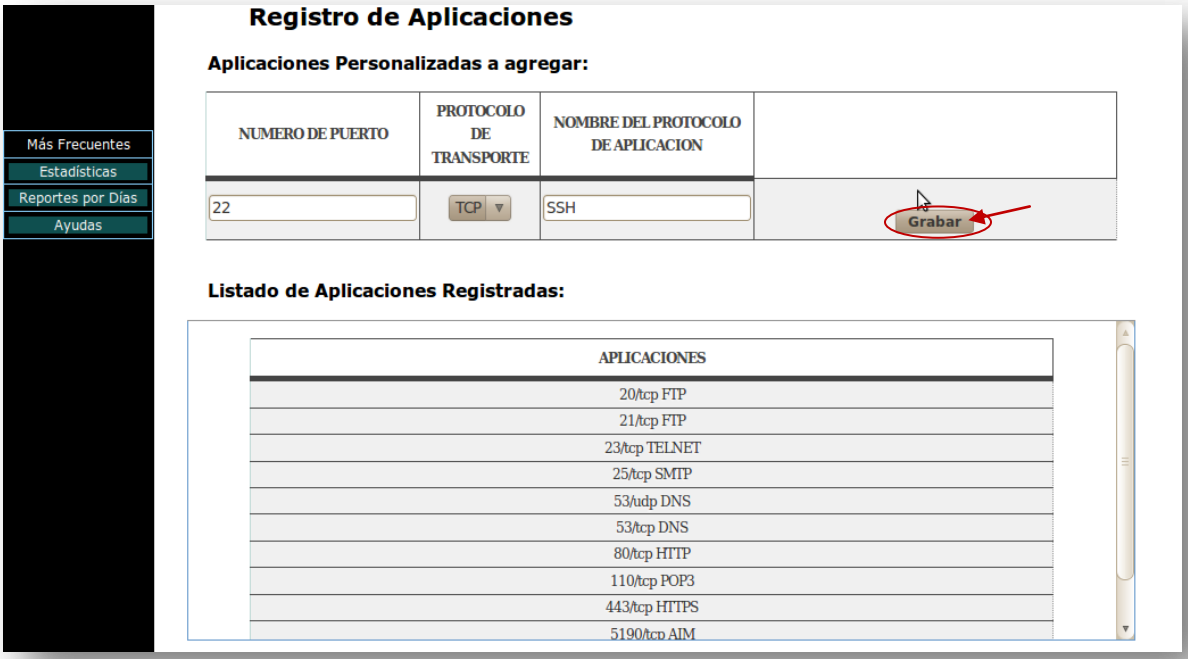
Ingrese un numero comprendido entre 1 y 65535 en Numero de Puerto, además en Protocolo de Transporte puede escoger si es TCP o UDP.



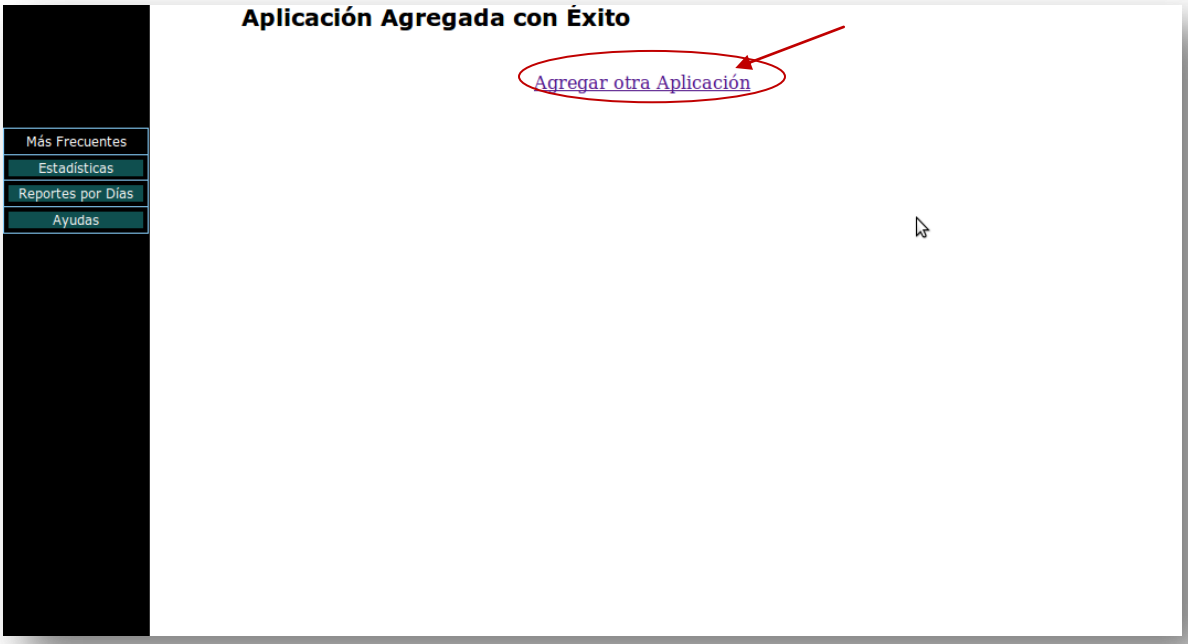
En Nombre del Protocolo de Aplicación, usted puede colocar el nombre del protocolo al que corresponde según el número del puerto ingresado anteriormente y presione Agregar.



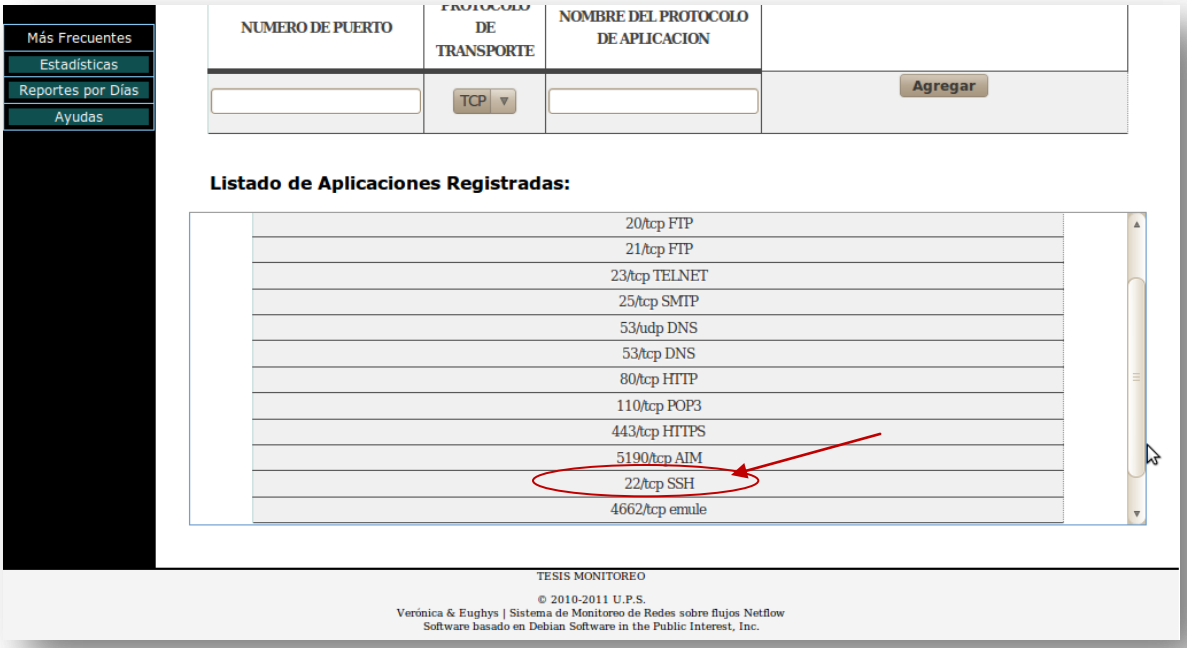
Posteriormente presione Grabar.



Apareciéndole la siguiente ventana, en la cual si da clic en Agregar otra Aplicación le permitirá registrar un nuevo Servicio:

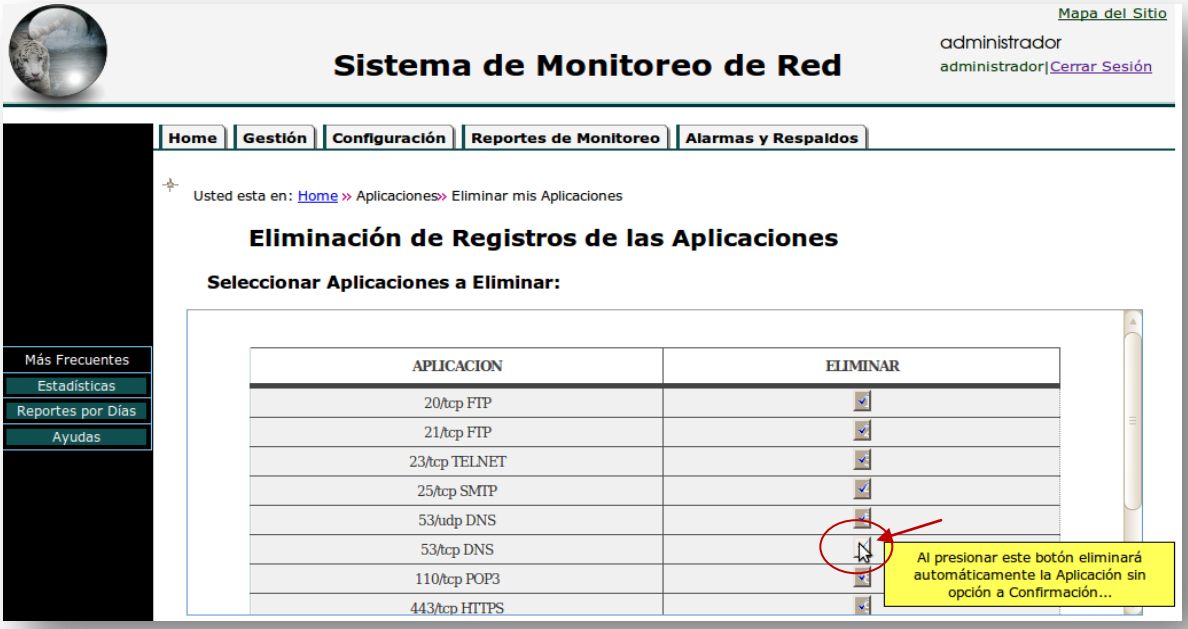


Al regrasar a la ventana de Registro de Aplicaciones usted puede observar que se a registrado correctamente el servicio que creo ya que este se visualizara en la tabla ubicada en la parte inferior de la ventana.



10. Ahora si desea Eliminar Servicios de clic en Gestión y Eliminar Aplicaciones.

Una vez que de clic en visto bueno que se encuentra ubicado junto a cada aplicación se borrara automáticamente.



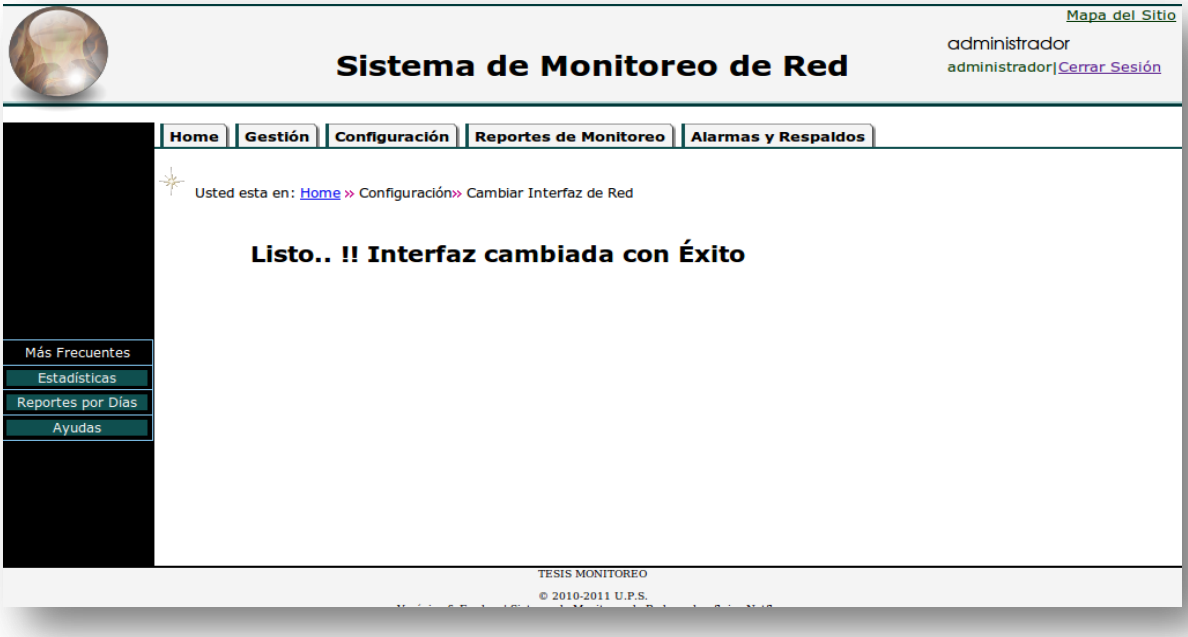
Posteriormente aparecerá la siguiente pantalla en la cual si da clic en el enlace Eliminar otra Aplicación, permitiéndole regresar para que elimine otro servicio.

11. Ingrese en Configuración, Configurar Interfaz para colocar una interfaz de Red diferente a la eth0 que es la que viene por Defecto.

Aquí usted deberá seleccionar la Interfaz de Red cableada por la que desea escuchar los flujos Netflow, aunque por defecto viene configurado con la interfaz eth0 y pulse Aceptar.

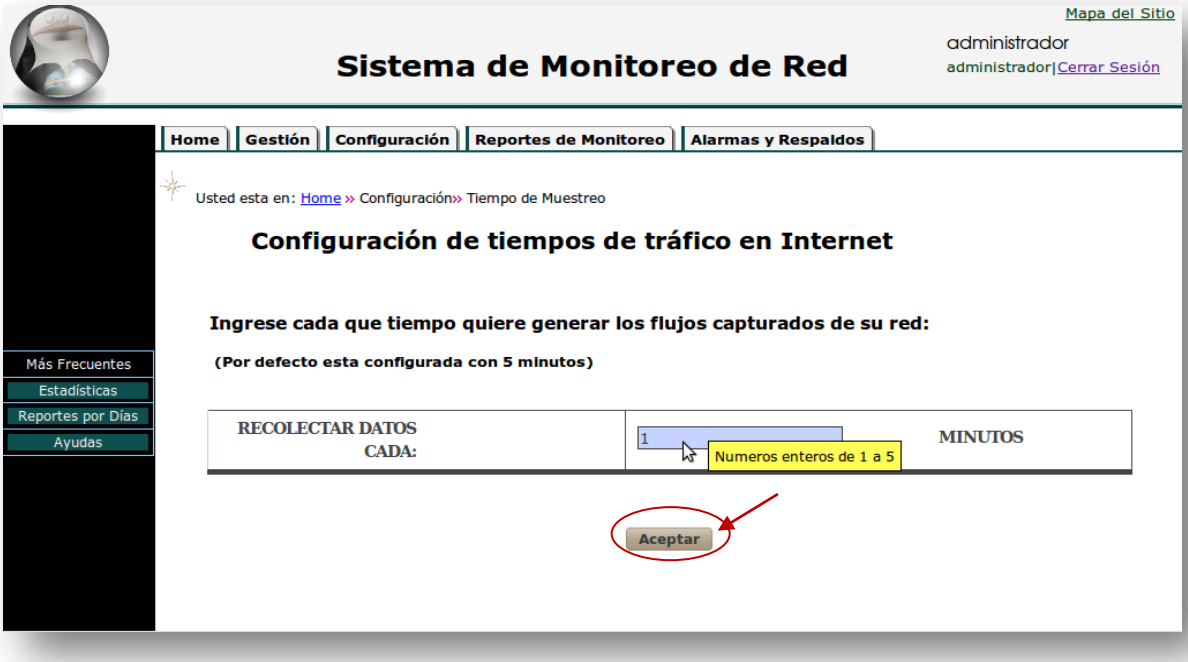
Luego pulse Continuar…. para confirmar y proceder a efectuar los cambios de la interfaz de red.

Presentándonos una página que indica que dicha interfaz ha sido modificada:

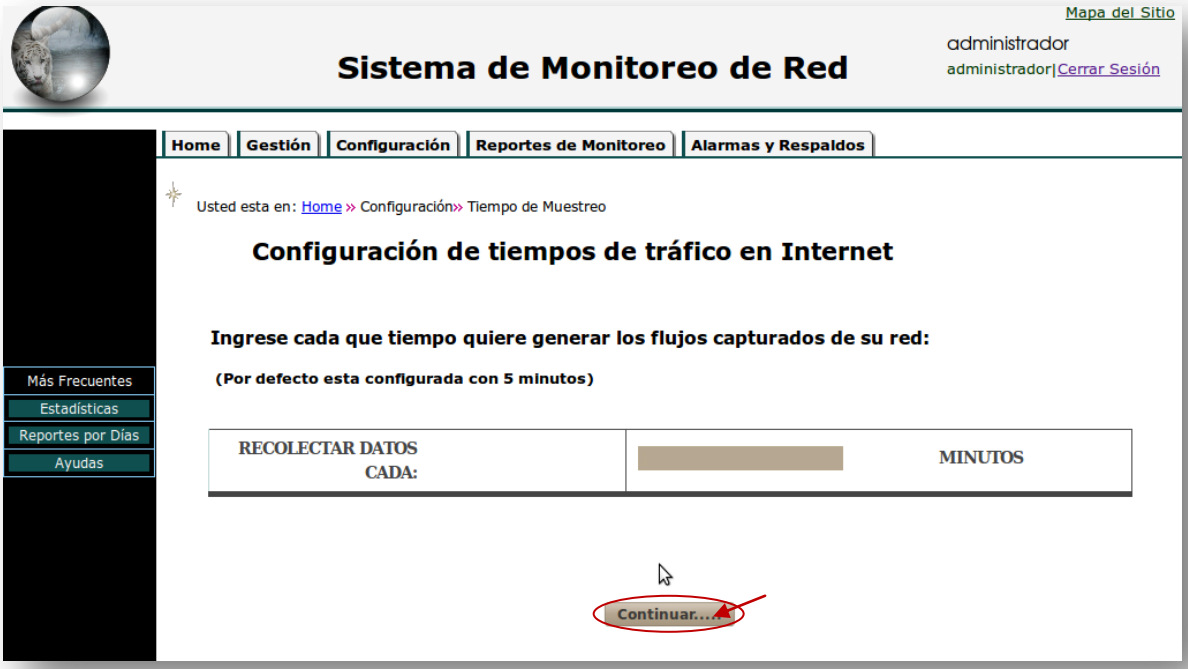


12. De clic en la pestaña Configuración, Configurar Tiempos de Captura para modificar el tiempo de muestreo de los flujos así como para su exportación hacia la base de datos.

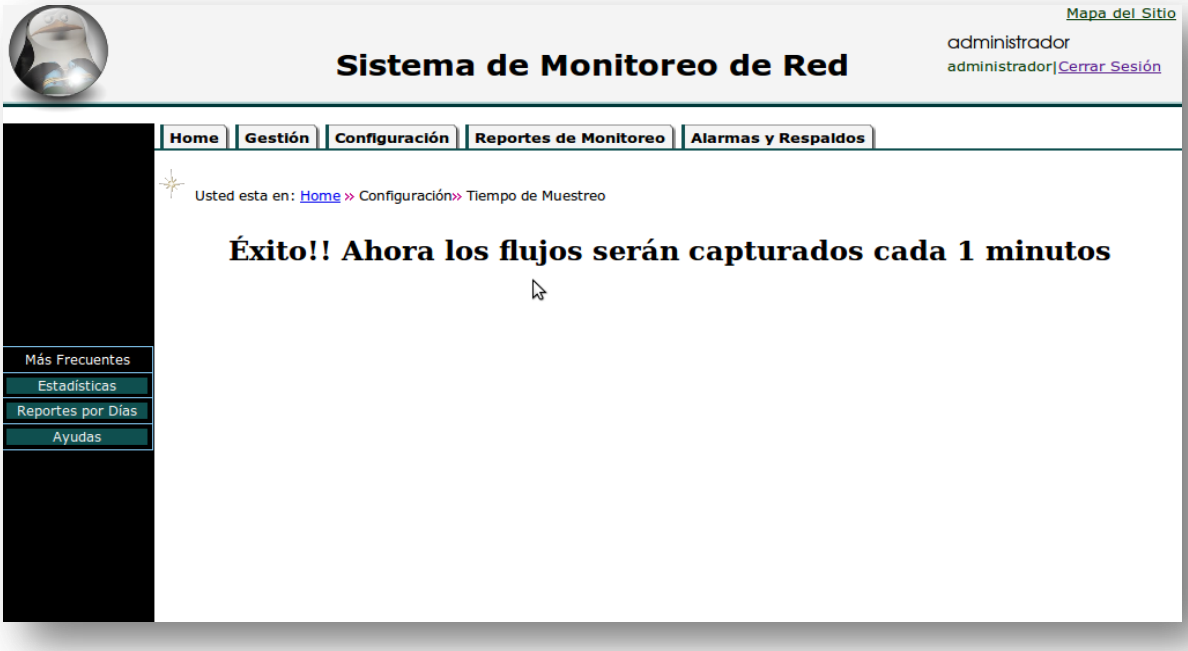
Ingrese el periodo de tiempo de recolección de datos comprendidos entre los valores de 1 a 5 minutos y pulse Aceptar.



Para guardar los cambios pulse Continuar…..

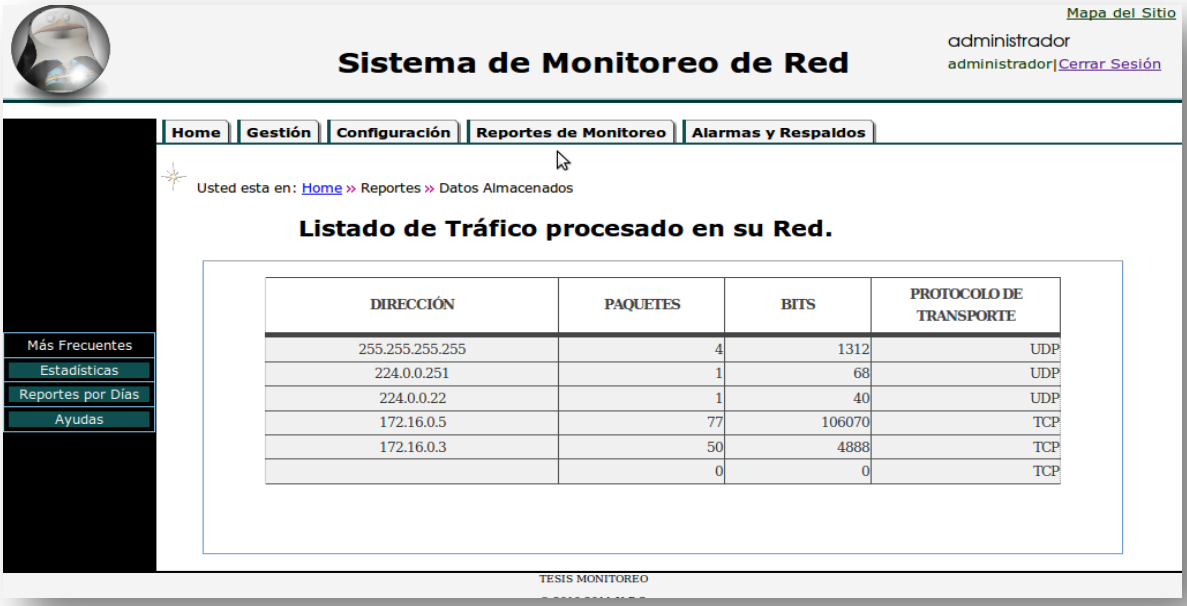


Apareciéndole la siguiente ventana que confirmará que los tiempos han sido modificados.



13. Para obtener reportes de los datos monitorizados que están almacenados en la Base de Datos de clic en Reportes de Monitoreo, Datos Almacenados

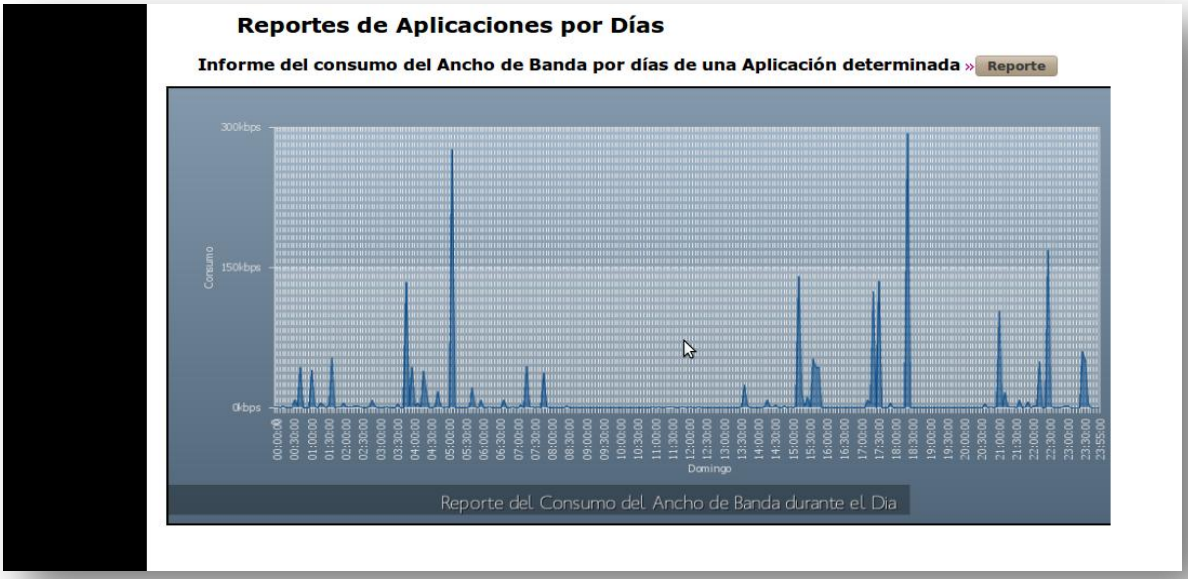
Presentándonos el siguiente cuadro de los flujos Netflow, donde se describe los paquetes consumidos, el número de bits y el protocolo de transporte consumido por una IP dada:



14. Para obtener un reporte General por día del consumo de ancho de banda de clic en Reportes de Monitoreo, Monitoreo General.

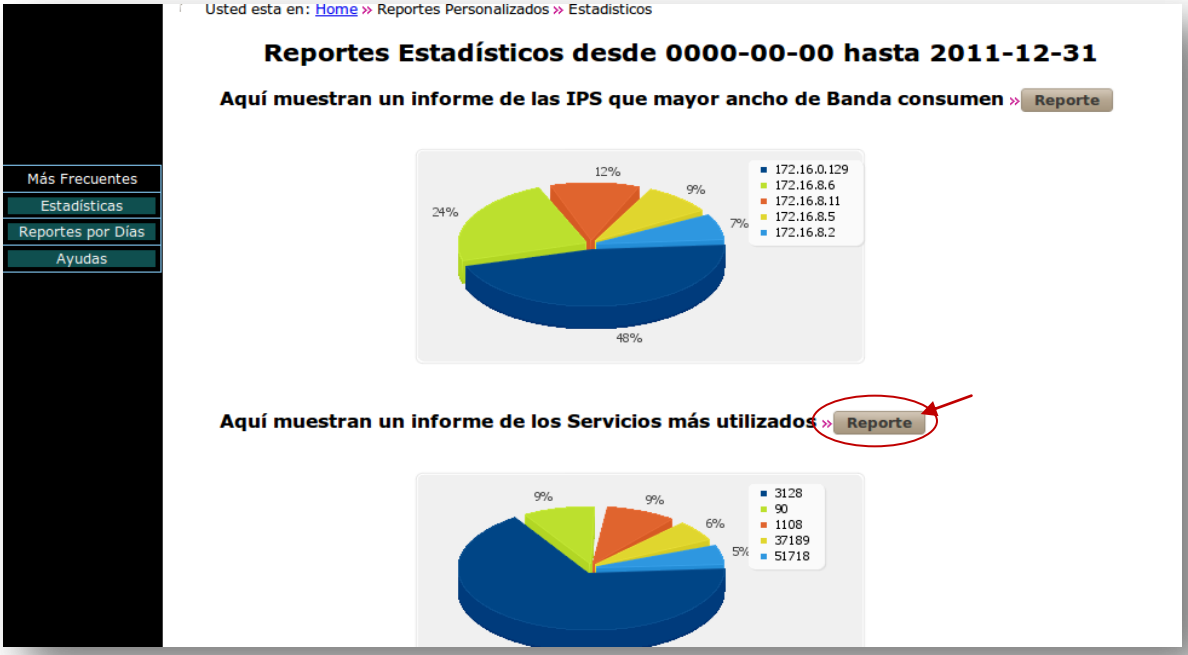
Para ello seleccione la fecha, en la parte superior podrá escoger el mes así como el año deseado, debajo de este se presentan los días, de clic sobre el que desee y presione Consultar para que se muestre la gráfica en la parte inferior.

Viéndose como se muestra a continuación, pero si da clic en Reporte se visualizara una ventana para que el documento pueda ser abierto en formato PDF.

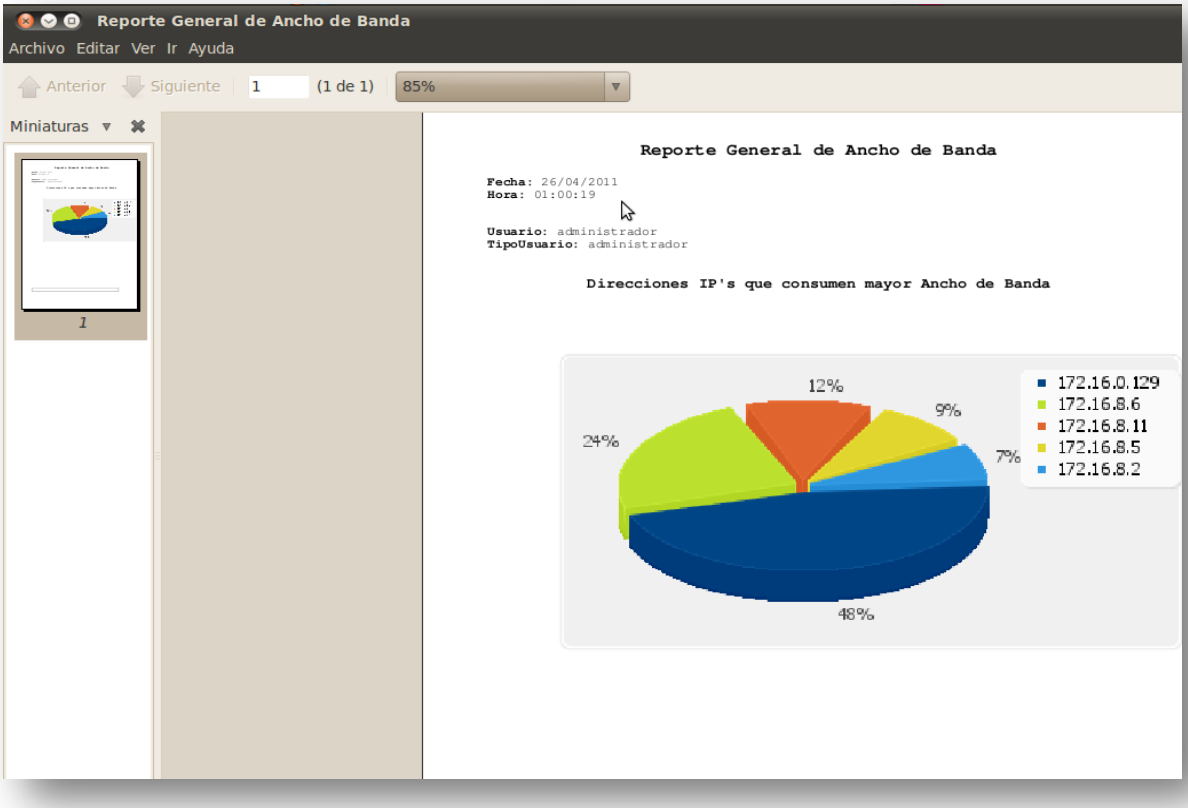


15. Para sacar un análisis general del flujo ya sea por IP o por Servicio, ingrese a Reportes de Monitoreo, Reportes Estadísticos

Aquí se muestran los reportes por IPs y Servicios que han consumido mayor Ancho de Banda y si desea sacar reportes en formato PDF usted puede dar clic en Reporte.



Si pulsa en Reporte le mostrará una pantalla para que visualice o guarde el documento PDF.



Para obtener reportes personalizados por días ingrese a Reportes de Monitoreo y en Reportes por Días.

Escoja la Fecha Inicio, Fecha Fin y pulse en Aceptar. Una vez pulsado se habilitara el campo para seleccionar el Tipo de Búsqueda.

Una vez habilitada usted puede seleccionar su reporte ya sea por IP o Aplicaciones en el campo Reporte por y pulse Consultar.

Posteriormente aparecerán una lista de IPs o Puertos por las que podrá realizar su consulta según lo que escogió anteriormente y pulse GraficarIP o GraficarPuerto.

Ahora se presentara un reporte con la IP o Aplicación seleccionada. Si se escogió por IP se visualizaran todas los puertos que fueron consumidos por dicha IP, caso contrario se mostraran todas las IPs que corresponden al Puerto seleccionado.

Ahora para sacar reportes por Horas, ingrese a Reportes de Monitoreo, Reportes por Horas.

Escoja la Fecha que desea para su reporte por Horas y presione el botón Seleccionar

Escoja las horas presentadas en Hora_Inicio y HoraFin y seleccione el Tipo de Búsqueda las cuales pueden ser por IP o Servicio, luego presione Consultar.

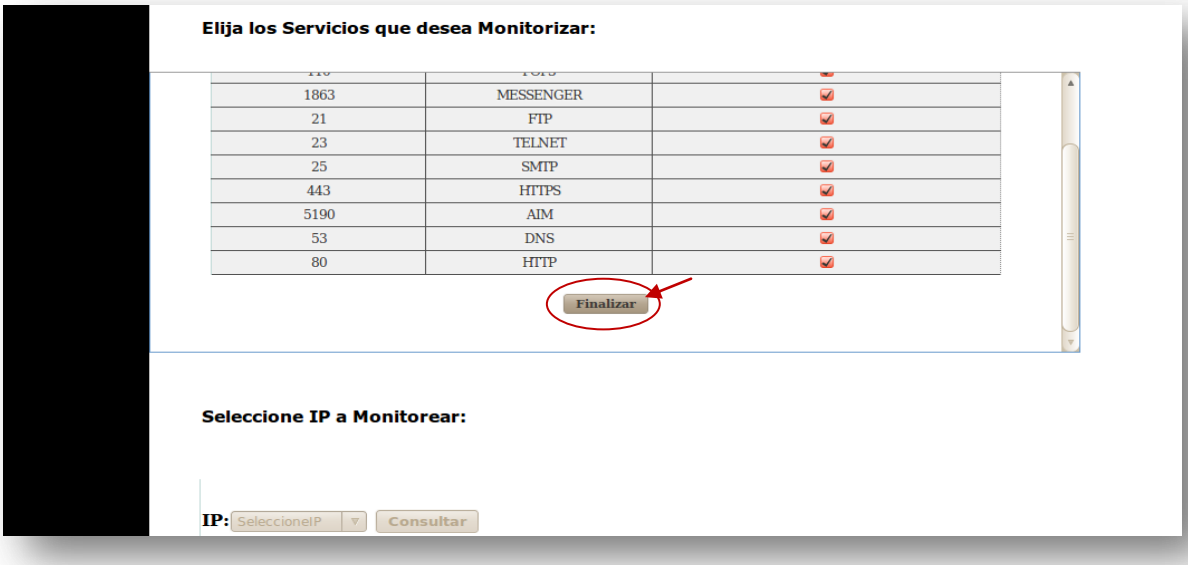
Escoja el puerto o servicio que desee para su consulta. Y presione Mostrar.

Visualizándose la siguiente grafica en la parte inferior de la ventana y en caso de querer visualizarlo en formato PDF de clic en Reporte.

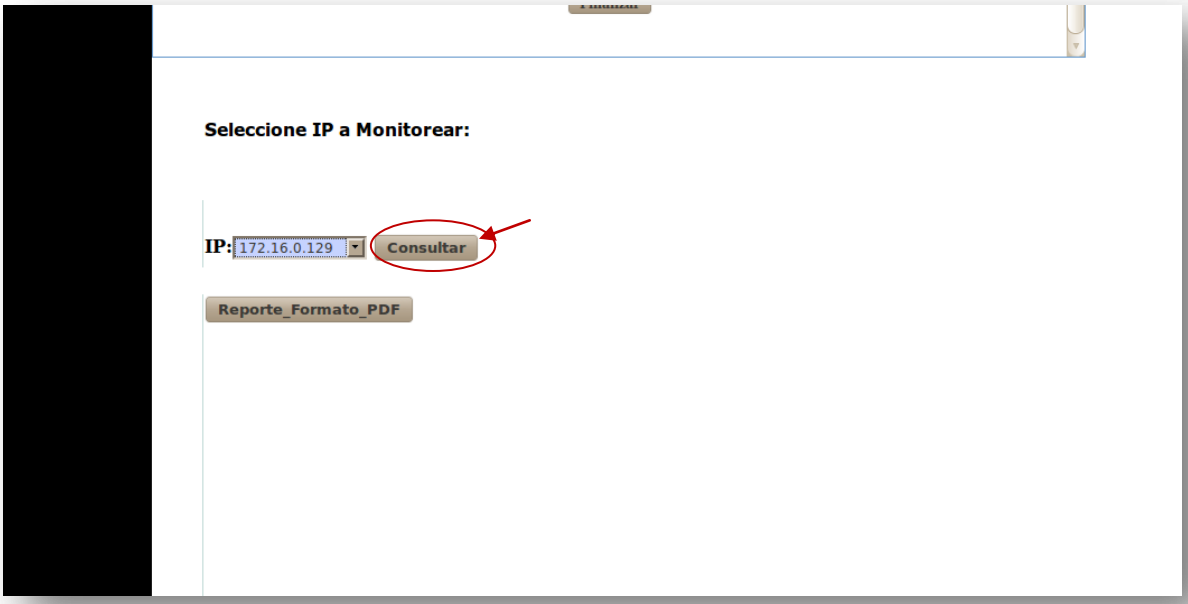
Para obtener un Reporte del Consumo de Ancho de Banda por Aplicación que realiza una IP dada en un día específico, de clic en Reportes de Monitoreo en Reportes por IP del Día.

Primero seleccione el mes y año junto con el día del que desea su consulta del calendario que se muestra a continuación.

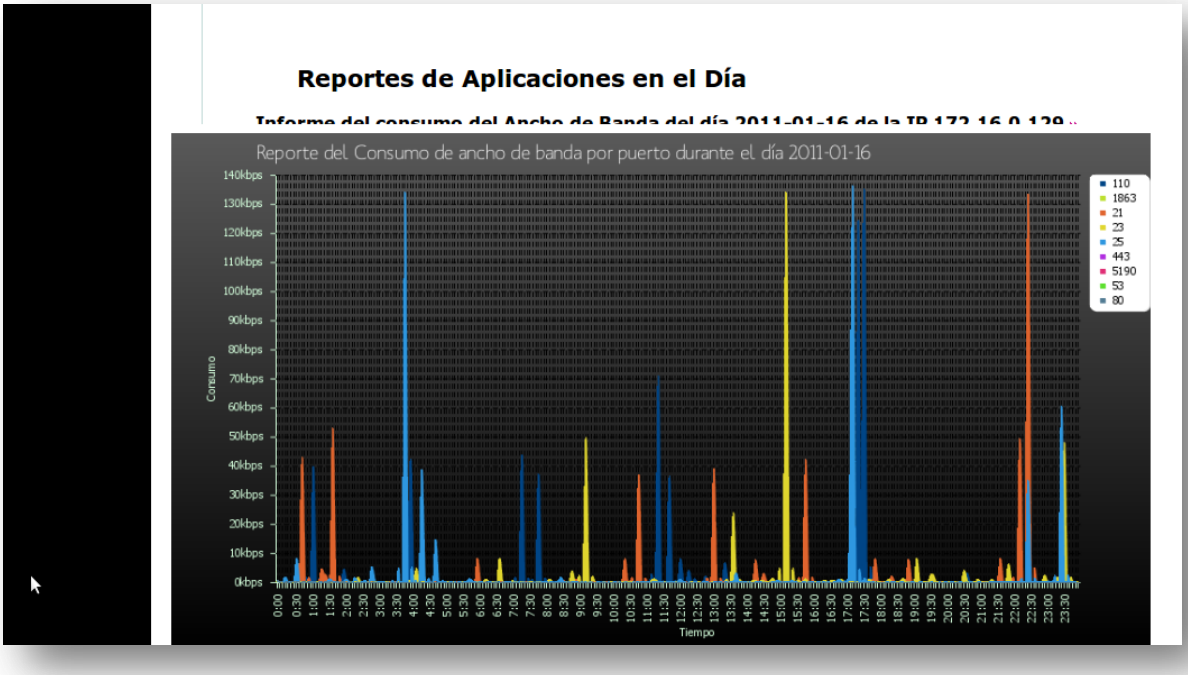
Posteriormente Elija los Servicios que desea Monitorizar: y pulse Finalizar. Puede escoger hasta 15 servicios para graficar al mismo tiempo, esto se da debido a que con un número mayor de servicios se excedan los parámetros del graficador, si usted tiene un número mayor de servicios puede graficarlos en grupos de 15 en 15.



Después elija la IP deseada de la lista mostrada en Seleccione IP a Monitorear: y pulse Consultar para visualizar la grafica en la parte inferior de la ventana, pero para visualizar en formato PDF pulse Reporte_Formato_PDF.



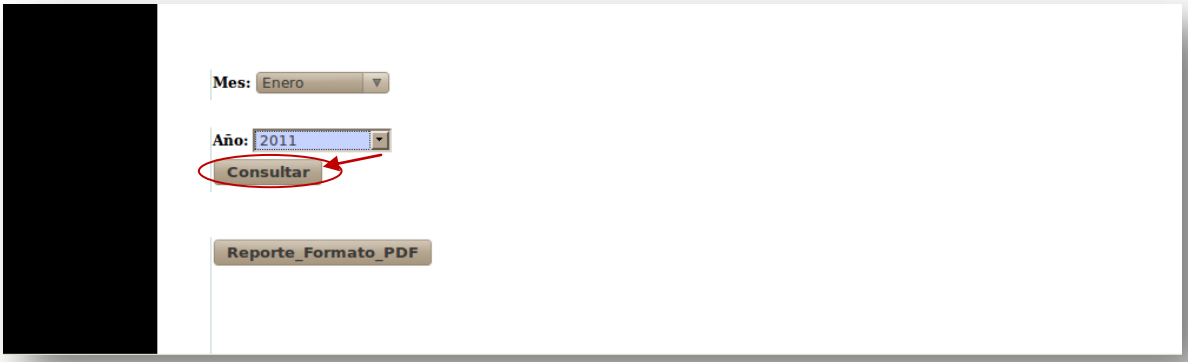
Mostrándose la siguiente grafica que se presenta a continuación:

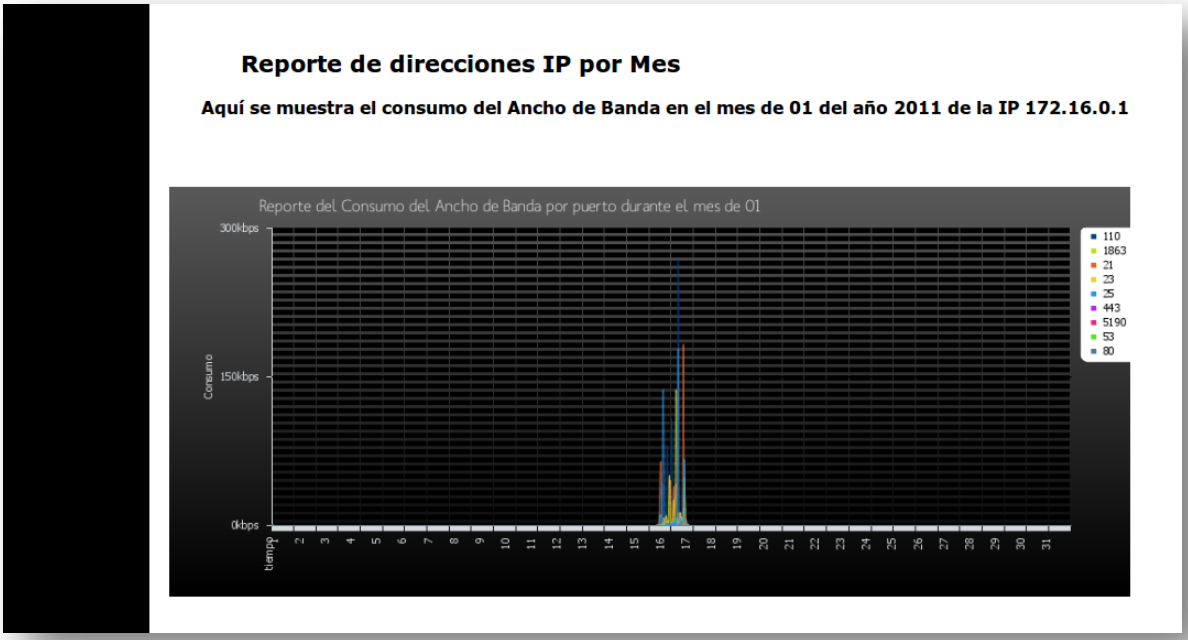


Para obtener un Reporte del Consumo de Ancho de Banda por Aplicación que realiza una IP dada en un mes específico, de clic en Reportes de Monitoreo en Reportes por IP al Mes.

Seleccione una de las IPs de la lista que se muestra en IP: y escoja los servicios que desea visualizar en la gráfica sin exceder de 15 aplicaciones y pulse Finalizar.

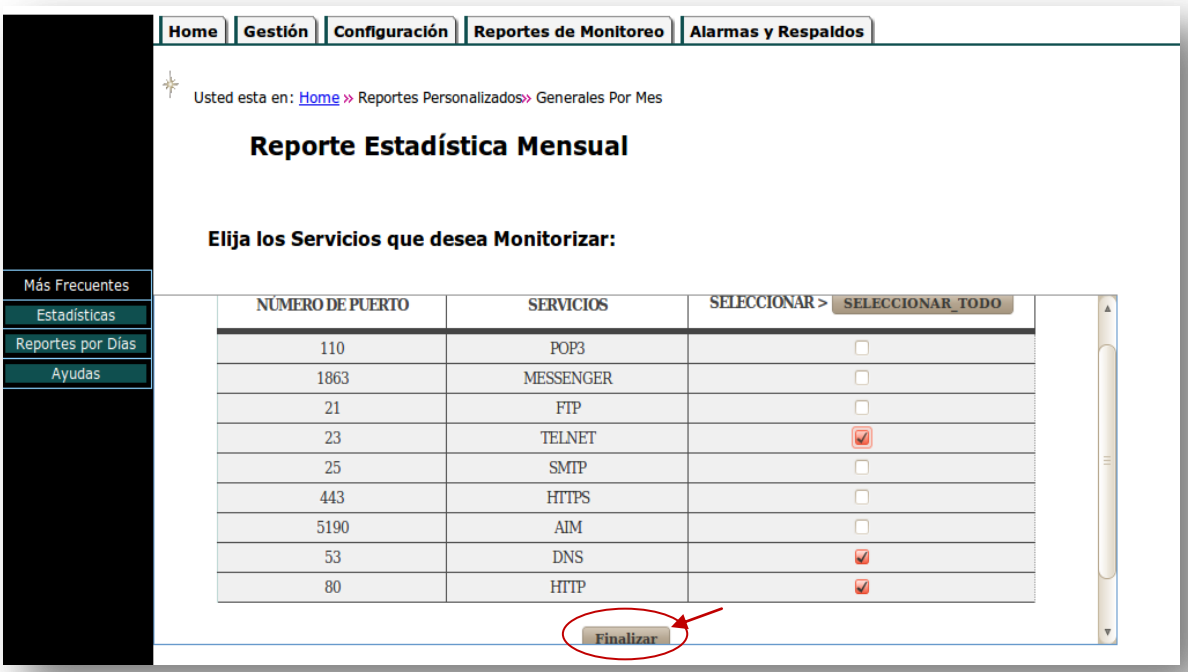
Luego se habilitaran los campos de Mes y Año donde usted deberá escoger el mes y el año del que desea su consulta y pulse el botón Consultar para visualizar su gráfica.



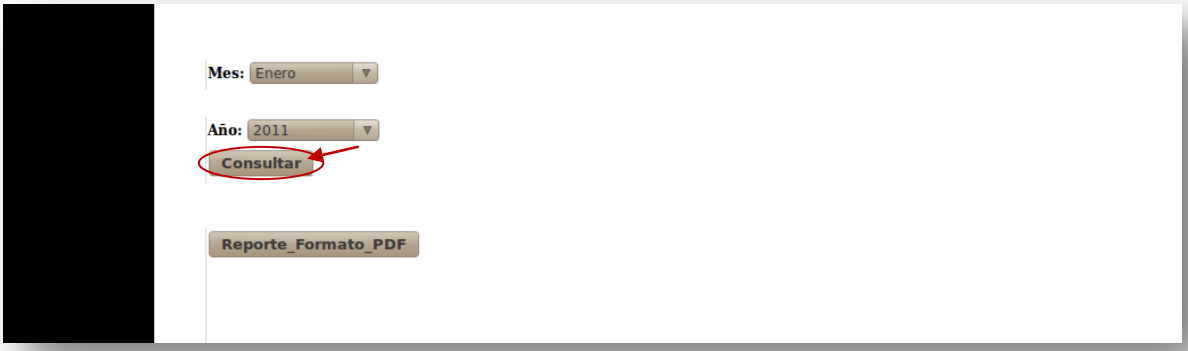


Para obtener un reporte general del consumo total del Ancho de Banda correspondiente a un mes específico de clic en Reportes de Monitoreo, en Reportes General por Mes.

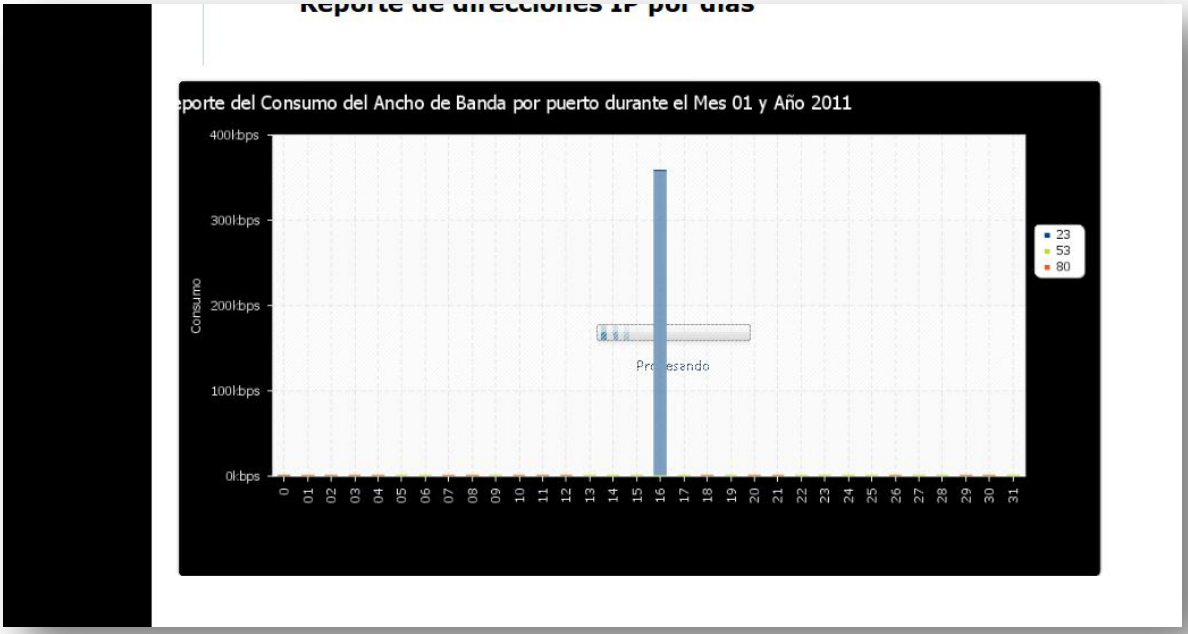
Primero seleccione un número de aplicaciones que no sobrepasen las 15 y pulse Finalizar.



Después seleccione el mes con el año que desea hacer su informe y pulse Consultar para visualizar su reporte en la parte inferior.

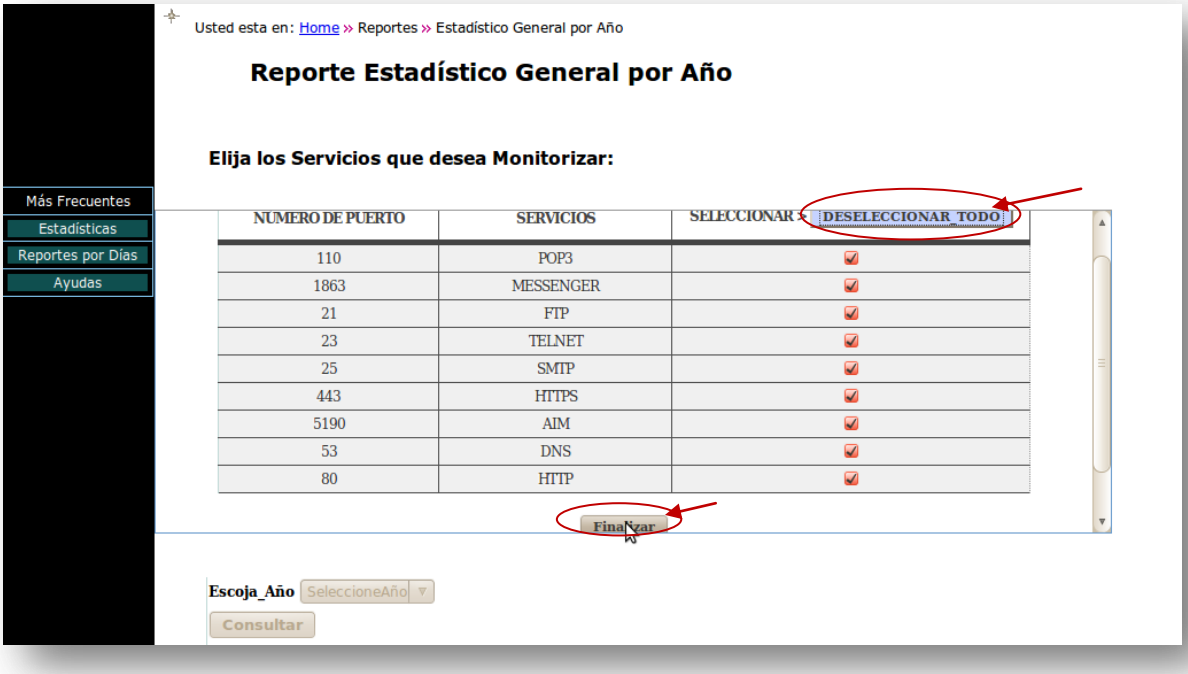


Mostrándose así la siguiente figura.

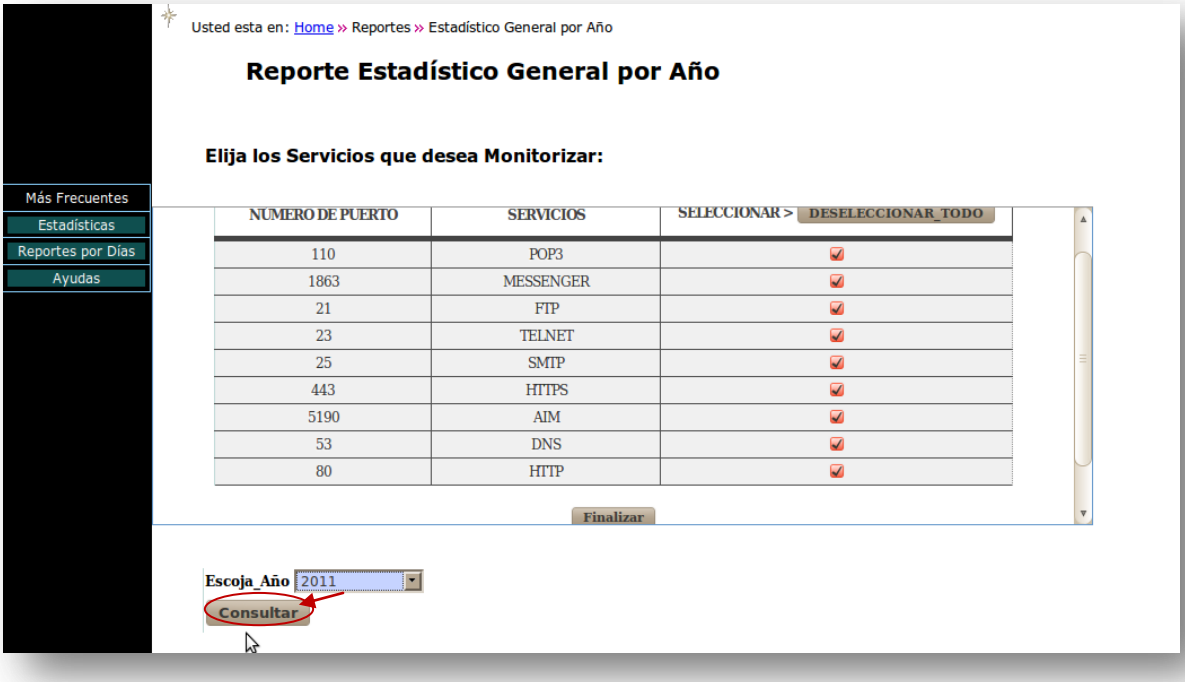


Para obtener un reporte general del consumo total del Ancho de Banda correspondiente a un año específico de clic en Reportes de Monitoreo, en Reportes General por Año.

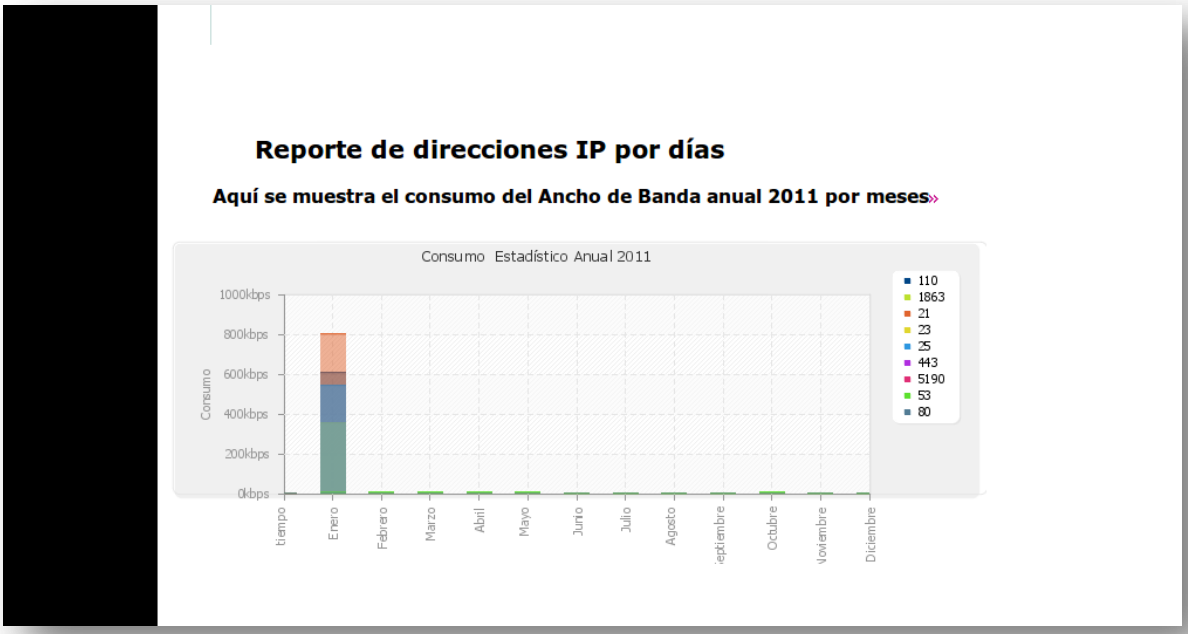
Para la creación de dicho reporte escoja todos los servicios al dar clic en SELECCIONAR_TODO si desea todas las aplicaciones o para deseleccionar en DESELECCIONAR_TODO, pero sin olvidar de no sobrepasar las 15 aplicaciones y pulse Finalizar.



Una vez deshabilitado el campo Escoja_Año, usted podrá seleccionar el año para el que desea realizar su reporte y pulse Consultar para mostrar la imagen.



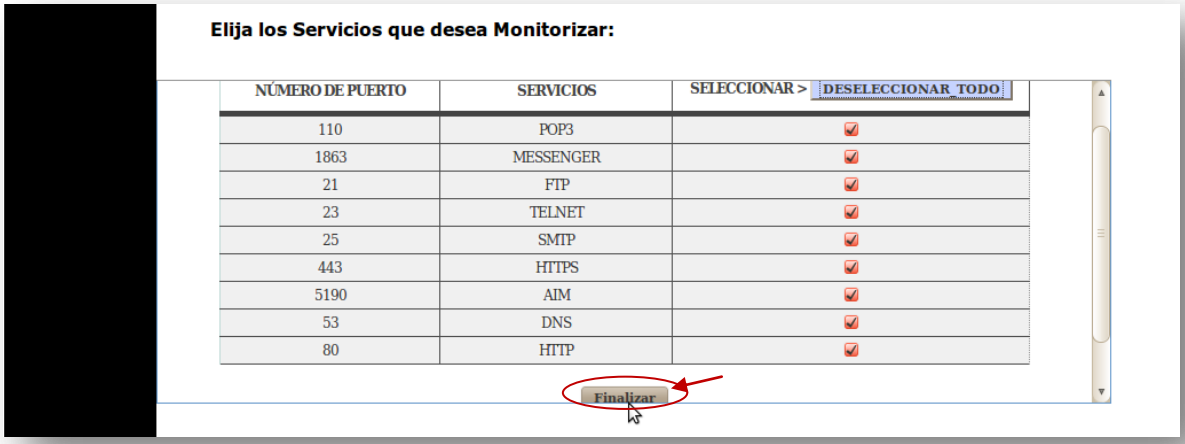
Apareciéndole el siguiente reporte anual:



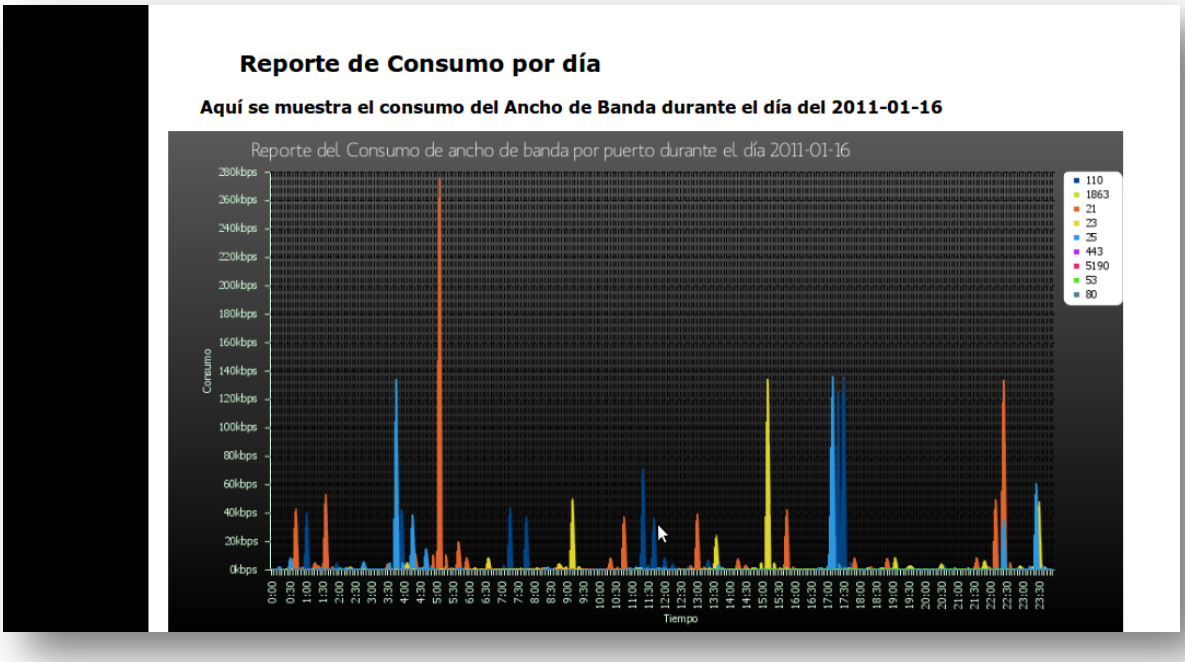
Para sacar un Reporte general diario por Aplicación de clic en Reportes de Monitoreo, en Reporte Diario.

Seleccione la fecha en el calendario que se muestra a continuación para esto primero seleccione el mes, año y de clic en el día, del que desea realizar dicha consulta

Luego de seleccionar los servicios, pulse Finalizar y posteriormente en Consultar para que se muestre en la parte inferior o pulse en Reporte_Formato_PDF para visualizarlo en un pdf.



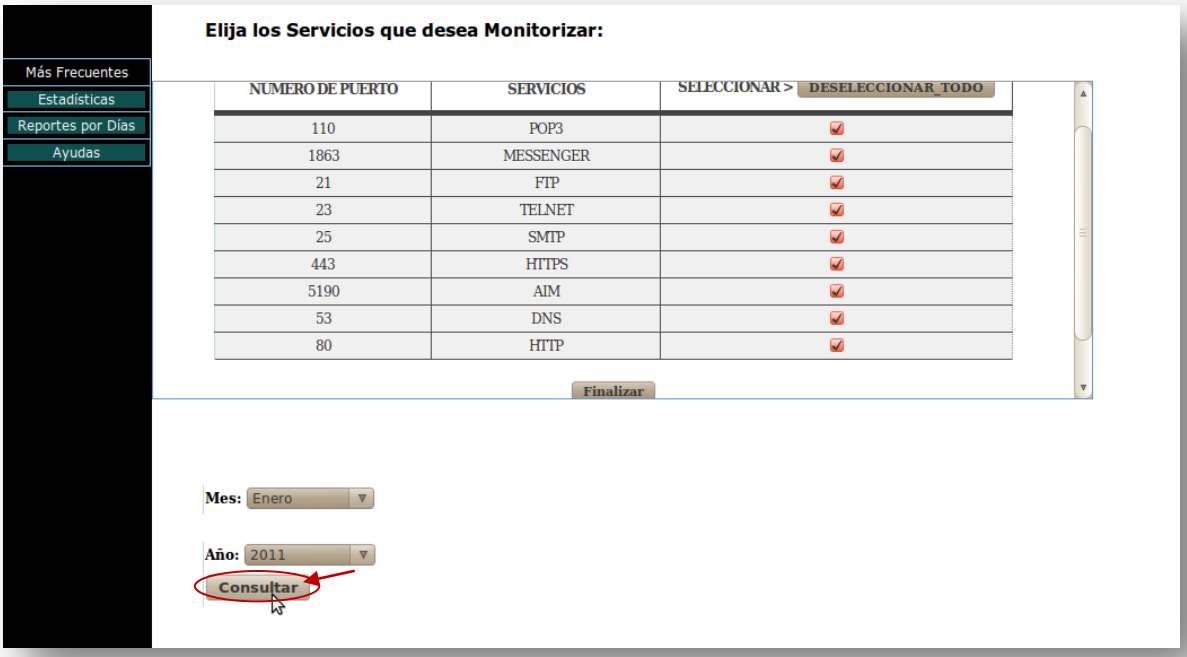
Luego usted podrá observar la siguiente gráfica que se muestra a continuación.



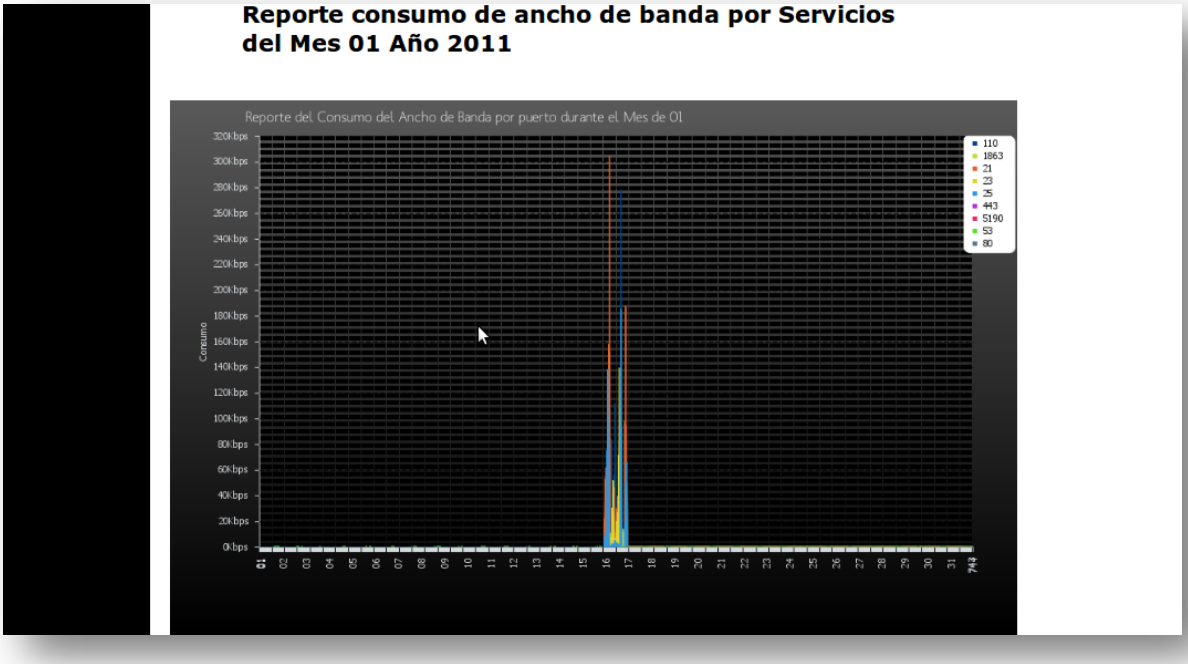
Para obtener un reporte general del consumo de ancho de banda por aplicación mensual, de clic en la pestaña Reportes de Monitoreo, en Reporte Mensual.

Usted deberá escoger las aplicaciones presentada en la siguiente tabla sin exceder de un número de 15, pulse en Finalizar para habilitar mes y año.

Una vez habilitada escoja el Mes y el Año para que después pulse **Consultar**.

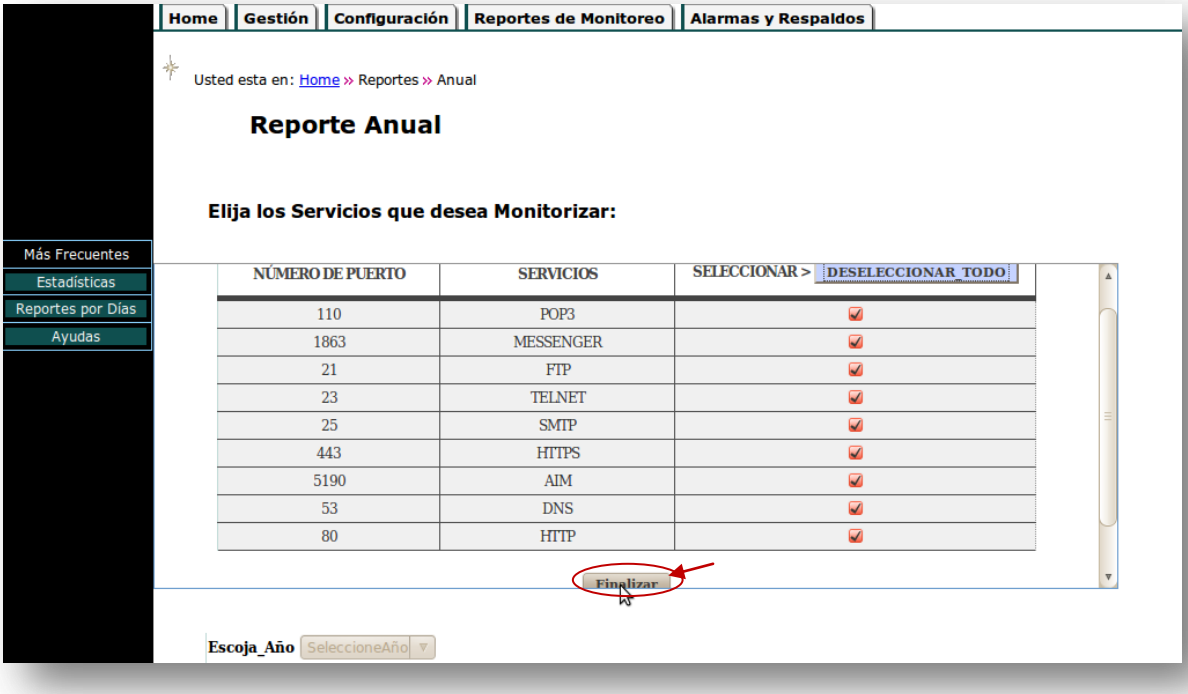


Mostrándose al final de la ventana la siguiente imagen.



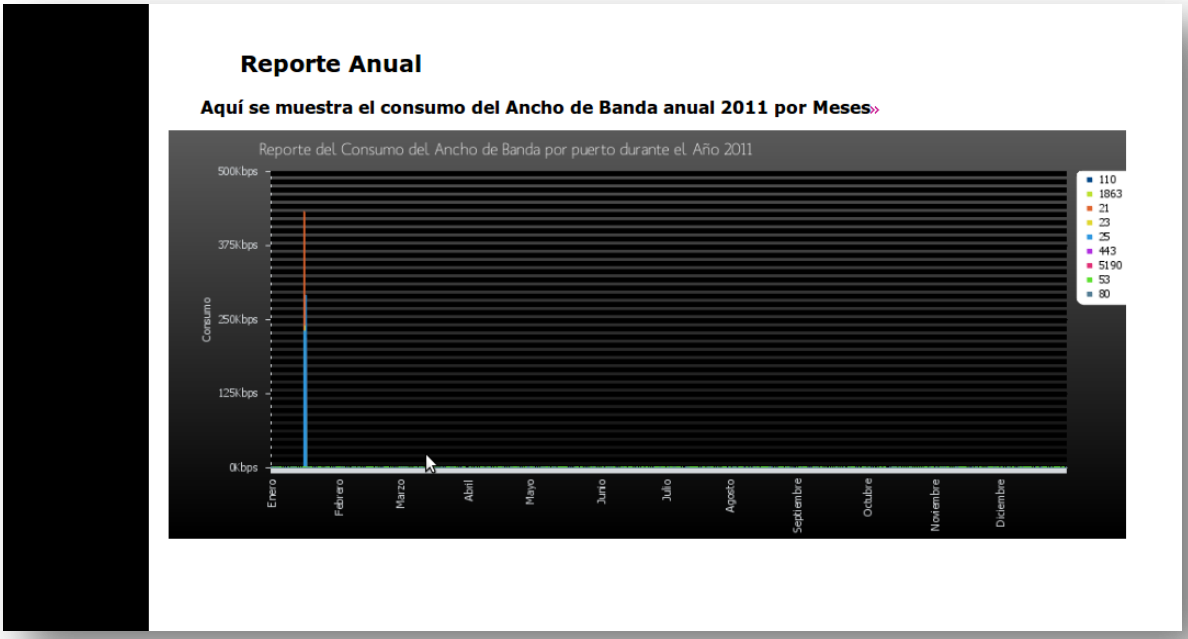
Para obtener reportes Anuales por aplicación del consumo de Ancho de Banda de clic en **Reportes de Monitoreo**, **Reporte Anual**.

Primero usted deberá escoger entre 1 a 15 aplicaciones y pulse **Finalizar** para habilitar el Año.



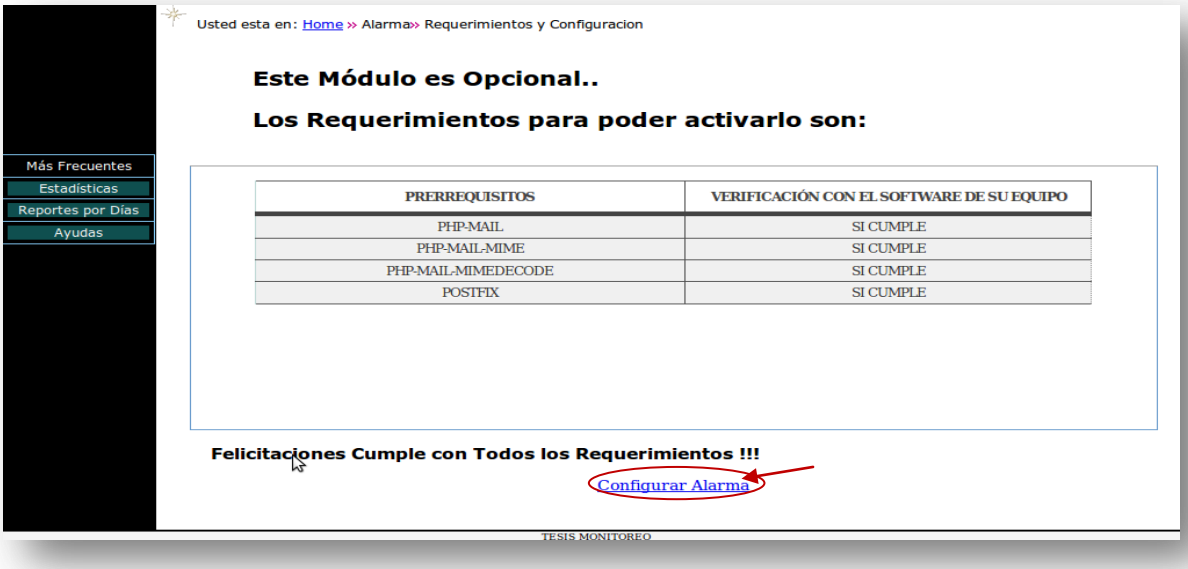
Segundo usted deberá escoger el Año, pulse en **Consultar** con esto se visualizara el reporte en la parte inferior o en caso de pulsar **Reporte_Formato_PDF** usted podrá guardar el reporte en formato pdf.

Mostrándose la siguiente gráfica del consumo de ancho de Banda anual después de esperar unos minutos.



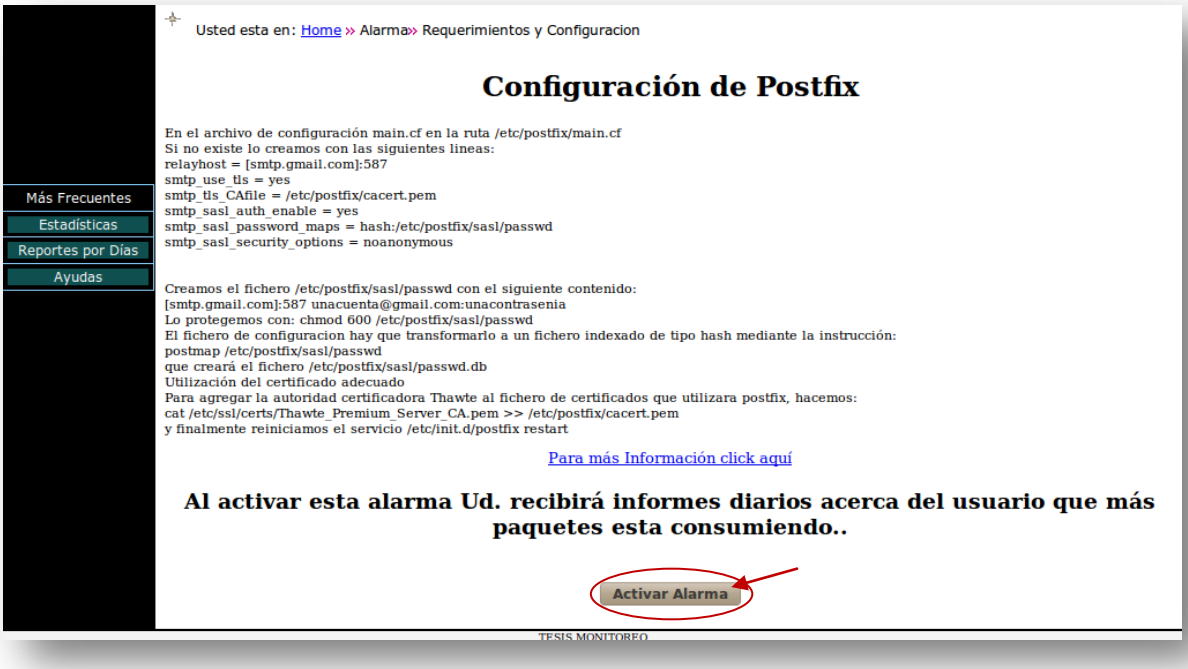
16. Para la configuración de la Alarma, ingrese a la pestaña Alarmas y Respaldos, en Requisitos y Configuración.

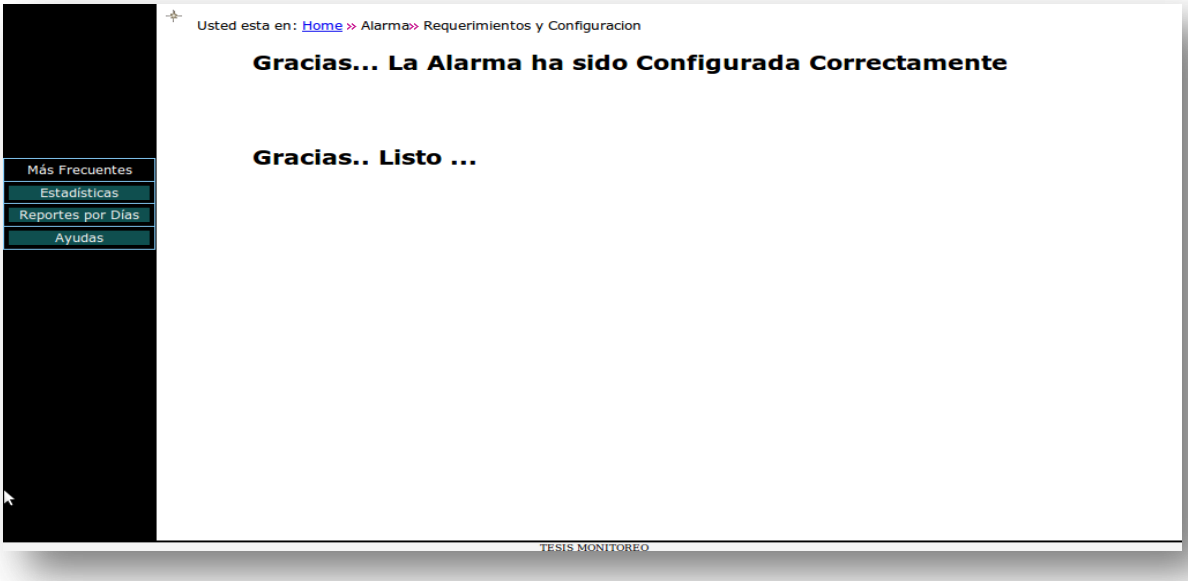
Aparecerá una ventana en la que indicaras los requisitos de software necesarios para que este modulo funcione correctamente una vez que usted observe que todos los requisitos consten como SI CUMPLE prosiga al enlace Configurar Alarma para la activación y envió periódico de reportes que serán para las 5 y 30 de la tarde, enviándole un reporte de la IP que mayor consumo de paquetes a realizado durante ese día



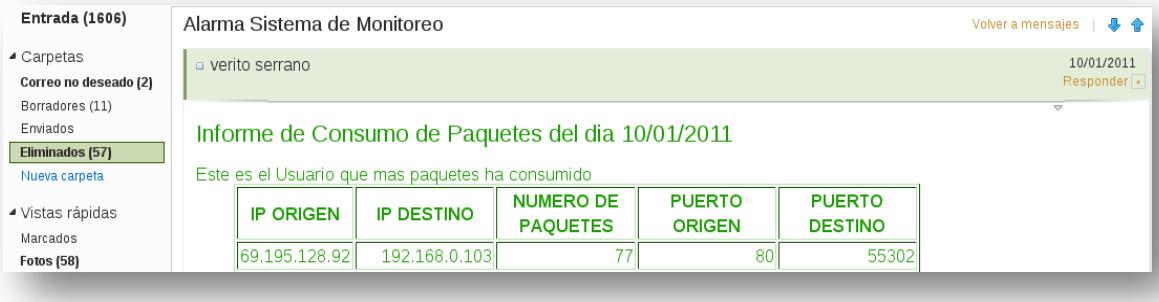
Luego se presenta una ventana con los pasos para configurar Postfix y si da clic en Para mayor información clic aquí: este lo llevara a una página más detallada sobre la configuración de Postfix.

En esta ventana también existe un botón Activar Alarma que permitirá que el administrador reciba todos los días a las 5 de la tarde un reporte de la IP que mayor consumo de ancho de banda tuvo en el día.





En su mail debe llegar un mensaje tal como se muestra:

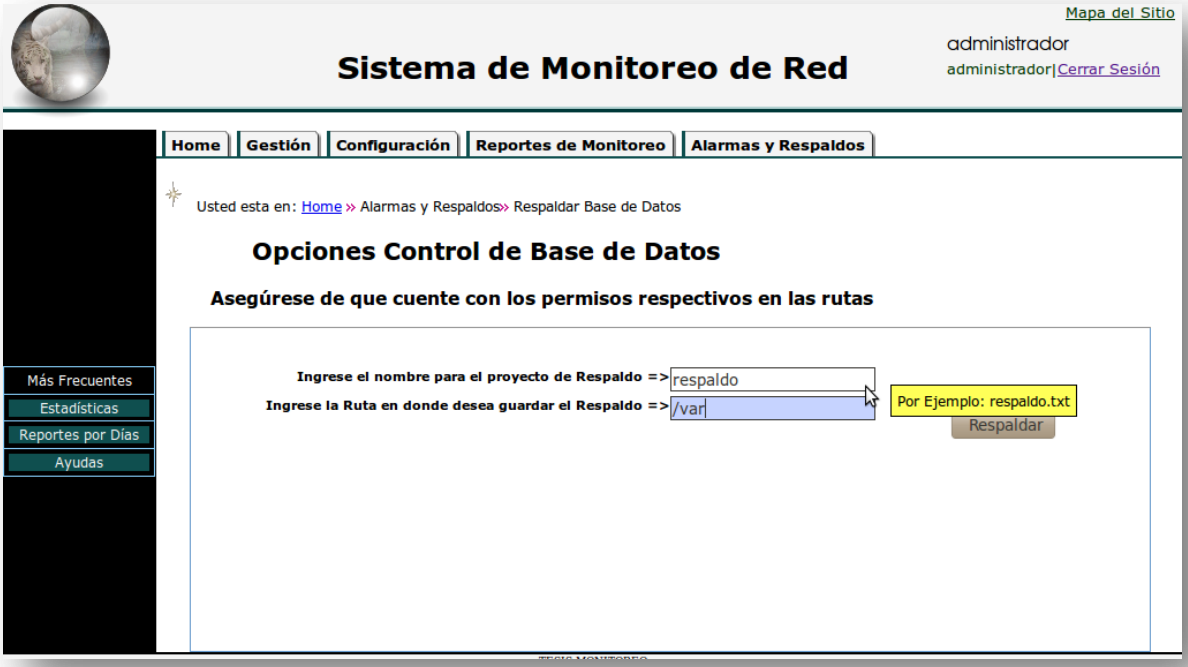


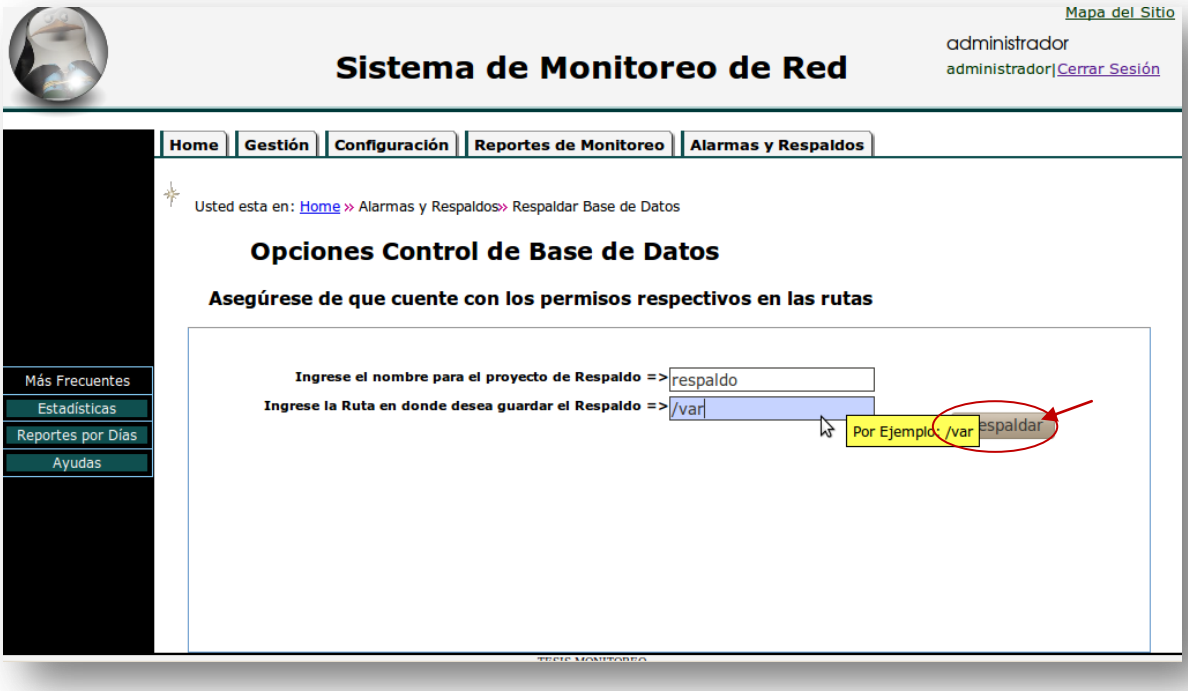
17. Para configurar los respaldos de los flujos que están almacenados dentro de la Base de Datos de clic en Alarmas y Respaldos, Respaldar y Limpiar BD.

Para realizar los respaldos de la Base de Datos usted debe dar permisos a la ruta donde va a importar su base de datos, siendo recomendable no respaldar en la carpeta /root/. Para dar permisos lo puede hacer con el comando:

```
chmod 777 /ruta_del_respaldo
```

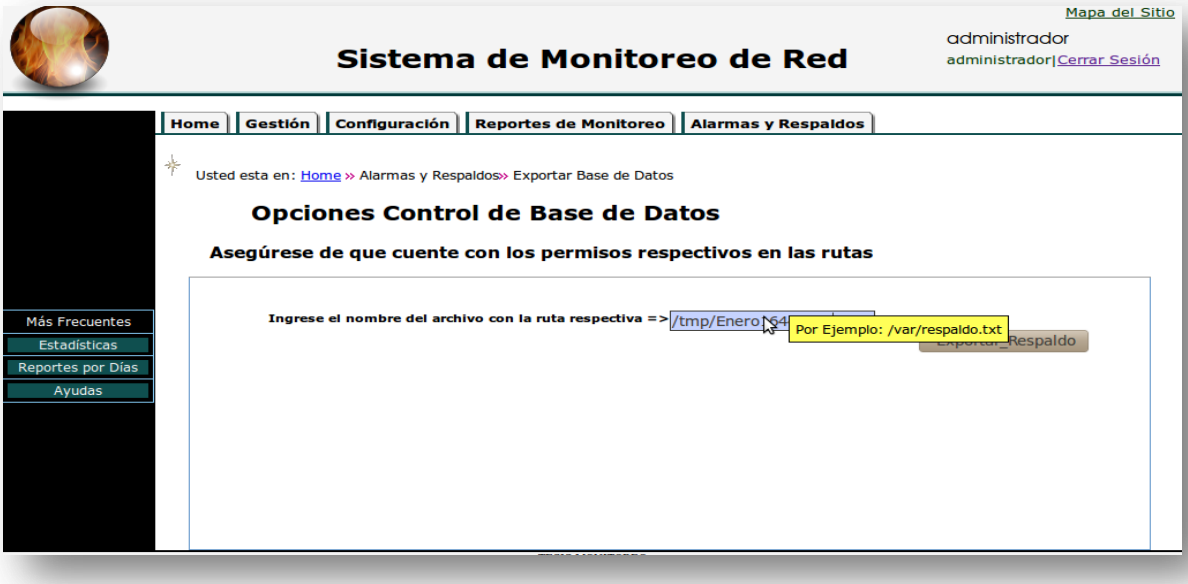
Posteriormente ingrese el nombre del proyecto y la ruta donde desea guardar dicho respaldo y pulse el botón Respaldar.



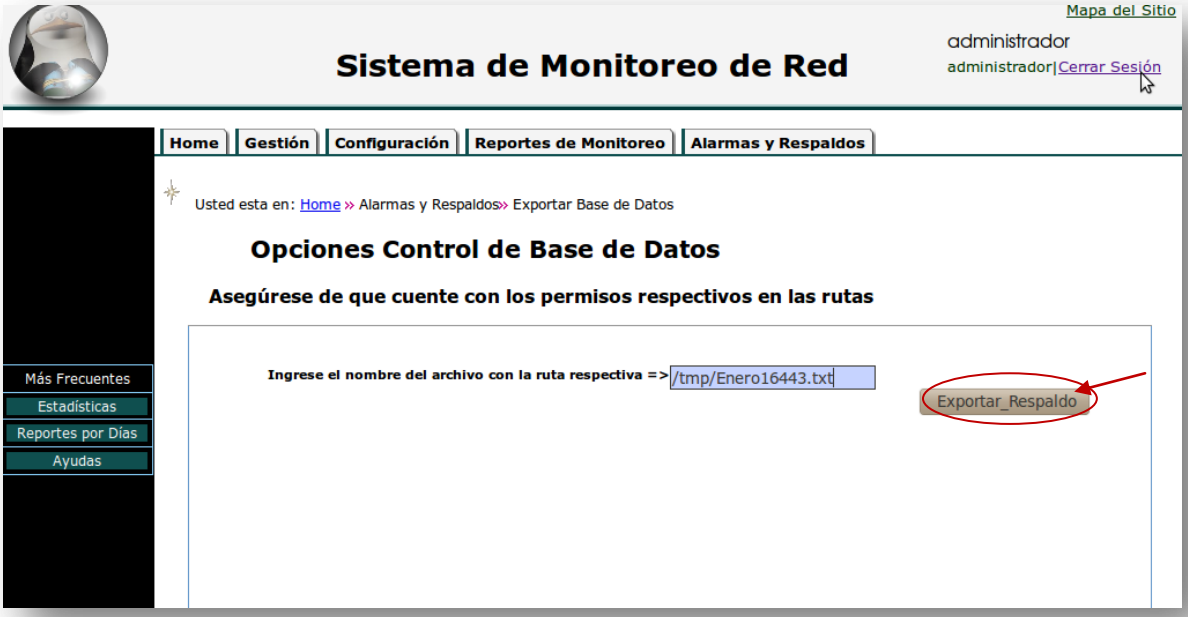


18. Si usted desea exportar desde un archivo de texto a la Base de Datos del sistema para consultar reportes a fechas anteriores de las existentes en la base, de clic en Alarmas y Respaldos en Exportar y Cargar Base.

Primero de permisos necesarios al archivo.txt y luego proceda a ingresar la ruta donde se encuentra el archivo con los flujos listos para ser exportados a la base de Datos del Sistema. Pero antes verifique si tiene el espacio suficiente para realizar dicha exportación.



Por último pulse en el botón Exportar_Respaldo.



Además si usted da clic dentro de Más Frecuentes en Estadísticas y Reportes por Días, usted esta accediendo de manera directa a estos Reportes. Pero si da clic en Ayudas este le conducirá a nuestro enlace web:

http://tesismonitoreo.byethost17.com/

La misma que contiene el instalador junto con los manuales de Usuario.

BIBLIOGRAFIA

Direccionamiento IPV4:
Universidad Nacional de Luján – Asignatura Teleinformática y Redes, "Direccionamiento IP",http://www.unlu.edu.ar/~tyr/tyr/TYR-2003/TYR-2003-DireccionamientoIP.pdf

Historia de la Internet:
es.wikipedia.org/wiki/Historia_de_Internet
Modelo OSI: FOROUZAN, BEHROUZ A.; COOMBS, CATHERINE; CHUNG FEGAN, SOPHIA, Transmisión de datos y redes de comunicaciones
http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/ip.htm
http://r_marca.pe.tripod.com/pagina1.htm
http://www.unicrom.com/Art_historia_internet.asp
http://www.krqd.com/tcpip.htm
http://docente.ucol.mx/al979604/public_html/ORIGEN%20DEL%20TCP.html
http://es.wikipedia.org/wiki/Historia_de_Internet

Cabecera IP:
http://f34k.files.wordpress.com/2008/01/microsoft-word-cabecera-ip.pdf

Entorno Cliente- Servidor:
http://fmc.axarnet.es/redes/tema_08.htm, http://es.wikipedia.org/wiki/Cliente-servidor

POP3:
http://es.wikipedia.org/wiki/Correo_electr%C3%B3nico

TCP:
El PROTOCOLO TCP, "Capítulo 4",
http://bibing.us.es/proyectos/abreproy/11306/fichero/TEORIA%252F09+-+Capitulo+4.pdf

SOCKETS:
http://www.masadelante.com/faqs/socket,
http://www.it.uniovi.es/docencia/GestionGijon/redes/Redes-Practica1-4.pdf

POP y SMTP:
http://danderesi.wordpress.com/2007/12/04/pop3-y-smtp/

IPV6:
http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

Define la Internet:
http://www.abcpedia.com/diccionario/definicion-internet.html
http://www.angelfire.com/ak5/internet0/
http://es.wikipedia.org/wiki/Internet
http://nti.uji.es/docs/nti/impiva.html

Define TCP-IP:
http://www.masadelante.com/faqs/tcp-ip
http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
http://technet.microsoft.com/es-es/library/cc787677(WS.10).aspx
http://www.definicionabc.com/tecnologia/tcpip.php
http://www.mastermagazine.info/termino/6829.php
http://definicion.de/tcp-ip/

Modelo OSI:
http://es.wikipedia.org/wiki/Modelo_OSI

Tipos de Conexión:
http://www.isftic.mepsyd.es/w3/programa/usuarios/ayudas/tipo_conexion.htm#adsl
http://www.alegsa.com.ar/Notas/135.php
http://es.wikipedia.org/wiki/TCP_IP
http://www.alfinal.com/Temas/tcpip.php

Ancho de banda
http://es.wikipedia.org/wiki/Ancho_de_banda
http://www.mastermagazine.info/termino/3854.php
http://www.masadelante.com/faqs/ancho-de-banda

Banda base:
http://es.wikipedia.org/wiki/Banda_base
http://www.textoscientificos.com/redes/senales/banda-base
http://www.mailxmail.com/curso-conceptos-basicos-redes/banda-base-banda-ancha
http://www.monografias.com/trabajos17/medios-de-transmision/medios-de-transmision.shtml
http://fmc.axarnet.es/redes/tema_07.htm

Inalámbrica:
http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica

ASO:
http://es.wikipedia.org/wiki/Organismo_de_Soporte_a_Direcciones_(ASO)
http://lacnic.net/documentos/lac/factsheet-sp.pdf
http://es.wikipedia.org/wiki/ICANN
http://es.wikipedia.org/wiki/Conmutador_(dispositivo_de_red)

ISP
http://www.itu.int/ITU-T/special-projects/ip-policy/final/IPPolicyHandbook-S.pdf
http://beta.redes-linux.com/manuales/routing/PIAM-Routing-Peering-v3.pdf
http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/1432/5/T11388%20CAP%201.pdf
http://dspace.epn.edu.ec/bitstream/123456789/751/3/T10506CAP1.pdf

Herramientas de Monitoreo:

http://wiki.gacq.com/index.php/Flowscan

OTROS:

STALLINGS, WILLIAM, Comunicaciones y redes de computadores/ Pearson Educación. Madrid. 6a. edición. 2000. 747 p. ilus
http://www.dante.net/upload/pdf/flowviz_MM-v2.pdf
http://explorer.cekli.com/articles/pdf/netflow-ipfix
http://tools.ietf.org/html/rfc1157.
snmp/gestion-de-redes.htm
http://es.wikipedia.org/wiki/SNMP
http://www.unix.com/es/unix-dummies-questions-answers/96904-linux-rrdtool-help-create-graph.html
http://www.netinst.com/assets/pdf/observerprodfamily_B.pdf
http://f34k.files.wordpress.com/2008/01/microsoft-word-cabecera-ip.pdf
http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf
http://www.insoftweb.com/contapyme/modulos/herramientas/generadordereportes/default.htm
http://www.bibliociencias.cu/gsdl/collect/eventos/index/assoc/HASH010e.dir/doc.pdf
http://www.e-deanetworks.com/web_documents/NTA_Datasheet_0408.pdf
http://www.unlu.edu.ar/~tyr/tyr/TYR-2003/TYR-2003-DireccionamientoIP.pdf
http://es.kioskea.net/contents/utile/fai.php3
http://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet
http://autogestion.ciudad.com.ar/ciudad/descargas/manuales/Manual_Funcionamiento_ISP.pdf
http://beta.redes-linux.com/manuales/routing/PIAM-Routing-Peering-v3.pdf
http://www.netopen.es/sistemas/subsecciones/InterISP.htm
http://es.wikitel.info/wiki/Gesti%C3%B3n_del_tr%C3%A1fico_en_Internet