ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA INFORMÁTICA

DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE SWITCH CAPA 3 BÁSICO BASADO EN LINUX

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO INFORMÁTICO MENCIÓN REDES

BAYRON ALEXANDER TOAPANTA BANDA

MARCELA GENOVEVA CEVALLOS GUAMBO

DIRECTOR: ING. PABLO RECALDE.

Quito, Marzo 2006

DECLARACIÓN

Nosotros, Bayron Alexander Toapanta Banda, Marcela Genoveva Cevallos Guambo, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

BAYRON ALEXANDER TOAPANTA BANDA

MARCELA GENOVEVA CEVALLOS GUAMBO

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Bayron Alexander Toapanta Banda y Marcela Genoveva Cevallos Guambo bajo mi supervisión.

Ing. Pablo Recalde

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Ante todo a Jehová Dios por darnos la vida, salud y energías, para enfrentarnos al mundo en que vivimos tan conflictivo y materialista, además que solicitamos nos siga proveyendo de nuestras necesidades tanto espirituales como materiales.

A nuestros familiares por apoyarnos y soportar todas las molestias que les causamos, mientras desarrollamos esta tesis pero a pesar de todo siguieron firmes en su apoyo.

A la Escuela Politécnica Nacional, por darnos la oportunidad de seguir incrementando nuestros conocimientos y llegar a convertirnos en profesionales.

Al nuestro amigo el Sr. Ing. Pablo Recalde, por ser un excelente Director de Tesis, al compartir con nosotros sus amplios conocimientos y experiencias, y así llegar al exitoso termino de este proyecto.

DEDICATORIA

Dedico todo mi esfuerzo, a mi Dios Jehová en especial, esposa y mis 2 hijas, mis padres, hermanos y amigos, en la realización y culminación de esta tesis, ya que Uds. son los motivos que me impulsaron a realizar esta meta.

Deseo de todo corazón nunca defraudarlos y de aquí en adelante trabajaré arduamente en el bienestar espiritual de mi familia, en compensación por todo el tiempo que los descuide mientras realizaba este proyecto.

Los ama
Bayron

La vida es hermosa, lo es aun más cuando hay logros que alcanzas con esfuerzo y compartes con las personas que mas necesitan de ti, dedico este trabajo a mi Padre Dios por haberme dado la oportunidad de estar escribiendo estas líneas, a mi querida Madre que es la persona más importante que tengo y es el principal apoyo para culminar esta carrera profesional, a mis tres hermanos por su colaboración y paciencia, espero de alguna manera contribuir su ayuda, los quiero.

Marcela

CONTENIDO

LISTADO DE GRÁFICOS

LISTADO DE TABLAS

LISTADO DE SCRIPTS

LISTA DE ABREVIACIONES Y SIMBOLOS

A

ACL : Listas de Control de Acceso (Access Control List)

ARP : Protocolo de Resolución de Direcciones (Address Resolution Protocol)

ATM : Modo de Transferencia Asincrónica (Asynchronous Transfer Mode)

AS : Sistema Autónomo (Autonomous System)

B

BGP : Protocolo Compuerta de Frontera (Border Gateway Protocol)

C

CRC : Chequeo de Redundancia Cíclica (Cyclic Redundancy Check)

CSMA/CD : Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones (Carrier Sense and Multiple Access with Collition Detection)

D

DARPA : Agencia de proyectos de investigacion avanzados para la defense (Defense Advanced Research Projects Agency)

DCN : Red de Computadoras Distribuidas (Distributed Computer Network)

DHCP :Protocolo de Configuración Dinámica de Host (Dinamic Host Configuration Protocol)

DNS : Sistema de Nombre de Dominio (Domain Name System)

E

EGP : Protocolo de Compuerta Exterior (Exterior Gateway Protocol)

F

FDDI : Interface de Datos Distribuida por Fibra (Fiber Distributed Data Interface)

FQDN : Nombre de Dominio Completamente Expresado (Full Qualify Domain Name)

FR : Frame Relay

FTP : Protocolo de Transferencia de Archivos (File Transfer Protocol)

H

HTTP : Protocolo de Transferencia de Hypertexto (Hypertext Transfer Protocol)

I

ICMP : Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol)

IEEE : Instituto de Ingenieros Eléctricos y Electrónicos (Institute Engineers Electrical and Electronic)

IGMP : Protocolo de Administración de Grupos de Internet (Internet Group Management Protocol)

IGP : Protocolo de Compuerta Interior (Interior Gateway Protocol)

InterNIC : Centro de Información de Red de Internet (Internet Network Information Center)

IP : Protocolo de Internet (Internet Protocol)

IPX : Intercambio de Paquetes por Internet (Internet Packet Exchange)

ISDN : Red Digital de Servicios Integrados (Integrated Service Digital Network)

ISO : Organización Internacional de Estándares (Internacional Standar Organization)

L

LAN : Red de Área Local (Local Area Network)

LLC : Control de Enlace Lógico (Logical Link Control)

M

MAC : Control de Acceso al Medio (Medium Access Control)

MAN : Red de Área Metropolitana (Metropolitan Area Network)

MTU : Unidad de Transferencia Máxima (Maximium Transmission Unit)

N

NAP : Protocolo de Adquisición Vecina (Neighbor Acquisition Protocol)

NIC : Conector de Interface de red (Network Interface Connector)

NR : Neighbor Reachability

O

OSI : Interconexión de Sistemas Abiertos (Open System Interconnection)

OSPF : Primer Sendero Abierto mas Corto (Open Shortest Path First)

P

PMTU : Unidad de Transferencia Máxima por Trayectoria (Path Maximun Transfer Unit)

PHP : Lenguage Prosesador Hypertexto (Hypertext Preprocessor)

PPP : Protocolo Punto a Punto (Point to Point Protocol)

R

RARP : Protocolo de Resolución de Direcciones en forma Reversa (Reverse Address Resolution Protocol)

RFC : Petición de Comentarios (Request For Comments)

RIP : Protocolo de Información de Ruteo (Routing Information Protocol)

S

SLIP : Protocolo de Enlace Internet en Serie (Serie Link Internet Protocol)

SMTP : Protocolo de Transferencia de Correo Simple (Simple Mail Transfer Protocol)

SQL : Lenguage de Consultas Estructuradas (Structure Query Language)

T

TCP : Protocolo de control de transporte (Transport Control Protocol)

TELNET : Protocolo de emulación de terminal

TFTP : Protocolo de Transferencia de Archivos Triviales (Trivial File Transfer Protocol)

TTL : Tiempo de Vida (Time To Live)

U

UDP : Protocolo de Datagramas de Usuario (User Datagram Protocol)

V

VLSM : Máscara de Subred de Longitud Variable (Variable Length Subnet Mask)

W

WAN : Red de Área Amplia (Wide Area Network)

X

XML : Lenguaje de Marcado Extensible (Extended Marked Language)

RESUMEN

El presente proyecto de tesis esta orientado a solventar los inconvenientes que atraviesan las empresas pequeñas y medianas en lo referente a la incorporación de dispositivos de alta tecnología, en sus redes de datos, que mejoren los problemas de dominios de colisión por medio de switch capa 3 comerciales de marcas prestigiosas reconocidas, debido a que estos son costosos tanto en sentido compra de equipos como en adiestramiento de personal técnico.

La solución que se presenta en este tema de tesis es la implementación de una simulación de switch capa 3 básico mediante el sistema operativo Linux, por medio de elementos y dispositivos de red básicos (bajos costos), y software de adquisición libre, reduciendo de esta manera el costo total del proyecto.

El switch aquí propuesto esta formado por 3 tarjetas de red, que se incorporan dentro de una PC común y corriente, que sirven para crear y administrar subredes al igual que cualquier otro switch capa 3 comercial, además que una de estas subredes es una VLAN móvil (usuarios móviles) a través de todas las interfases de red.

El administrador tiene la opción de crear 3 diferentes subredes, las cuales pueden o no usar la tecnología subneting en cada una de ellas.

El prototipo de switch básico capa 3 utiliza un servidor DHCP con técnica multi-scope, para proporcionar direcciones IP a sus clientes y en base a esta acción asignar al usuario a la VLAN correspondiente.

Adicionalmente se ha incorporado un servidor DNS, como ayuda del switch básico capa 3, para identificar a un host por medio de su FQDN (Nombre de Dominio Completamente Cualificado), sin importar a que subred esta asignado en ese instante.

Como en toda red de datos es indispensable enrutar paquetes y manejar reglas de seguridad, el prototipo de switch básico capa 3 tiene incorporado un Firewall básico.

Todo los antes mencionado, el administrador de la red las puede modificar, por medio de una interfaz de aplicación, en forma gráfica.

PRESENTACIÓN

Este proyecto de titulación se ha elaborado con el propósito de brindar una solución alternativa, a las empresas medianas y pequeñas, en la compra de un dispositivo electrónico de red que solucione los problemas de dominios colisión y la creación de redes virtuales sin necesidad de entrar en gastos elevados.

La solución aquí descrita es la implementación de un switch básico capa 3 basado en el sistema operativo Linux, el mismo que fue realizado de acuerdo a una secuencia ordenada de etapas según se iba desarrollando el proyecto de tesis planteado.

El trabajo comienza con un breve resumen de porque se crea este dispositivo lógico de red y después se describe el funcionamiento del mismo.

El primer capítulo consta de un marco teórico sobre conceptos de redes de computadores el cual incluye características de TCP/IP, asignación dinámica de direcciones IP, así como también el funcionamiento del switch y router.

El segundo capítulo constituye el desarrollo del prototipo de switch básico capa 3 basado en Linux., en el que se inicia con un análisis de requerimientos de hardware y software necesarios para la implementación del mismo, a continuación se plantea un diseño de cómo debe estar estructurado el switch capa 3 y la función que este debe realizar, y por último se realiza una explicación detallada de su implementación.

En el capítulo tres se realiza un análisis costo-beneficio sobre aspectos técnicos, económicos, legales y operativos de acuerdo a la realidad nacional actual.

Como último capítulo se presentan las conclusiones y recomendaciones obtenidas a lo largo del desarrollo del proyecto. Al final de los capítulos se encuentra un anexo el cual describe el funcionamiento de la interfaz de aplicación.

CAPITULO I

MARCO TEORICO

1.1 REDES DE COMPUTADORAS

1.1.1 ¿QUÉ ES UNA RED?

"Es un conjunto de por lo menos dos ordenadores interconectados entre si a través de medios físicos de interconexión pueden ser por cable coaxial, fibra óptica, inalámbrica, enlaces satelitales, etc, y dispositivos electrónicos de conexión, que pueden ser módems, hubs, routers, switchs, Firewalls, etc, para de esta manera poder compartir información, reducir costos, aumentar/mantener el rendimiento acorde con la carga, etc. Existen varios tipos de informaciones que pueden los ordenadores intercambiarse, entre estas se tiene: correo electrónico, archivos, videos, música, imágenes, etc. De igual forma, los medios físicos[1]".

1.1.2 MODELO OSI

"A este modelo se lo conoce como modelo de referencia OSI (*Open System Interconnetion*, interconexión de sistemas abiertos). Fue creado por la Organización Internacional de Normas (ISO)[2]", con el fin de estandarizar los protocolos que se utilizan en la creación de nuevas redes por parte de los diseñadores.

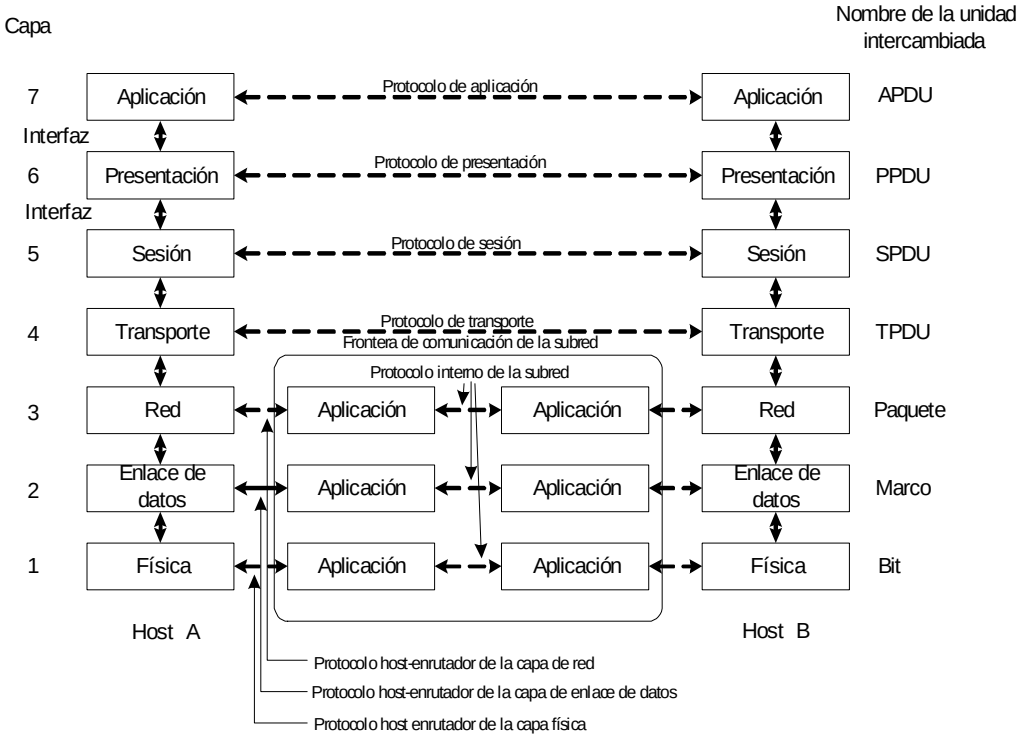
---

[1] SAMANIEGO, Gustavo, Apuntes de Redes de Computadores, Redes de Computadoras. Quito. 16/05/2003. Páginas: 1,2.

[2] SAMANIEGO, Gustavo, Apuntes de Redes de Computadores, Modelo de Referencia OSI. Quito. 16/05/2003. Páginas: 6.

La pila del modelo OSI esta compuesto por siete capas, cada una de estas tiene una función bien definida y también se relaciona con sus capas inmediatas a través de interfaces también bien definidas.

GRÁFICO 1. 1
MODELO DE REFERENCIA OSI



FUENTE: SAMANIEGO, Gustavo. Apuntes de redes de computadoras. 2003, página 7

1.1.2.1 La capa física

La capa física comprende todo lo relacionado con los medios por donde los bits viajan de un host a otro, es decir el canal de transmisión. En esta capa se toma en cuenta los estilos de diseño, cuantos voltios debe usarse para representar el valor de 1 y el valor de 0, el tiempo de duración del valor 1 así como del valor 0, la seguridad de que los bits que van de un host a otro lleguen no se corrompan, el número de pines que tendrá el conector de la red, así como su identificación, en otras palabras, en la capa física se determina que el diseño de las interfaces tanto eléctricas, mecánicas y topológicas.

1.1.2.2 La capa de enlace de datos

Los datos que llegan en bruto desde la capa física se descomponen en segmentos llamados marcos de datos, con el fin de transformarlos en una línea que parezca libre de errores de transmisión para la capa de red. Estos marcos de datos son de unos cientos o miles de datos y van en forma secuencial, también generan marcos de acuse de recibo que se las envía al receptor con el fin de confirmar que un marco de dato a llegado de lo contrario este se lo reenviara por parte del transmisor hasta que el acuse de recibe confirme su llegada.

Los marcos de datos pueden sufrir daños por diversas circunstancias en el trayecto, y esta capa es la que debe resolver el problema y otros más como son los marcos perdidos, los duplicados, regulación del tráfico, control del acceso al canal compartido en el caso de redes de difusión, así como el problema de que el tráfico de datos viajen en ambas direcciones.

1.1.2.3 La capa de red

En el gráfico 1-1 se ve que existe la “Frontera de comunicación con la subred” y la capa de red es la encargada de controlar el funcionamiento de ésta. El encaminamiento de los datos desde la fuente al destino puede ser por medio de tablas estáticas que se interconectan a la red y rara vez cambian o dinámicas por medio de nuevos paquetes que reflejan la carga actual de la red.

Esta capa es la que determina el inicio de cada conversación y se encargan del control de congestión de datos con el fin de evitar los cuellos de botella, logrando así enviar los paquetes de nodo a nodo usando un circuito virtual o datagramas.

Otra de las funciones de la capa de red consiste en dividir los mensajes de la capa de transporte (segmentos) en unidades más complejas, denominadas paquetes, a los cuales se les asigna direcciones lógicas de los host que se encuentran comunicando, con la finalidad de encaminar la información a través de la red en base a las direcciones del paquete, los métodos de conmutación y enrutamiento.

A la capa de red también le corresponde resolver los problemas de interconexión de redes heterogéneas: todos los hots tendrán un identificador a nivel de capa de red (conocidos en internet como direcciones IP) independientemente de las redes que tengan en las capas inferiores.

En esta capa trabajan los ruteadores, dispositivos que se encargan de encaminar o dirigir los paquetes de datos desde el host origen hasta el host destino a través de la mejor ruta posible entre ellos.

1.1.2.4 La capa de transporte

La función de esta capa es asegurarse que los segmentos de datos (“mensajes”) lleguen de un host origen a un host destino, asignándoles números de secuencia para asegurarse que los host receptores vuelvan a unir los datos en el orden correcto antes de enviarlos a la capa de red.

Esta capa también crea conexiones de red distintas por cada conexión de transporte que la capa de sesión las necesite, pero si el volumen de transmisión de datos es alto, la capa de transporte puede crear múltiples conexiones de red. Esta capa también tiene la potestad de multiplexar varias conexiones de transporte en la misma conexión de red, en el caso de que el costo de creación de una conexión sea elevado.

Además la capa de transporte debe dar el mecanismo de “control de flujo” a fin de que el receptor no llegue a saturarse de información que le este llegando del host transmisor, asegurando que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo.

La capa de transporte se encarga de lograr una transferencia de datos segura y un transporte confiable de datos entre los nodos de la red, ocultando los detalles a las capas superiores, para esto la capa de transporte establece, mantiene y termina adecuadamente las conexiones que se establecen dentro de una red,

proporcionando un servicio confiable mediante el uso de sistemas de detección y recuperación de errores de transporte.

Incluye controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones.

1.1.2.5 La capa de sesión

Esta capa permite establecer sesiones[3] entre usuarios que tengan máquinas diferentes. Además proporciona servicios mejorados a la capa de transporte como por ejemplo el manejo del control de diálogo, es decir, que este puede permitir el tráfico de datos en un sentido o ambos a la vez.

Otro servicio es el agrupamiento, en el cual se marcan los datos para definir grupos con propósitos diferentes.

La capa de sesión da el servicio de creación de puntos de sincronismo con el fin de recuperar transferencias largas de datos fallidas.

1.1.2.6 La capa de presentación

Esta capa se encarga de la sintaxis y semántica de la información que se envía. También codifica los datos que le llega de la capa de aplicación a una forma estándar acordada, con el propósito de que diferentes computadores puedan interpretar textos y números de forma única y correcta.

1.1.2.7 La capa de aplicación

En esta capa se encuentran localizados los protocolos[4] y programas que el usuario utiliza para comunicarse con la red, como también el software que resolverá la incompatibilidad de terminales de todo el mundo llamado *"terminal virtual de red"* mediante el cual será posible el envío de correo electrónico, transferencia de archivos y otros servicios.

---

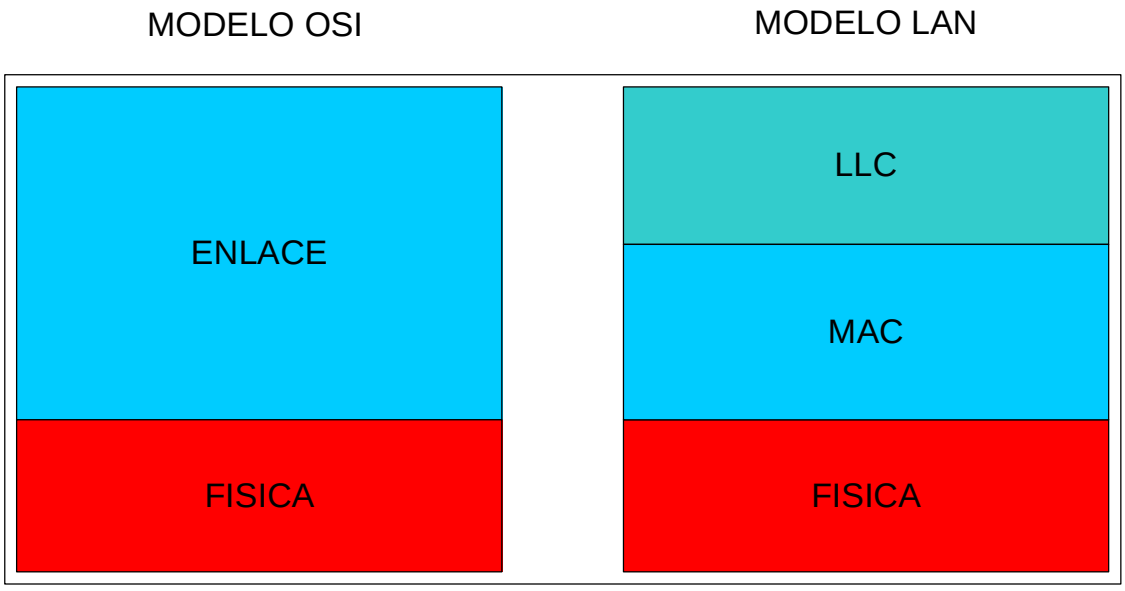
[3] Sesión es un programa de negociación y establecimiento de conexión con otro nodo.
[4] Entre los protocolos de la capa de aplicación se tiene: HTTP, FTP, TELNET, etc.

1.1.3 ESTANDARIZACIÓN DE LAS LAN`S

Las redes de área local (LAN abreviación del inglés “Local Area Network”) son utilizadas para cubrir áreas relativamente pequeñas, aproximadamente no exceden 1 Km. de extensión, con el único propósito de compartir recursos caros (discos, impresoras, etc) y datos entre los usuarios. La longitud máxima de esta red es de 500 a 1000 metros según la topología. Existen dos tipos básicos de redes LAN: Ethernet (bus lógico) y Token Ring (anillo lógico). La norma IEEE[5] 802 es la especificación para las redes LAN.

El modelo de redes LAN es de tres capas pero para el modelo OSI solo se toma las dos primeras capas. La capa inferior coincide con la de OSI o sea la capa física, la superior es la capa de enlace pero para el modelo OSI ésta la subdivide en dos subcapas: La inferior se llama subcapa MAC (Medium Access Control) y la subcapa superior llamada LLC (Logical Link Control).

GRÁFICO 1. 2
COMPARACIÓN DE LOS MODELOS OSI Y LAN



FUENTE: LOPEZ, Mariano. Teoría de las redes informáticas. http://www.redesafull.com.ar/outline.js. Acceso último: 06/04/2005

[5] Ver lista de abreviaturas

El motivo de separación de las dos subcapas es porque la administración del acceso a un medio compartido no se lo realiza en el control de enlace tradicional de la capa 2 y porque para un mismo LLC se puede proveer varias opciones de MAC.

1.1.3.1 Subcapa LLC

Son algunas las funciones que realiza esta subcapa, entre ellas es mantener el enlace, sincronizar las tramas, establecer una comunicación del tipo sin conexión y no confiable entre las terminales, el control de errores mediante el código de redundancia cíclica (CRC) y la confirmación de frames recibidos. Esta labor la cumple tanto para una red Ethernet como para una Token Ring.

1.1.3.2 Subcapa MAC

Como se observa es parte de la capa de enlace según el modelo OSI y entre las funciones que debe realizar esta subcapa es, controlar cómo los dispositivos que conforman la red podrán acceder al medio, haciendo esto la diferencia entre una red Ethernet de una Token Ring o Token Bus.
Esta subcapa también tiene la posibilidad de identificar a cada elemento que esta en la red mediante el direccionamiento, detectar errores y descartar frames con error, y delimitar las frames.

1.1.4 REDES LAN VIRTUALES (VLAN)

1.1.4.1 Resumen histórico

"Debido a la creciente necesidad de ancho de banda, por el incremento de usuarios en la red y los nuevos modelos de aplicaciones multimedia, los mayores distribuidores de equipamientos de redes de área local (LAN) conmutadas, propusieron un conjunto de soluciones llamadas redes de área local virtuales (VLAN´s), con el fin de añadir funciones de conmutación y software de gestión más avanzadas. Este desarrollo comenzó en 1994/1995[6]".

[6] ANÓNIMO. Redes Virtuales (vLANs): Un nuevo concepto en Redes Computacionales. http://www.ibw.com.ni/~alanb/tecno/thpage.htm. Acceso último: 01/06/2005.

Con el fin de aumentar el ancho de banda disponible para cada usuario en una LAN, basada en el compartir ancho de banda, se suele optar por la segmentación de sus segmentos y anillos, pero esto trae consigo dificultades en la gestión de la red, debido a que cada segmento suele contener un promedio de 30 a 100 usuarios.

Para poder superar este inconveniente y aumentar el ancho de banda cuantiosamente a cada usuario, se utiliza LAN´s basadas en conmutación, ya que mediante esta técnica cada computador, posee una conexión dedicada dentro de la red al dispositivo de concentración.

En una LAN conmutada la función tradicional del router lo pasa a realizar el conmutador LAN, quedando aquel a efectuar funciones de gestor de red, con lo que se consigue contener de 100 a 500 usuarios.

Mediante la utilización de los conmutadores junto con las VLAN´s, se logra que cada segmento de red contenga como mínimo un usuario, mientras tanto que los dominios de broadcast pueden contener 1000 usuarios o más.

1.1.4.2 Definición de una VLAN

Es la agrupación lógica de estaciones de trabajo que se comunican entre si, como si estuvieran conectados al mismo cable, con el fin de formar segmentos diferentes de red, sin necesidad de que estos segmentos se encuentren en el mismo edifico o campus, para brindar seguridad al segmento, enrutar información de los usuarios hacia nuevas localizaciones, contención de broadcast al crear segmentos de red más pequeños, aumentar la eficiencia en la gestión de los segmentos de red, proporcionar escalabilidad, etc.

La red virtual permite separar la visión lógica de una red de su estructura física mediante la creación de comunidades de host con un mismo interés, con

definición lógica para la colaboración de sistemas informáticos de redes. La comunicación entre VLAN´s se hace a través del protocolo estándar 802.1Q[7].

Por razón de que existen varias maneras de definir las VLAN´s, estas se las dividen en 5 tipos principales: basadas en puertos, basadas en MAC, VLAN´s de capa 3, VLAN´s basadas en reglas y basadas en DHCP.

1.1.4.3 VLANs Basadas en Puertos (Membership by Port Group)

Las redes virtuales basadas en puertos es el tipo más sencillo ya que un grupo de puertos forma una VLAN, un puerto solo puede pertenecer a una VLAN. Aquí el puerto del switch pertenece a una VLAN, por tanto, ahí alguien posee un servidor conectado a un puerto y este pertenece a la VLAN Z, el servidor estará en la VLAN Z.

Según este esquema, la VLAN consiste en una agrupación de puertos físicos que puede tener lugar sobre un conmutador o también, en algunos casos, sobre varios conmutadores.
Para asignar equipos a una VLAN específica se hace en base a los puertos a los que están conectados físicamente.
A lo largo de la aparición de este tipo de VLANS sus primeras implementaciones podían ser construidas sobre un único conmutador y para definir la pertenencia a la red virtual lo hacían por grupos de puertos, por ejemplo los puertos 1, 2, 3,7 y 8 sobre un conmutador forman la VLAN A, mientras que los puertos 4,5 y 6 forman la VLAN B.

La segunda generación de implementaciones de VLANs basadas en puertos contempla la aparición de múltiples conmutadores, por ejemplo, los puertos 1 y 2 del conmutador 1 y los puertos 4, 5,6 y 7 del conmutador 2 forman la VLAN A; mientras que los puertos 3, 4, 5, 6,7 y 8 del conmutador 1 combinados con los puertos 1, 2,3 y 8 del conmutador 2 configuran la VLAN B.

---

[7] Normativa que la IEEE establece para las redes locales virtuales (VLAN`s)

La agrupación por puertos es todavía el método más común de definir la pertenencia a una VLAN, y su configuración es bastante directa. El definir una red virtual completamente basada en puertos no permite a múltiples VLANs el incluir el mismo segmento físico (o conmutador).
Una de las limitaciones de las VLANs por puertos es que el administrador de la red ha de reconfigurar la VLAN cada vez que un usuario se mueve de un puerto a otro.

1.1.4.4 VLANs basadas en MAC (Membership by MAC address)

Estas redes virtuales se forman mediante la agrupación de estaciones finales en base a sus direcciones MAC (Medium Access Control)[8]. A pesar de que estas se crearon con el fin de superar las limitaciones de las VLANs basadas en puertos, estas presentan ventajas y desventajas.

A este tipo de redes se las conoce también como VLANs orientadas a usuario, debido a que el administrador puede trasladar el host físicamente a otro lugar de la red sin que este pierda su pertenencia a la VLAN, siendo esto una gran ventaja para el administrador.

La desventaja que presentan estas redes, en las cuales existan miles de estaciones de trabajo, es que a todos los usuarios se los debe configurar inicialmente para que estos pertenezcan al menos a una VLAN.

1.1.4.5 VLANs de Capa 3 (Layer 3 Based VLANs)

Para la implementación de estas VLANs, se asocia un grupo de estaciones de trabajo tomando en cuenta el tipo de protocolo o sus direcciones de capa de red.

Al igual que en el caso anterior, estas también presentan ventajas y desventajas, que a continuación se las describe.

---

[8] Es el encargado de proveer el acceso al medio de transmisión por parte de los dispositivos de red.

Para los administradores cuyas estrategias en VLANs están basadas en servicios o aplicaciones, constituye una ventaja que las VLANs permitan particionar por tipo de protocolo. El hecho que los usuarios tengan la posibilidad de mover sus estaciones de trabajo sin que se necesite volver a reconfigurar las direcciones de red, es otro beneficio para el administrador. Estas VLANs reducen el gasto de transporte, puesto que no existe la necesidad de marcar las tramas para que los miembros de la red puedan comunicarse por medio de conmutadores.

La desventaja en estas VLANs es que sus conmutadores son mucho más lentos, debido a que deben inspeccionar direcciones en paquetes en la capa 3 en lugar de buscar direcciones MAC en una trama. Además de tener problemas al tratar con protocolos no enrutables como NetBIOS, tampoco son efectivas para protocolos que implican configuración manual, como por ejemplo: IPX [9] y AppleTalk[10].

1.1.4.6 VLANs basadas en Reglas (Policy Based VLANs)

La implementación de estas VLANs son más potentes y flexibles ya que se las crea en base a combinación de reglas, según las necesidades que tenga el administrador de la red, como por ejemplo: reglas de acceso con el fin de instaurar ciertas seguridades en la red.

1.1.4.7 VLAN por DHCP

En este tipo de Vlan's la dirección IP del computador le entrega automáticamente el servidor DHCP y en base a esta acción asignar al usuario la vlan correspondiente.

1.1.5 DISPOSITIVOS DE CONEXIÓN

Una red puede contener algunos dispositivos de conexión entre ellos se encuentran:

[9] Ver lista de abreviaturas
[10] Arquitectura y protocolos de red de Apple Computer

- **NIC´s (Network Interface Connector).-** Es la que establece la interfaz entre la PC o terminales y el medio físico.

- **REPETIDORES.-** Permiten agregar o insertar segmentos de cableado y son elementos activos ya que su función es amplificar las señales eléctricas, estos trabajan a nivel de la capa 1. La longitud máxima que se puede unir los segmentos de red es de 2.5 Km., esto es 4 repetidores y 5 segmentos de 500 m (regla 5, 4, 3, 2, 1).

- **CONCENTRADORES O HUBS.-** La capa en la que trabaja es la física y es el punto central desde el cual parten los cables hasta los distintos puertos de red, siguiendo una topología de estrella, la velocidad de trabajo es de 10/100 Mbits/s. La información que difunde es broadcast, es decir, que la información que recibe por un puerto lo envía por todos los demás.

- **SWITCHES.-** Prácticamente realizan la misma función que el hub, lo novedoso de este dispositivo es que se le agregó una cierta inteligencia, el cual le sirve para repetir la señal solo a las interfaces necesarias y así evitar las colisiones debido al aumento de trafico innecesario en la red. Otra característica es que los puertos del switch pueden trabajar a la misma velocidad que trabaja la red que la contiene. Los switches trabajan en la capa 2 y 3 dependiendo del nivel de funciones que realicen, para mas detalle de cada uno de estos dirigirse al capítulo 1.4.2 y 1.4.3 respectivamente.

- **BRIDGES O PUENTES.-** Este dispositivo trabaja a nivel de capa 2, interconecta redes de tipo LAN (similares o diferentes) y crear así una sola red LAN lógica, para almacenar y despachar las tramas. Se los considera repetidores selectivos puesto que discrimina el tráfico de las tramas tomando en consideración las direcciones de destino.

- **ROUTERS (Encaminadores).**- Trabajan a nivel de capa 3, tienen la capacidad de filtrar el tráfico de un modo inteligente. Su funcionamiento está basado, en gran medida en la información del protocolo contenida en cada

paquete. Impiden la propagación de las colisiones de unos segmentos a otros de la red. Separan totalmente los segmentos convirtiéndolos en redes lógicas totalmente diferentes, que denominamos subredes, e incluso modifican el contenido de los paquetes retransmitidos. Pueden llegar a transmitir los paquetes a la misma velocidad que a la que circulan por la red y es por eso que se pueden conectar redes con formatos de direccionamiento incompatibles. Estos almacenan y reexpiden paquetes entre redes heterogéneas, esto es, LAN – WAN, MAN – WAM, WAN – WAN. Realizan decisiones de encaminamiento y balanceo de la carga.

- **GATEWAY O PASARELAS.-** Tiene la función de traducir diferentes tipos de protocolos, trabaja en cualquiera o en todas las capas del modelo OSI, pero es preferible que estén en las capas superiores, el inconveniente es que el trabajo lo realiza en forma lenta en comparación con los dispositivos anteriores.

1.2 CONOCIMIENTOS BÁSICOS DE TCP/IP

1.2.1 ORÍGENES DE TCP/IP

Los inicios del protocolo TCP/IP, se basa en un proyecto de investigación realizado a finales de los ’60 en los Estados Unidos, financiado por DARPA, (Defense Advanced Research Projects Agency, o Agencia de Proyectos Avanzados de Investigación en Defensa).

Este proyecto se fundamentó en la investigación de tecnologías de comunicación entre redes de diferentes características y no necesariamente compatibles. Se basaba en la transmisión de paquetes de información, y tenia por objetivo la interconexión de redes, como resultado de esto nacen dos redes una de uso exclusivamente militar denominada MILNET y una de investigación denominada ARPANET, que fue una red experimental, y se convirtió en una red funcional en el año de 1975.

Para lograr que las redes tengan comunicación se desarrollaron varios protocolos. Los protocolos de control de transmisión (TCP) y el protocolo de Internet (IP), este

conjunto de protocolos forman la pila TCP/IP y en el año de 1983 fue adoptado como un estándar para la conexión de una máquina en red.

Finalmente ARPANET creció y se convirtió en lo que ahora se conoce como Internet, llegando a integrarse ella misma a Internet en el año 1990.

El uso de TCP/IP se extendió a nivel mundial a tal punto que compañías empresariales construyen redes TCP/IP, e Internet se le puede considerar como la corriente principal de consumo tecnológico.
Los principales motivos de la popularidad de TCP/IP se deben a la independencia del fabricante, soporta múltiples tecnologías, puede funcionar en máquinas de cualquier tamaño, es un estándar de EEUU desde 1983.

1.2.2 TERMINOLOGÍA DE TCP/IP

TCP son las siglas de Protocolo de Control de Transporte (Transport Control Protocol), e IP de Protocolo de Internet (Internet Protocol), cuando se combinan forman un conjunto de varios protocolos denominados TCP/IP.

1.2.3 DEFINICIÓN TCP/IP

"TCP/IP está definido por un conjunto de protocolos cooperativos y complementarios, los cuales trabajan en conjunto con el objetivo de transmitir información a través del Internet. El conjunto de Protocolos TCP/IP abarca el Protocolo de Control de Transporte e Internet, así como también otros varios"[11].

1.2.4 PROTOCOLOS TCP/IP MÁS COMUNES

A continuación se hace referencia a los protocolos mas comunes del conjunto de protocolos TCP/IP, son su respectivo propósito especificando a que capa del modelo OSI pertenece cada uno.

[11] JAMSA, Kris; COPE, Ken. Programación en Internet. McGraw-Hill. 1996, página 61

Tabla 1. 1 Protocolos
TCP/IP MÁS COMUNES.

Protocolo	Propósito
IP (Protocolo de Internet)	Es un protocolo que pertenece a la capa de Red y su función principal es la entrega de paquetes al host destino. No aporta fiabilidad, control de flujo o recuperación de errores.
TCP (Protocolo de Control de Transporte)	Es un protocolo que pertenece a la capa de Transporte y su función principal es proporcionar una conexión lógica fiable entre parejas procesos. Es un protocolo confiable.
UDP (Protocolo de Datagrama de Usuario)	Es un protocolo que pertenece a la capa de Transporte y se diferencia de TCP es que es menos completo y no es confiable, suministra un mecanismo para que una aplicación envíe un datagrama a otra.
ICMP (Protocolo de Control de Mensajes de Internet)	Es un protocolo que pertenece a la capa de Red y su función principal es llevar mensajes de error de la red y notifica otras condiciones que requieren atención de software de red.

FUENTE: ANONIMO. Redes TCP/IP. http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-087-2-intro.tcpip.html. Ultimo Acceso: 12/06/2005

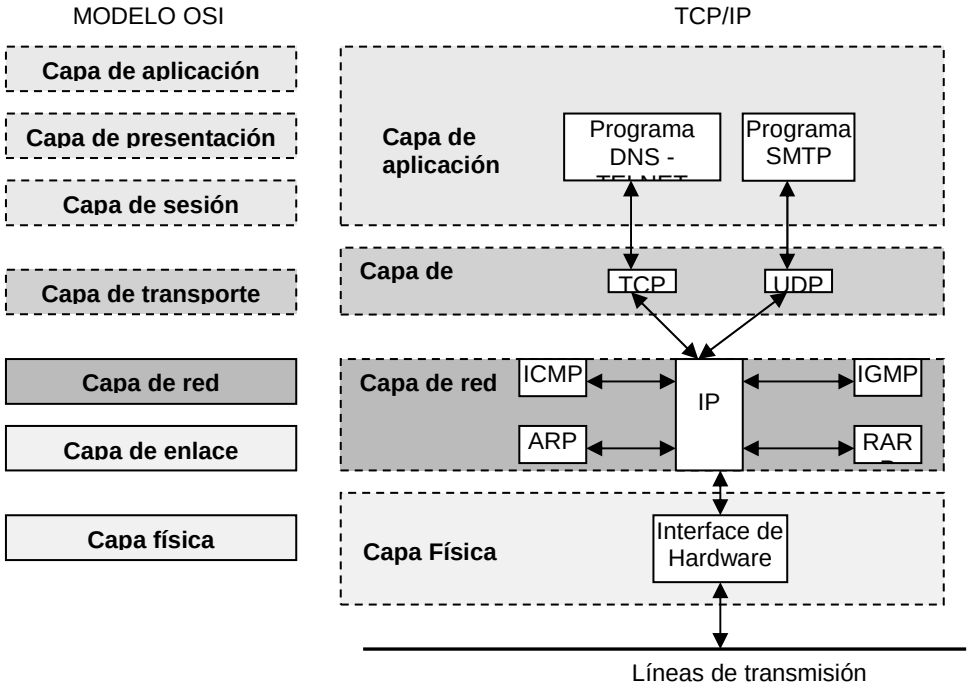
1.2.5 TCP/IP Y OSI

En el capítulo 1.1.2 se detalló el Modelo OSI el mismo que es un modelo referencial que posee siete capas bien definidas, pero en la práctica en el modelo TCP/IP algunas de esas capas se agrupan dividiéndose en cuatro capas las mismas que están distribuidas como se muestra en el gràfico 1.3.

El modelo OSI representa una red como una pila vertical de capas o módulos y asocia a cada capa un protocolo respectivo, en cambio en el modelo TCP/IP un protocolo dado puede ser utilizado por otros protocolos en la misma capa, en este caso el modelo OSI definiría dos capas diferentes. Otra diferencia es que las normas de OSI tienen a ser prescriptivas, es decir que una capa cualquiera tiene que necesariamente pasar por todas las capas que se encuentran debajo de ella, mientras que los protocolos TCP/IP tienen a ser descriptivos, esto implica que se pueden desarrollar programas que eviten pasar por la capa de Transporte y hablen directamente con la de red. Finalmente los protocolos de TCP/IP primero

GRÁFICO 1. 3

MODELO OSI Y LA PILA DE PROTOCOLOS TCP/IP



Fuente: JAMSA, Kris; COPE, Ken. Programación en Internet. McGraw-Hill. 1996, página 62

fueron desarrollados y probados, y posteriormente se describió en un RFC (Request For Comments, documentos informativos), mientras que en el modelo OSI el proceso fue a la inversa.

1.2.5.1 Principales Funciones de cada capa del Modelo TCP/IP

El diseño de Red TCP/IP utiliza cuatro capas del Modelo OSI que son: Capa de Aplicación, Transporte, Red, y Física. A continuación se define brevemente el propósito y función de cada una:

Capa Aplicación.- se relaciona con la capa de aplicación, presentación y sesión del Modelo OSI. Se incluyen protocolos destinados a proporcionar servicios, como por ejemplo transferencia de ficheros (FTP, File Transport Protocol), correo

electrónico (SMTP, Simple Mail Transfer Protocol), conexión remota (TELNET), transferencia de hipertexto (HTTP, Hypertext Transfer Protocol)

Capa de Transporte.- su similar es la capa de transporte del modelo OSI, los protocolos de este nivel, tales como TCP y UDP se encargan de proporcionar a la capa de aplicación un flujo de datos entre máquinas y proporcionar la fiabilidad necesaria en el transporte de los mismos.

Capa de Red.- Se corresponde con la capa de red del modelo OSI, incluye el protocolo IP que se encarga de enviar los paquetes de información a sus destinos correspondientes, es decir se ocupa del movimiento de paquetes por la red, estos paquetes pueden tomar caminos diferentes a su destino y llegar de manera desordenada pero las capas superiores se encargan de reordenarlos. Esta capa se encarga también del ruteo de los paquetes y de evitar la congestión. Define un formato de paquete y el protocolo IP (Protocolo de Internet).

Capa Física.- Esta capa se encarga de transmitir bits por un canal de comunicación y entre sus funciones se encuentran: definir las características físicas y eléctricas, manejar los voltajes y pulsos eléctricos, además de especificar cables, conectores y componentes de interfaz con el medio de transmisión.

1.2.6 ETHERNET 802.3 Y CSMA/CD

Actualmente la mayoría de redes de Área Local utilizan la tecnología Ethernet ya que es la más común y popular debido a que posee un buen balance entre velocidad, costo y facilidad de instalación, esta tecnología se sitúa entre la capa física y de enlace en un red TCP/IP.
El estándar Ethernet está definido por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) como el estándar IEEE 802.3. Este estándar define las reglas para configurar una Ethernet y especifica a su vez como interactúan entre sí los elementos de una red Ethernet.

Para conectar un computador a una red se necesita de un medió físico que me permita realizar un enlace, este medio es una tarjeta de interfase, la cual

pertenece a una tecnología específica. Si se utiliza Ethernet es necesario una tarjeta de interfase Ethernet, si se usa Token Ring de IBM, se emplea una tarjeta de interfase Token Ring, etc.

La tarjeta de interfase se conectará a un cable formando así un enlace del computador con la red. Todas las computadoras de la red mediante la tarjeta de interfase se conectaran al mismo cable y cuando la aplicación envíe información por la red los datos fluirán de una tarjeta a la siguiente. A continuación se menciona las principales características de la tecnología Ethernet:

- Cada tarjeta de interfase Ethernet en una red específica tiene una única dirección. La dirección tiene 6 bytes (48 bits) de longitud y es representada en formato hexadecimal por ejemplo la dirección 52-96-CC-C6-BF-F1.
- A medida que la información fluye por la red, la tecnología Ethernet los encapsula en una trama.
- La trama Ethernet se divide en varios campos ente los cuales tenemos la dirección destino, la dirección origen, los datos en sí y un campo que identifica al tipo de datos.
- Cada tarjeta de interfase Ethernet en la red verifica su dirección en las tramas Ethernet que pasan por el bus de datos. Si es que la dirección destino le corresponde a ese computador entonces recibe la trama para procesarla, caso contrario la descarta.
- Hay una dirección destino especial en hexadecimal FF FF FF FF FF FF, la trama que contenga esta dirección significa que está dirigida a todas las computadoras de la red.
- Las redes Ethernet se implementan con una topología física de estrella y lógica de bus, y se caracterizan por su alto rendimiento a velocidades de 10-100 Mbps.

1.2.6.1 Funcionamiento de la Tecnología Ethernet

El funcionamiento de las redes Ethernet se basa que en cualquier momento las máquinas pueden empezar a transmitir, pero antes de hacerlo escuchan si el canal se encuentra ocupado. En este caso, esperan un tiempo y vuelven a

intentarlo. En el caso en que dos computadoras mediante la tarjeta de interfase transmitan al mismo tiempo los datos se da un choque o colisión. La tecnología Ethernet maneja este tipo de colisiones de esta manera: al momento de detectar una colisión de datos se pide que en un tiempo aleatorio pequeño las dos tarjetas de interfase vuelvan a transmitir, reduciendo la posibilidad de que coincidan nuevamente la transmisión. Este fenómeno se denomina colisión, y la porción de los medios de red donde se producen colisiones se denomina dominio de colisiones. Las máquinas poseen mecanismos de detección de las colisiones y algoritmos de postergación que determinan el momento en que aquellas que han enviado tramas que han sido destruidas por colisiones pueden volver a transmitirlas.

La tecnología Ethernet utiliza el Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA/CD), pues utiliza el acceso aleatorio en el sentido de que no existe un tiempo predecible o calendarizado para que transmita una estación. El orden de transmisión es rotatorio.

El Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA/CD) realiza tres funciones:

1. "Transmitir y recibir paquetes de datos.

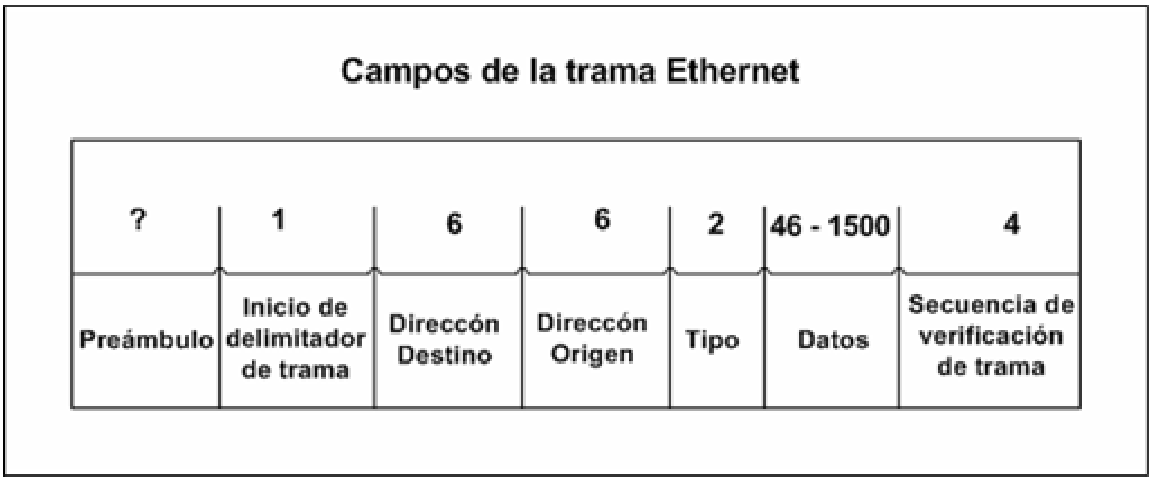
2. Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores.

3. Detectar errores dentro de los paquetes de datos o en la red.[12]"

[12] MORENO, Luciano. Tipos de redes. http://www.htmlweb.net/redes/topologia/topologia_3.html. Acceso último: 13/06/2005.

1.2.6.2 Formato de trama Ethernet

GRÁFICO 1. 4
CAMPOS DE LA TRAMA ETHERNET



Fuente: MORENO, Luciano. Tipos de redes. http://www.htmlweb.net/redes/topologia/topologia_3.html. Acceso último: 13/06/2005.

"**Preámbulo**: Patrón de unos y ceros que indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3. La trama Ethernet incluye un byte adicional que es el equivalente al campo Inicio de Trama (SOF) de la trama IEEE 802.3.

Inicio de trama (SOF): Byte delimitador de IEEE 802.3 que finaliza con dos bits 1 consecutivos, y que sirve para sincronizar las porciones de recepción de trama de todas las estaciones de la red. Este campo se especifica explícitamente en Ethernet.

Direcciones destino y origen: Incluye las direcciones físicas (MAC) únicas de la máquina que envía la trama y de la máquina destino. La dirección origen siempre es una dirección única, mientras que la de destino puede ser de broadcast única (trama enviada a una sola máquina), de broadcast múltiple (trama enviada a un grupo) o de broadcast (trama enviada a todos los nodos).

Tipo (Ethernet): Especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.

Longitud (IEEE 802.3): Indica la cantidad de bytes de datos que sigue este campo.

Datos: Incluye los datos enviados en la trama. En las especificación IEEE 802.3, si los datos no son suficientes para completar una trama mínima de 64 bytes, se insertan bytes de relleno hasta completar ese tamaño (tamaño mínimo de trama). Por su parte, las especificaciones Ethernet versión 2 no especifican ningún relleno, Ethernet espera por lo menos 46 bytes de datos.

Secuencia de verificación de trama (FCS): Contiene un valor de verificación CRC (Control de Redundancia Cíclica) de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas."[13]

"Cuando un paquete es recibido por el destinatario adecuado, les retira la cabecera de Ethernet y el checksum de verificación de la trama, comprueba que los datos corresponden a un mensaje IP y entonces lo pasa a dicho protocolo para que lo procese. El tamaño máximo de los paquetes en las redes Ethernet es de 1500 bytes."[14]

1.2.7 EL PROTOCOLO IP

El Protocolo de Internet (IP) pertenece a la capa de red y su función principal es la entrega de paquetes al host destino. No aporta fiabilidad, control de flujo o recuperación de errores ya que deja que esta situación sea manejada por otras capas.

Existen otros protocolos que sirven de apoyo para el protocolo IP y son el Protocolo de Control de Mensajes de Internet (ICMP, Internet Control Message Protocol) y el Protocolo de Manejo de Grupos de Internet (IGMP, Internet Group Management Protocol), estos protocolos básicamente ayudan a manejar

[13] MORENO, Luciano. Tipos de redes. http://www.htmlweb.net/redes/topologia/topologia_3.html. Acceso último: 13/06/2005.
[14] MORENO, Luciano. Tipos de redes. http://www.htmlweb.net/redes/topologia/topologia_3.html. Acceso último: 13/06/2005.

mensajes especiales de la red, como los de error y transmisiones múltiples. El Protocolo de Resolución de Direcciones (ARP, Address Resolution Protocol) y el Protocolo de Resolución de Direcciones Inverso (RARP, Reverse Address Resolution Protocol), estos protocolos sirven para convertir las direcciones de protocolo de alto nivel (direcciones IP) a direcciones de red físicas (dirección MAC).

1.2.8 LA DIRECCIÓN IP

Una dirección IP es una dirección de Internet que es asignada a cada interfaz de red o host con el objetivo de identificarla en Internet. La dirección IP es administrada por el Centro de Información de Internet (InterNIC, Internet Network Infomation Center) y es única en toda la Internet. Existen actualmente dos versiones de dirección IP, versión 4 de IP (IPv4) y versión 6 de IP (IPv6).

1.2.9 VERSIÓN 4 DE IP (IPv4)

La dirección IP es un número de 32 bits, o 4 bytes, de longitud. Se la puede representar en notación decimal, por conveniencia, ya que se las puede leer con mayor facilidad que la representación binaria, hexadecimal o entera. A continuación un ejemplo de una dirección IP en varias notaciones:

GRÁFICO 1. 5
NOTACIONES DE DIRECCIONES IP

Notación	Dirección IP
Binaria	10000110 00011000 00001000 01000010
Entera	2,249,721,922 (o -2,045,245,374)
Hexadecimal	0x86180842
Decimal	134.24.8.66

Ejemplo de notaciones de direcciones IP

La notación decimal que es la representación más común, se representa cada byte de dirección IP como una serie de números decimales separados por puntos.

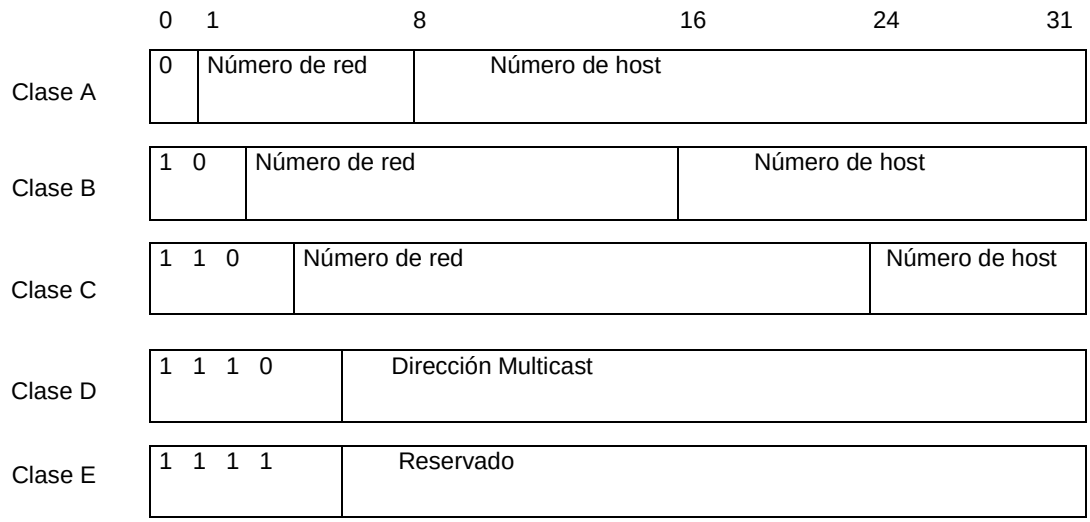
Una dirección IP incluye un número de dirección de red y un número de dirección (asignada a la dirección de host). Los primeros bits del primer byte se utilizan para identificar una clase de dirección, la misma que especifica cuántos bytes utiliza la dirección como número de identificación de dirección de la red.

Internet reserva dos direcciones. Un campo de direcciones que contenga sólo unos representa una dirección de difusión (broadcast), es decir que es un mensaje para todas las computadoras de la red, y una dirección de red que contenga sólo ceros representa a la dirección propia de la red.

1.2.9.1 Clases de Direcciones IP

Existen cinco clases de direcciones IP, como se muestra en el siguiente gráfico:

GRÁFICO 1. 6
CLASES DE DIRECCIONES IP



Fuente: ANÓNIMO. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/. Ultimo Acceso: 20/02/2005.

A cada grupo de dirección de red y grupo de dirección de hosts se resta dos direcciones reservadas la dirección de difusión (que es todo unos) y la dirección de red (que es todo ceros).

Dirección Clase A

Si el primer bit de una dirección IP es 0, ésta dirección pertenece a una red de clase A. Los 7 bits siguientes sirven para el número de identificación de red permitiendo 126 posibles redes. Los restantes 24 bits se emplean para el número de hosts, de tal manera que cada red puede tener hasta 16, 777,214 hosts.

Dirección Clase B

Si los dos primeros bits de una dirección IP son 1 0, ésta es una dirección de clase B. Los 14 bits siguientes sirven para el número de identificación de red permitiendo 16382 posibles redes. Los restantes 16 bits se emplean para el número de hosts, de tal manera que cada red puede tener hasta 65,534 hosts.

Dirección Clase C

Si los tres primeros bits de una dirección IP son 1 1 0, ésta es una dirección de clase C. Los 21 bits siguientes sirven para el número de identificación de red permitiendo 2, 097,150 posibles redes. Los restantes 8 bits se emplean para el número de hosts, de tal manera que cada red puede tener hasta 254 hosts.

Dirección Clase D

Si los cuatro primeros bits de una dirección son 1 1 1 0, ésta pertenece a una dirección reservada especial. El primer byte toma valores entre 224 y 239, estas direcciones son llamadas direcciones de clase D. Se reserva para multicasting[15], usada para direccionar grupos de hosts en un área limitada.

Dirección Clase E

Si los cinco primeros bits de una dirección son 1 1 1 1 0, El primer byte toma valores entre 240 y 247, estas direcciones son llamadas direcciones de clase E. Se reserva para usos en el futuro.

[15] Cada grupo esta representado por un número de 28 bits y tiene la ventaja de ser selectivo en la entrega de datagramas

Direcciones IP Especiales

A continuación se presentan direcciones IP que son consideradas especiales:

- Todos los bits a 0: significa “este” host (direcciones IP con número de host = 0) o “esta” red (dirección IP con número de red = 0).
- 0 bits a 1: significa “todas” las redes o “todos” los hosts.
- Dirección 127.0.0.1: denominada dirección de loopback, significa que no debe encaminarse a través de la red, sino directamente del controlador de salida al de entrada.

1.2.9.2 Redes Privadas

Son redes que se usan exclusivamente dentro de una organización y que no requieren conectividad IP con Internet. Existen tres rangos de direcciones reservadas para esto:

- 1 red de clase A: 10.x.x.x
- 16 redes clase B: del 172.16.x.x al 172.31.x.x
- 256 redes clase C: del 192.168.0.x al 192.168.255.x

1.2.9.3 Máscara de red

El término Mascara de Red es muy conocido y utilizado en redes TCP/IP. Como se sabe una dirección IP tiene una parte llamada de red y una parte de host, pero hay que recordar que estas partes es diferente para cada clase de dirección IP.

Para obtener la máscara de red se debe poner unos (1s) en todos los bits de la parte de red y ceros (0s) en todos los bits de la parte de host. El motivo del calculo de la máscara de red es con el fin de determinar el número de subredes que contiene una red.

Por ejemplo la máscara para una red de clase A es 255.0.0.0, para una red de clase B la máscara es 255.255.0.0 y para una red de clase C es 255.255.255.0.[16]

Ejemplo:

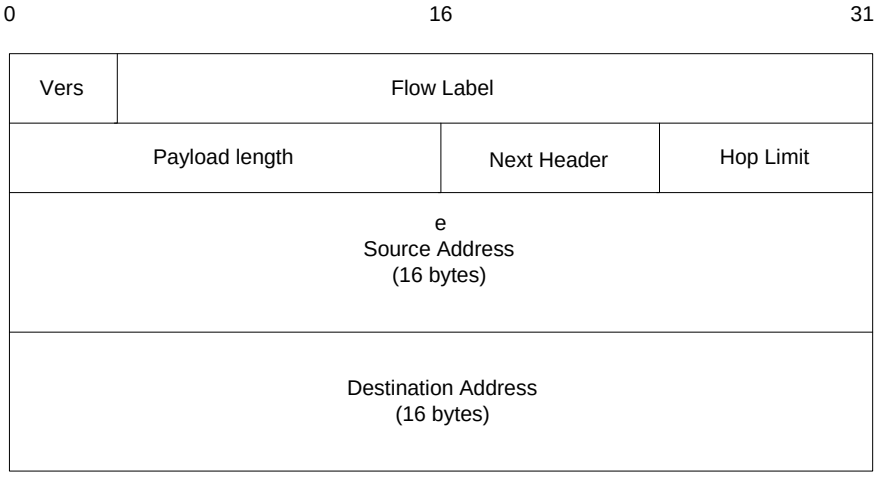
Dir IP: 27.104.0.19	=>	00011011	.	01101000	.	00000000	.	00010011		
Máscara de red:		11111111	.	00000000	.	00000000	.	00000000		
		RED				HOST				
		255	.	0	.	0	.	0		

1.2.10 VERSIÓN 6 DE IP (IPv6)

IPv6 incrementa la longitud de la cabecera IP de 20 a 40 bytes. La cabecera IPv6 contiene dos direcciones de 16 bytes (fuente y destino) precedidas de 8 bytes de control y esto lo consigue suprimiendo opciones de control que en la IPv4 se las tiene. Los campos de uso poco frecuente que se han eliminado de la cabecera se han pasado a extensiones de cabecera opcionales.

GRÁFICO 1. 7

CABECERA IPv6



Fuente: ANÓNIMO. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/. Ultimo Acceso: 20/02/2005.

[16] Estas máscaras se refieren a redes que no contienen subredes

Se espera que todos los nodos IPv6 determinen dinámicamente la PMTU de cada enlace[17] y los nodos fuente solo enviarán paquetes que no excedan el tamaño del PMTU. Por ello, los router's IPv6 los routers no tendrán que fragmentar paquetes en mitad de rutas con mas de un salto permitirán hacer un uso mucho más eficiente de las rutas. En la actualidad esta propuesto que cada enlace soporte una MUY de 576 bytes, pero este valor, como el resto de las especificaciones de IPv6, está sujeto a cambios.

1.2.11 SUBREDES, VLSM

1.2.11.1 Subredes o Subneting

A medida que las subredes IP han crecido, una subred nace con la necesidad de dar flexibilidad al uso de direcciones IP buscando formas de utilizar su espacio de direccionamiento con más eficiencia,

"Una dirección de subred es cualquier dirección derivada del esquema de subdivisión de red, el cual sólo cobra significado dentro de la red donde lo definió.[18]"

"La dirección IP de un host en una red se subdivide de nuevo en un número de red y uno de host, esta segunda red se denomina subred, de tal manera que la red principal llega a ser un conjunto de subredes.

El término Subred, implica dividir la dirección IP en tres capas:

Nombre de red + nombre de subred + nombre de host

La dirección local es la combinación del número de subred y del host.
Existen dos tipos de subredes que son: estático y de longitud variable. La subred estática utiliza la misma máscara de red para todas las subredes de la red

[17] Descrita en el RFC 1191 – Cálculo de PMTU's
[18] JAMSA, Kris; COPE, Ken. Programación en Internet. McGraw-Hill. 1996, página 82.

dividida. La subred de longitud variable (VLSM) puede utilizar diferentes máscaras para las subredes de la red"[19].

1.2.11.2 VLSM (Variable Length Subnet Mask)

Máscara de subred de longitud variable establece que una subred puede tener máscaras de subred diferentes, con la condición de que compartan el mismo prefijo de red. El objetivo principal de VLSM es optimizar el espacio de dirección disponible, esto es especialmente importante si se usan direcciones públicas IP versión 4, que son escasas.

Si se utiliza una máscara de subred de tamaño fijo, es decir la misma máscara de subred en todas las subredes, todas estas subredes tienen que tener el mismo tamaño. Por ejemplo, si la subred más grande necesita 200 hosts, todas las subredes tienen que tener el mismo tamaño de 256 direcciones IP. Así, a una subred que necesita 10 equipos, se asigna la misma subred de 256 direcciones; las restantes 246 direcciones se desperdician. Incluso los enlaces seriales (WAN), que sólo necesitan dos direcciones IP, requieren la misma subred, de 256 direcciones.

El concepto básico de VLSM consiste en dividir una red en subredes de tamaño fijo, luego, se vuelven a subdividir algunas de estas subredes, en pedazos cada vez más pequeños, acomodándose al tamaño requerido.

A continuación se presenta un ejemplo, si tomamos como base una dirección: 172.16.15.0 , al ser esta dirección de clase B, la máscara de red tendrá 16 bits. Cuando llevemos la máscara a 22 bits, lograremos subdividirla en 64 subredes de 1024 direcciones cada una.

Si entre nuestras necesidades tenemos que asignar alguna subred de menos de 60 direcciones, podremos utilizar una máscara de 26 bits, es decir: 1024 subredes de 64 direcciones cada una, y todo sin perder la posibilidad de seguir utilizando la máscara anterior de 22 bits para solucionar el problema de alguna subred grande de hasta 1024 hosts que debamos acomodar.

---

[19] ANÓNIMO. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/. Ultimo Acceso: 20/02/2005.

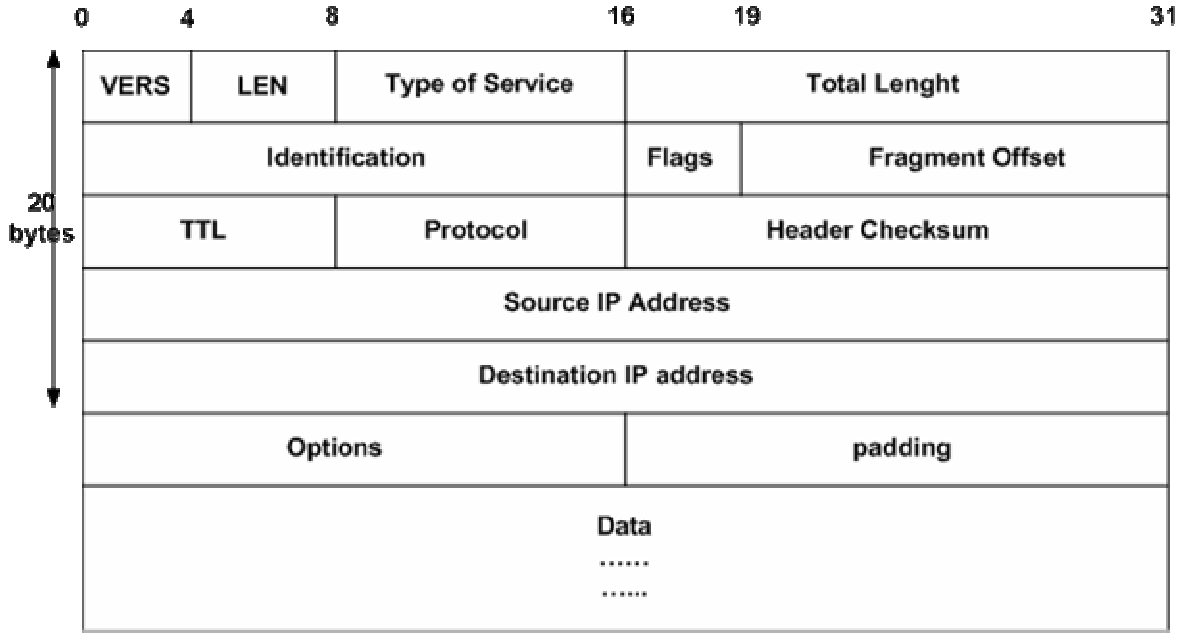
1.2.12 EL DATAGRAMA IP

Es la unidad de transferencia de la pila IP. TCP/IP encapsula casi toda la información que viaja a través de Internet dentro de un datagrama IP. Un datagrama tiene un formato que contiene una cabecera con información para IP y los datos relevantes para las capas superiores.

1.2.12.1 Formato del Datagrama IP

Un encabezado IP consume 20 bytes de espacio de almacenamiento. El siguiente gráfico muestra un datagrama IP con los campos en el encabezado IP identificados.

GRÁFICO 1. 8
FORMATO DEL DATAGRAMA IP



Fuente: ANÓNIMO. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/. Ultimo Acceso: 20/02/2005.

Donde:

"**VERS.-** Es la versión del protocolo.

LEN.- Longitud de la cabecera IP contada en cantidades de 32 bits.

Type of Service.- Indica la calidad del servicio solicitado para este datagrama IP.

Total Lenght.- Da la longitud total del datagrama, cabecera y datos, el cual esta dada en bits.

Identification.- Un número único que asigna el emisor para ayudar a reensamblar un datagrama fragmentado.

Flags.- Son banderas de control, entre las que tenemos: 0 es un valor reservado, DM no fragmentar, y MF mas fragmentos.

Fragment Offset.- Usado con datagramas fragmentados, para ayudar al reensamblado de todo el datagrama. El valor es el número de partes de 64 bits (no se cuentas los bits de la cabecera) contenidas en fragmentos anteriores.

Time to Live.- Es el tiempo en segundos que se le permite viajar a este datagrama.

Protocol Number spotipprotn.- Indica el protocolo de alto nivel al que IP debería entregar los datos del datagrama.

Header Checksum.- Es el checksum de la cabecera. Se calcula como el complemento a uno de la suma de los complementos a uno de todas las palabras de 16 bits de la cabecera

Source IP Address.- La dirección IP de 32 bits del host emisor.

Destinatio IP Address.- La dirección IP de 32 bits del host receptor.

Options.- Longitud variable. No requiere que toda implementación de IP sea capaz de generar opciones en las datagramas que crea, pero si que sea capaz de procesar datagramas que contengan opciones.

Padding.- Si se usa una opción, el datagrama se rellena con bytes a cero hasta la siguiente palabra de 32 bits.[20]"

1.2.12.2 Fragmentación

Para que un datagrama IP pueda viajar a través de la red es necesario imponer un tamaño máximo de trama que pueda transmitir la red. Esta unidad de

[20] ANÓNIMO. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/3376c418.html#dhcp. Acceso último: 25/05/2005

transferencia máxima se denomina MTU (“Maximium Transmission Unit”). La fragmentación consiste en un método de dividir un solo datagrama en dos o más datagramas pequeños, y luego reensamblarlos en el host de destino IP. La fragmentación ocurre cuando la longitud del datagrama IP excede la unidad de transferencia máxima física de la red. Otra razón es cuando un datagrama atraviesa un enrutador y la unidad de transferencia máxima de éste es menor que la red local emisora. Para el control de la fragmentación existen campos en el datagrama IP que ayudan a su reensamblado correcto.

1.2.13 ENCAMINAMIENTO O ENRUTAMIENTO IP

El encaminamiento es la función principal que realiza la capa IP. La clave para la entrega de datagramas IP es la tabla de enrutamiento IP. Una tabla de enrutamiento IP almacena las direcciones de destinos seleccionados en la red; en otras palabras, el software de red puede buscar una tabla de enrutamiento a fin de hallar la mejor ruta o trayectoria para llegar a su destino. Existen los protocolos de enrutamiento que manejan todas las entradas de la tabla de enrutamiento.

1.2.13.1 Encaminamiento Directo e Indirecto

El encaminamiento directo consiste en que si un host que desea transmitir a otro host que se encuentran en la misma red física, el datagrama IP puede ser enviado directamente encapsulando el datagrama IP en una trama.

El encaminamiento indirecto ocurre cuando un host desea transmitir a un host que se encuentre en una red distinta, para este caso la única forma para alcanzar el destino es atravesar uno o varios routers. “La dirección del primer salto se denomina ruta indirecta y es lo que necesita el host fuente, el router recibe el datagrama y se responsabiliza del segundo salto, y así sucesivamente.[21]

[21] ANÓNIMO. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/. Acceso último: 20/02/2005.

1.2.13.2 Tabla de encaminamiento IP

Consiste en que cada host guarda el conjunto de mapeados entre las direcciones IP de destino y las direcciones IP del siguiente salto para ese destino en una tabla llamada tabla de encaminamiento IP. En esta tabla se encuentran tres tipos de mapeado:

1. "Rutas directas, para redes conectadas localmente
2. Rutas indirectas, para redes accesibles a través de uno o más routers.
3. Una ruta por defecto, que contiene la dirección IP de un router que todas las direcciones IP no contempladas en las rutas directas o indirectas han de usar.[22]"

Con la finalidad de que IP determine la ruta para un datagrama de salida se denomina algoritmo de encaminamiento IP.

1.2.14 PROTOCOLO ICMP ("INTERNET CONTROL MESSAGE PROTOCOL")

El Protocolo de Mensajes de Control de Internet sirve para informar errores producidos en el procesamiento de datagramas IP, es parte integral de IP y debe ser implementado por módulo IP, se usa para informar algunos errores en cualquier datagrama IP con la excepción de mensajes IP, para evitar repeticiones infinitas.

Los mensajes ICMP nunca se envían en repuesta a datagramas con una IP de destino que sea de broadcast o multicast, tampoco se envían en respuesta a un datagrama que no tenga una dirección IP de origen que represente a un único host.

Existen dos aplicaciones basadas en el ICMP que son: el Ping y el Traceroute, el Ping se utiliza para determinar si un host es alcanzable mediante el envío de uno o más datagramas a un host de destino determinado solicitando una respuesta y

[22] ANÓNIMO. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/. Acceso último: 20/02/2005.

calcula el tiempo que toma en retornarla. El Traceroute nos permite determinar la ruta que siguen los datagramas IP de host a host.

El Ping usa los mensajes ICMP Echo y Echo Reply para determinar si un host es alcanzable. El Traceroute envía datagramas IP con bajos TTLs para que expiren durante la ruta que les dirige al destino. Utiliza los valores de los mensajes ICMP Time Exceeded para determinar en que parte de la red expiraron los datagramas y reconstruye así un esquema de la ruta hasta el host de destino

1.2.15 PROTOCOLO IGMP ("INTERNET GROUP MANAGEMENT PROTOCOL")

"El Protocolo de Administración de Grupos de Internet es una extensión del protocolo IP, se utiliza para realizar multicast, que consiste cuando el envío de datos a una dirección IP puede alcanzar múltiples servidores de una red y/o todas las máquinas de una subred. Además de emplearse para pasar información se utiliza para establecer los miembros de la red, para pasar información de los miembros y establecer rutas.[23]"

1.3 ASIGNACIÓN DE DIRECCIONAMIENTO IP

1.3.1 ASIGNAMIENTO ESTÁTICO

Es cuando la configuración de un ordenador se la realiza de manera manual, pero si el ordenador se mueve de la red a otro lugar diferente, se debe configurarlo con otra dirección diferente.

El asignamiento estático se utiliza, por lo general, cuando existe un número pequeño de enrutadores en una red, pero cuando existe un solo gateway en la red, la mejor opción es este tipo de Asignamiento. Para este tipo de asignación de direcciones se deben construir tablas de enrutamiento en forma manual.

[23] ANÓNIMO. Protocolos de Internet. http://www.zator.com/Internet/A3_7.htm. Último Acceso: 25/06/2005

1.3.2 ASIGNAMIENTO DINÁMICO (DHCP)

DHCP (Dynamic Host Configuration Protocol) son las siglas en inglés del Protocolo de configuración dinámica en un host, que es empleado para que los hosts (clientes) que están formado parte de una red puedan obtener su configuración de forma dinámica a través de un servidor de protocolos, obteniendo de esta forma la dirección IP, la máscara de red, la dirección de broadcast, las características del DNS, la puerta de enlace, etc.

Este protocolo apareció en octubre de 1993 como protocolo estándar y toda información más profunda se la puede hallar en el RFC[24] 2131.

Mediante DHCP el administrador tiene la facilidad de supervisar y distribuir direcciones IP de forma automática y centralizada, así mismo, podrá enviar y asignar una nueva dirección IP si el ordenador se ha trasladado físicamente a otra parte de la red.

El protocolo DHCP incluye tres tipos de asignación de direcciones IP que son:

- **Asignación manual.-** Para este tipo de asignaciones se utiliza tablas de direcciones MAC, esto es que se otorgará la dirección IP, que le asigne la tabla MAC, únicamente a los ordenadores cuyas direcciones MAC consten en esta tabla. De manera similar existe el protocolo "BOOTP o Internet Bootstrap Protocol el cual permite también la asignación de la configuración de red en forma dinámica pero a partir de su definición estática para cada cliente en una base de datos en el servidor.[25]"

[24] Informe que los investigadores informáticos envían al Internet Architecture Board en el cual proponen y diseñan la creación de nuevos protocolos, los cuales deben estar sujetos a normas que previamente son impuestas.

[25] CASTELLANOS, Alina. El servicio DHCP. http://www.linux.cu/maual/avanzado-html/node29.html . Acceso último: 04/04/2005.

- **Asignación automática.-** El administrador determina un rango de direcciones IP, y una de las que este libre, se le asigna permanentemente al ordenador que lo solicite.

- **Asignación dinámica.**- Este método de asignación es el que permite la reutilización de direcciones IP de un rango de direcciones que el administrador a determinado cuando un computador, a través de la interfaz de red, ingresa a formar parte de la red.

El protocolo DHCP puede identificar a sus clientes de dos formas:

1. Mediante la dirección MAC (Medium Access Control) de la tarjeta de red del cliente

2. Un identificador que le indique el cliente.

Existen otros protocolos de gestión de direcciones, como por ejemplo BOOTP, pero DHCP es más avanzado, aunque ambos son los más usados.
Es cierto que el servicio DHCP tiene la finalidad de otorgar direcciones IP dinámicamente, pero eso no limita que entregue direcciones fijas a clientes especiales que por sus funcionalidades lo requieran, como por ejemplo el servicio DNS.

Entre las configuraciones opcionales que un servidor DHCP puede proveer son:

- Dirección del servidor DNS
- Nombre DNS
- Puerta de enlace de la dirección IP
- Dirección de publicación masiva
- Máscara de subred
- Tiempo máximo de espera del ARP
- MTU para la interfaz
- Servidores de servicio de información de red

- Dominios NIS
- Servidores de protocolo de tiempo de red
- Servidores SMTP
- Servidores TFTP
- Nombre del servidor WINS

DHCP permite acelerar y facilitar la configuración de muchos hosts en una red, con el fin de evitar posibles errores humanos. Los puertos que el IANA a determinado para el protocolo DHCP es: 67/udp para las computadoras servidor y 68/udp para las computadoras cliente, siendo los mismos puertos para BOOTP.

1.3.2.1 Funcionamiento del Protocolo DHCP

El servidor DHCP tiene un programa que esta a la escucha, de los clientes que pertenecen a la red de información, el cual almacena tablas de posibles direcciones IP a otorgar además del resto de la información. Cuando un cliente requiere o solicita el servicio (DHCPDISCOVER) lo hace en forma de *broadcast* a través de la red. Los servidores que recibieron este pedido le responden con sus respectivas propuestas (DHCPOFFER), el cliente se entera de esto y solo a uno de ellos lo notifica (DHCPREQUEST), el cual le confiere la información requerida (DHCPPACK). Dicha información se mantiene mientras el computador, a través de su interfase de red, no se desconecte de la red o hasta que el plazo del *lease time*[26] ("contrato") no expire. Una vez vencido el plazo del contrato con el servidor se lo puede renovar, fundamentalmente la dirección IP, y adquirir una nueva o extender el plazo y así mantener la misma información. También el cliente podrá solicitar la renovación o liberación de sus datos.

Si al recibir el cliente el mensaje (DHCPPACK) detecta que los parámetros de configuración tienen algún inconveniente, éste envía un mensaje (DHCPDECLINE) y reinicia el proceso de configuración. El cliente debería

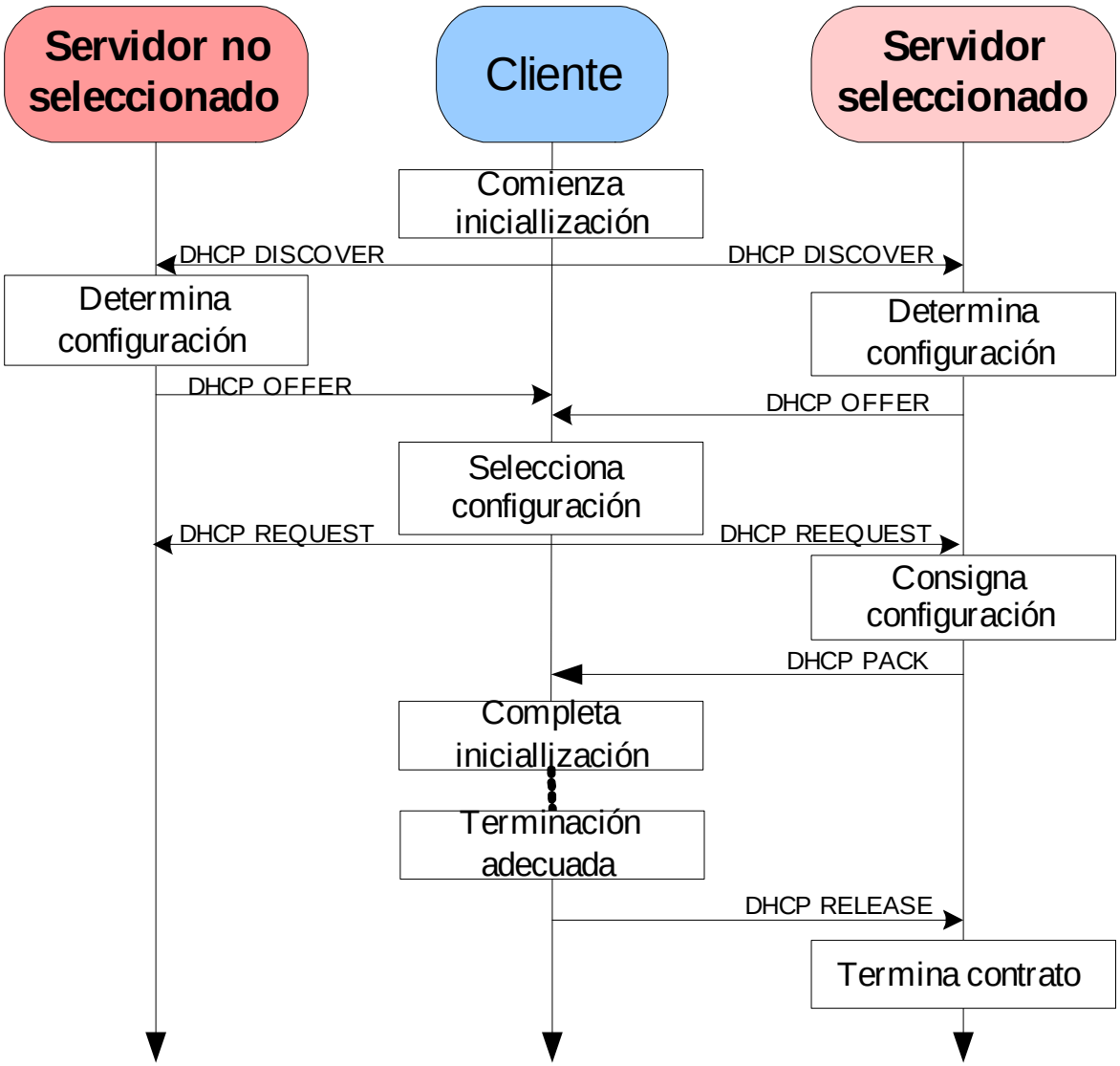
[26] Es el tiempo que un cliente DHCP mantiene como propios los datos que le otorgo el servidor (el servicio DHCP), se puede decir, que es el tiempo de contrato que mantiene el cliente con el servidor.

esperar un mínimo de diez segundos antes de reiniciar este proceso para evitar un exceso de tráfico en la red en caso de que se produzca algún bucle.

1.3.2.2 Mensajes que se intercambian en el protocolo DHCP

GRÁFICO 1. 9

DIAGRAMA DE LAS ETAPAS DEL PROTOCOLO DHCP



FUENTE: CASTELLANOS, Alina. El servicio DHCP. http://www.linux.cu/maual/avanzado-html/node29.html . Acceso último: 04/04/2005.

1. **"DHCPDISCOVER:** Mensaje que envía el cliente a la red en forma de broadcast para detectar los servidores.

2. **DHCPOFFER:** Mensaje que el servidor envía al cliente con una oferta de configuración.

3. **DHCPREQUEST**: Mensaje de solicitud de un cliente a un servidor para:

   a. Aceptar la oferta de un servidor determinado, mientras a los demás los rechaza
   b. Confirmar la exactitud de la información asignada antes del reinicio del sistema
   c. Extender el plazo de un contrato de dirección IP determinada

4. **DHCPPACK:** Mensaje que el servidor le envía al cliente, en el cual le entrega la configuración asignada excepto la dirección IP que ya fue aceptada.

5. **DHCPNAK**: Mensaje que el servidor le envía al cliente para informarle que la dirección que tiene asignada esta incorrecta o que el contrato ha expirado.
6. **DHCPDECLINE**: Mensaje que el cliente da al servidor mediante el cual le dice que sigue usando la dirección determinada.

7. **DHCPREALEASE**: Mensaje que el cliente envía al servidor en el cual rechaza la dirección asignada y da por terminado cualquier contrato anteriormente establecido.

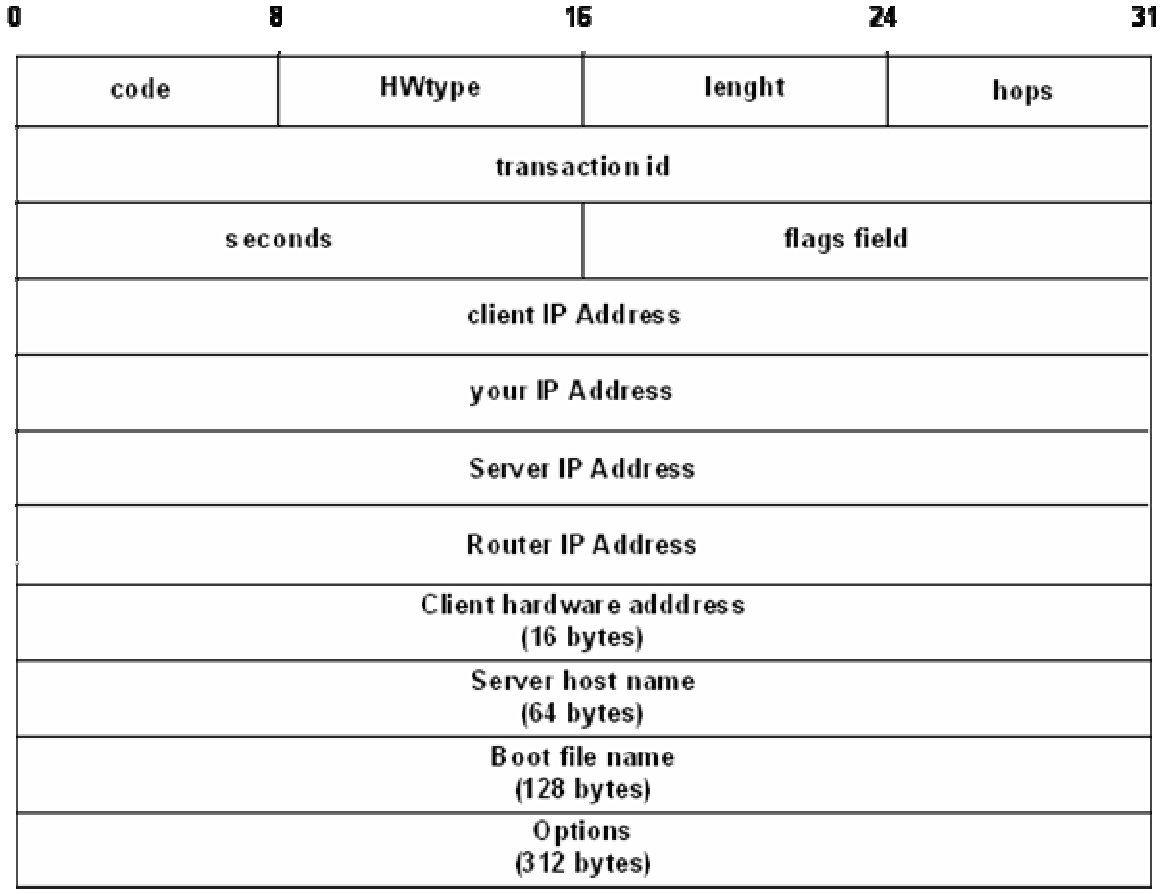
8. **DHCPINFORM**: Mensaje del cliente al servidor solicitando los parámetros de configuración excepto la dirección IP, pues ya lo tiene asignada.[27]"

[27] ANÓNIMO. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/3376c418.html#dhcp. Acceso último: 25/05/2005

1.3.2.3 Estructura del formato DHCP

GRÁFICO 1. 10

ESTRUCTURA DEL FORMATO DHCP



FUENTE: Anónimo. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/3376c418.html#dhcp. Acceso último: 25/05/2005

"code.- Indica solicitud o respuesta, toma dos valores que son 1: Request y 2: Replay.

HWType.- Indica que tipo de hardware esta presente, por ejemplo 1: Ethernet, 6: IEEE 802 Networks.[28]"

"Length.- Longitud en bytes de la dirección hardware. Por ejemplo Ethernet y las redes en anillo usan 6.

[28] Anónimo. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/3376c418.html#dhcp. Acceso último: 25/05/2005

hops.- El cliente lo pone a 0. Cada Router que retransmite la solicitud a otro servidor lo incrementa, con el fin de detectar bucles. Según el RFC para determinar un bucle debe tener el valor de 3.

Transaction ID.- Número aleatorio usado para comparar la solicitud con la respuesta que genera.

Seconds.- Fijado por el cliente. Es el tiempo transcurrido en segundos desde que el cliente inició el proceso de arranque.

Flags Field.- El bit más significante de este campo se usa como flag de broadcast. Todos los demás bits deben estar a 0; están reservados para usos futuros. Normalmente, los servidores DHCP tratan de entregar los mensajes DHCPREPLY directamente al cliente usando unicast. La dirección de destino en la cabecera IP se pone al valor de la *dirección IP* fijada por el servidor DHCP, y la dirección MAC a la *dirección hardware* del cliente DHCP. Si un host no puede recibir un datagrama IP en unicast hasta saber su propia dirección IP, el bit de broadcast se debe poner a 1 para indicar al servidor que el mensaje DHCPREPLY se debe enviar como un broadcast en IP y MAC. De otro modo, este bit debe ponerse a cero.

Cient IP address.- Fijada por el cliente. O bien es su dirección IP real, o 0.0.0.0.

Your IP address.- Fijada por el servidor si el valor del campo anterior es 0.0.0.0

Server IP address.- Fijada por el servidor.[29]**„**

“Router IP address.- Fijada por el "router" retransmisor si se usa retransmisión BOOTP.

[29] Anónimo. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/3376c418.html#dhcp. Acceso último: 25/05/2005.

Client hardware address.- Fijada por el cliente y usada por el servidor para identificar cuál de los clientes registrados está arrancando.

Server host name.- Nombre opcional del host servidor acabado en X'00'.

Nombre del fichero de arranque.- El cliente o bien deja este campo vacío o especifica un nombre genérico, como "router" indicando el tipo de fichero de arranque a usar. En la solicitud de DHCPDISCOVER se pone al valor nulo. El servidor devuelve el la ruta de acceso completa del fichero en una respuesta DHCPOFFER. El valor termina en X'00'.

Options.- Los primeros cuatro bytes del campo de opciones del mensaje DHCP contienen el cookie (99.130.83.99). El resto del *campo* de opciones consiste en parámetros marcados llamados *opciones*. Remitirse al RFC 1533 para más detalles.[30]"

1.3.2.4 Almacenamiento de los mensajes de configuración

El protocolo DHCP permite el almacenamiento persistente de los parámetros de configuración de red de los clientes, ya que asigna un valor y una clave única a cada cliente y lo almacena, la clave contiene por ejemplo un número de subred y un identificador único dentro de la subred, y el valor contiene los parámetros de configuración del cliente.

1.3.2.5 Protocolo Bootp

Se sabe que un computador para poder arrancar, debe contener información necesaria dentro de su disco, pero mediante el protocolo BOOTP ya no es necesario que la máquina contenga disco alguno ya que este protocolo efectúa arranques remotos en redes IP, solo se requiere que éste forme parte de una red

---

[30] Anónimo. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/3376c418.html#dhcp. Acceso último: 25/05/2005

LAN, con ciertas limitaciones, ya que desempeñaran las funciones de una estación de trabajo, concentrador de terminales, etc.

Para hacer esto posible se debe almacenar en la ROM (“Read Only Memory”) una pila de IP mínima sin información de configuración, la cual obtendrá información suficiente para descargar el código de arranque necesario. No especifica BOOTP como realiza esta descarga pero habitualmente utiliza TFTP (“Trivial File Transfer Protocol”).

El protocolo BOOTP realiza los siguientes procesos:

- El cliente debe configurar su propia dirección hardware, la cual se almacena en la ROM.

- El cliente BOOTP envía, en forma de broadcast, su dirección hardware dentro de un datagrama UDP al servidor. Como desconoce su dirección IP, utiliza la 0.0.0.0 y para la dirección IP del servidor utiliza la 255.255.255.255 (broadcast). Esto lo hace a través del puerto UDP 67.

- Como el servidor tiene su fichero de configuración, al recibir el datagrama, busca la dirección IP que concuerde con la dirección hardware del cliente, y esta se la envía nuevamente al cliente BOOTP dentro del datagrama en el campo correspondiente. Para esto utiliza el puerto UDP 68. Esto lo puede hacer de las formas siguientes:

- Si el cliente conoce su dirección IP (incluida en la solicitud BOOTP), el servidor envía directamente el datagrama a esa dirección. Si el caché de ARP de la pila de protocolos del servidor desconoce la dirección hardware correspondiente a esa dirección IP lo hará mediante el uso de la ARP (Address Resolution Protocol) habitual.

- En el caso que el cliente desconozca su dirección IP, entonces el servidor será el encargado de averiguarlo mediante la caché de ARP. El servidor no

puede utilizar ARP para saber la dirección IP del cliente ya que ni el mismo lo sabe, en este caso puede resolver de dos formas:

a. Si el servidor tiene un mecanismo para actualizar directamente su propia caché ARP sin usar ARP, lo utiliza y envía directamente el datagrama.

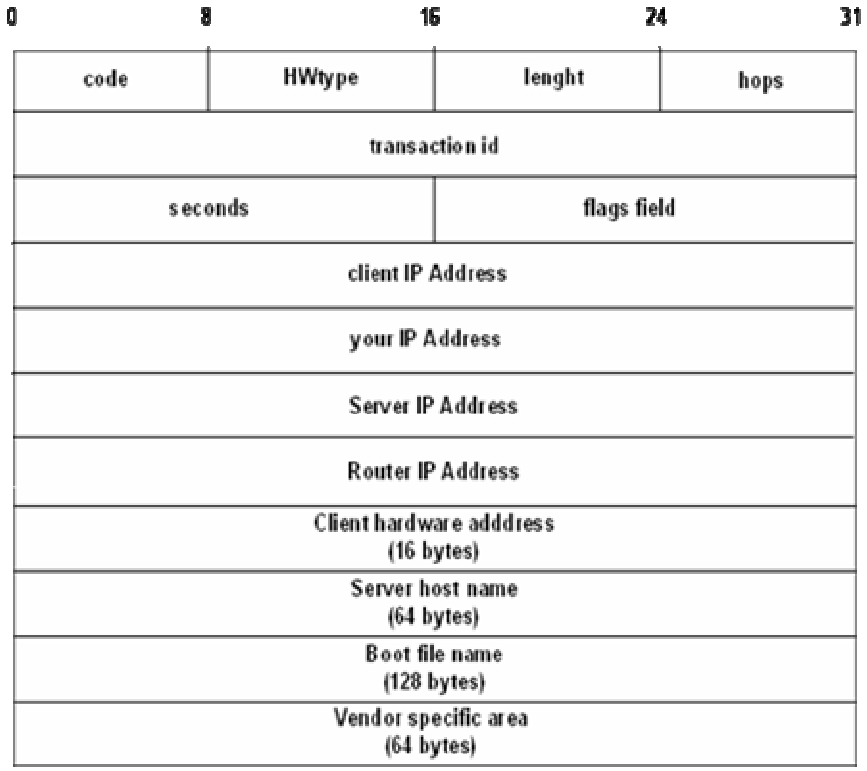
b. Si el servidor no puede actualizar su propia caché, debe enviar una respuesta en forma de broadcast.

- Por último el cliente al recibir la información de su dirección IP lo almacenará y empezará el proceso de arranque.

1.3.2.6 ESTRUCTURA DEL FORMATO BOOTP

GRÁFICO 1. 11

ESTRUCTURA DEL FORMATO BOOTP



Fuente: Anónimo. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/3376c417.html#dhcp. Acceso último: 25/05/2005

"code.- Si tiene el valor de 1 indica una solicitud (Request), pero si el tiene el valor de 2 indica una respuesta (Replay).

HWType.- Indica que tipo de hardware esta presente, por ejemplo 1: Ethernet, 6: IEEE 802 Networks

Length.- Longitud en bytes de la dirección hardware. Por ejemplo Ethernet y las redes en anillo usan 6.

hops.- El cliente lo pone a 0. Cada Router que retransmite la solicitud a otro servidor lo incrementa, con el fin de detectar bucles. Según el RFC para determinar un bucle debe tener el valor de 3.
Transaction ID.- Número aleatorio usado para comparar la solicitud con la respuesta que genera.

Seconds.- Fijado por el cliente. Es el tiempo transcurrido en segundos desde que el cliente inició el proceso de arranque.

Flags Field.- El bit más significante de este campo se usa como flag de broadcast. Todos los demás bits deben estar a 0; están reservados para usos futuros. Normalmente, los servidores DHCP tratan de entregar los mensajes DHCPREPLY directamente al cliente usando unicast. La dirección de destino en la cabecera IP se pone al valor de la *dirección IP* fijada por el servidor DHCP, y la dirección MAC a la *dirección hardware* del cliente DHCP. Si un host no puede recibir un datagrama IP en unicast hasta saber su propia dirección IP, el bit de broadcast se debe poner a 1 para indicar al servidor que el mensaje DHCPREPLY se debe enviar como un broadcast en IP y MAC. De otro modo, este bit debe ponerse a cero. [31]"

"Cient IP address.- Fijada por el cliente. O bien es su dirección IP real, o 0.0.0.0.

Your IP address.- Fijada por el servidor si el valor del campo anterior es 0.0.0.0

Server IP address.- Fijada por el servidor.

---

[31] Anónimo. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/3376c417.html#dhcp. Acceso último: 25/05/2005.

Router IP address.- Fijada por el "router" retransmisor si se usa retransmisión BOOTP.

Client hardware address.- Fijada por el cliente y usada por el servidor para identificar cuál de los clientes registrados está arrancando.

Server host name.- Nombre opcional del host servidor acabado en X'00'.

Boot file name.- El cliente o bien deja este campo vacío o especifica un nombre genérico, como "router" indicando el tipo de fichero de arranque a usar. En la solicitud de DHCPDISCOVER se pone al valor nulo. El servidor devuelve el la ruta de acceso completa del fichero en una respuesta DHCPOFFER. El valor termina en X'00'.

Vendor-specific area.- Área específica del distribuidor (opcional). Se recomienda que el cliente llene siempre los cuatro primeros bytes con un *"magic cookie"* o galleta mágica. Si el cookie específica de un distribuidor no se usa, el cliente debería utilizar 99.130.83.99 seguido de una marca de fin (255) y fijar los bis restantes a cero. Remitirse al RFC 1533 para más detalles.[32]"

1.3.2.7 Protocolo Dhcp/Scope

SCOPE

Es un rango completo y consecutivo de posibles direcciones IP para una red. El scope típicamente define una única subred física sobre su red para el cual el servicio DHCP es ofrecido. Scope también provee vías principales al servidor para administrar la distribución y asignación de direcciones IP como también cualquier parámetro de configuración relacionada con sus clientes de red.

Por lo tanto se dice que el scope (“ámbito”), es el intervalo de direcciones de red que estarán disponibles para que el servidor las asigne a los clientes, además con esto se pueden definir subredes físicas.

---

[32] Anónimo. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/3376c417.html#dhcp. Acceso último: 25/05/2005

1.3.2.8 Protocolo Dhcp/Multi-Scope

MULTISCOPE

Es un grupo de scopes que pueden ser usados para soportar múltiples subredes IP lógicas sobre la misma subred física. El multiscope se utiliza con el fin de facilitar la administración del contenido de una lista de “miembros scope” o “hijos scope”, los cuales pueden ser activados conjuntamente. El multiscope no se utiliza para configurar otros detalles del uso de un scope, pero para configurar otras propiedades usadas con multiscope, se necesita configurar propiedades de los miembros scope individualmente.

1.4 FUNCIONAMIENTO DE UN SWITCH

1.4.1 PROTOCOLO ARP (“ADDRESS RESOLUTION PROTOCOL”)

El Protocolo de Resolución de Direcciones es el encargado de convertir las direcciones de protocolo de alto nivel (direcciones IP) a direcciones de red físicas (dirección MAC).

“En una red, los host se identifican a través de su dirección física. Los protocolos de alto nivel direccionan a los host de destino con una dirección simbólica (dirección IP), el momento que tal protocolo quiera enviar un datagrama a la dirección IP de destino el manejador de destino no lo entiende. En consecuencia se suministra un módulo (ARP) que traducirá la dirección IP a la dirección física del host destino. Utiliza una tabla (llamada a veces ARP) para realizar esta traducción.

Cuando la dirección no se encuentra en la caché ARP, se envía un broadcast en la red, con un formato especial llamado petición ARP. Si una de las máquinas en la red reconoce su propia dirección IP en la petición, devolverá una repuesta ARP al host que la solicitó. La respuesta contendrá la dirección física de hardware así como información del encaminamiento, tanto esta dirección como la ruta se almacenan en la caché del host solicitante. Todos los posteriores datagramas enviados a esta dirección IP se podrán asociar a la dirección física

correspondiente, que será la que utilice el manejador de dispositivo para mandar el datagrama de la red.[33]"

1.4.1.1 Tablas ARP

Las tablas ARP establecen enlaces entre las capas de protocolo y de 'link' (en caso de una red local Ethernet, sería entre dirección IP y dirección MAC). Cada host de una subred necesita conocer la dirección física de los demás para poder mandar paquetes a los destinatarios adecuados. Estas direcciones se almacenan en un caché ARP.

En caso de no conocer la dicha dirección MAC, se hace una petición de broadcast, la máquina con tal dirección IP contesta, y el host almacena esta MAC en su caché.

1.4.2 SWITCH CAPA 2

Opera en la capa de Enlace del Modelo OSI, y es el tipo de switch de red de área local (LAN) más básico.

Un switch capa 2 toma sus decisiones de envío de datos en base a la dirección MAC destino, segmentan la red en dominios de colisión proporcionado un mayor ancho de banda por cada host.

La configuración y el soporte de múltiples protocolos es transparente a los host, de la misma manera el soporte de las redes virtuales (VLAN's), las cuales son una forma de segmentación que permite crear dominios de broadcast formando así grupos de trabajo independientes de la localización física.

Existen dos esquemas para el envío de tráfico: Cut-trough, el mismo que comienza el proceso de envío antes de que el frame sea completamente recibido

[33] ANÓNIMO. Tutorial y descripción técnica de TCP/IP. http://ditec.um.es/laso/docs/tut-tcpip/. Ultimo Acceso: 20/02/2005.

y el otro esquema Store-and-forward, el cual lee y valida el paquete completo antes de iniciar el proceso de envío.

1.4.3 SWITCH CAPA 3

Un switch capa 3 integran routing y switching con la finalidad de producir altas velocidades.

Las principales funciones de un switch consiste en: Procesamiento de Rutas (esto incluye construcción y mantenimiento de la tabla de enrutamiento usando RIP y OSPF), Envío de paquetes (una vez que el camino es determinado, los paquetes son enviados a su dirección destino. El TTL (Time-To-Live) es decrementado, las direcciones MAC son resueltas y el checksum IP es calculado) y Servicios Especiales (traslación de paquetes, priorización, autenticación, filtros.)

1.4.4 DOMINIOS DE COLISIÓN

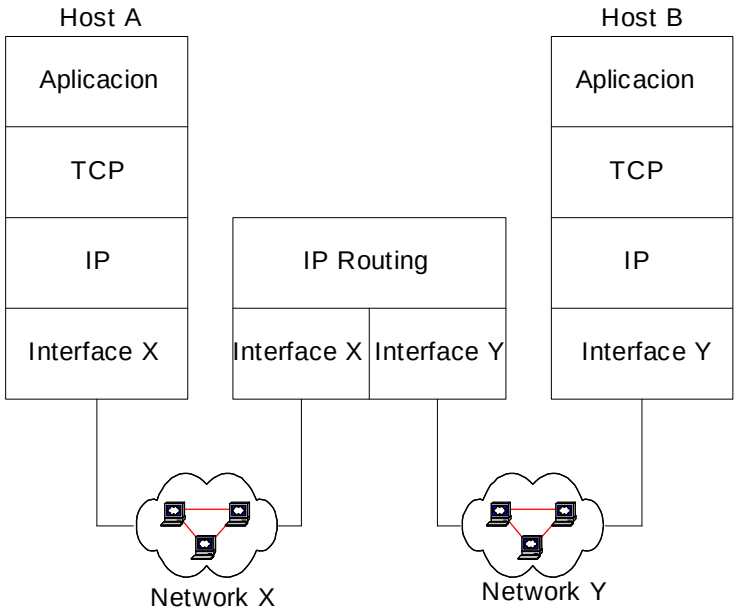
Un dominio de colisión es un segmento del cableado de la red que comparte las mismas colisiones. Cada vez que se produzca una colisión dentro de un mismo dominio de colisión, afectará a todos los ordenadores conectados a ese segmento pero no a los ordenadores pertenecientes a otros dominios de colisión. Todas las ramas de un hub forman un mismo dominio de colisión (las colisiones se retransmiten por todos los puertos del hub). Cada rama de un switch constituye un dominio de colisiones distinto, las colisiones no se retransmiten por los puertos del switch.

1.5 FUNCIONAMIENTO DE UN ROUTER

El ruteo es el proceso mediante el cual se selecciona un camino adecuado para que una máquina pueda enviar paquetes a otra, a través de la red, mientras que el ruteador es el computador que realiza dicha selección.

GRÁFICO 1. 12

FUNCIONAMIENTO DEL ROUTER EN IP



Fuente: Anónimo. Biblioteca personal. Capítulo 3. Protocolos de encaminamiento. Página 118

1.5.1 NIVEL DE RUTEO

El ruteo ocurre a muchos niveles. Por ejemplo, en una red de área amplia se conoce que tiene algunos conmutadores y de hecho tienen muchas conexiones físicas, en este caso la misma red es la responsable de rutear los paquetes desde que salen hasta que lleguen a su destino.

"Una de las funciones básicas de IP es la habilidad para conectar distintas redes físicas.[34]"

El ruteo puede dividirse en dos partes: por entrega directa y por entrega indirecta.

1.5.1.1 Ruteo por entrega directa

La entrega directa es cuando una estación de trabajo envía un datagrama a otra, a través de una sola red física. Esta entrega de datagramas no involucra

[34] ANÓNIMO. Biblioteca personal. Capítulo 3. Protocolos de encaminamiento. Página 118

ruteadores. El equipo transmisor debe saber si la información de destino reside en una de las redes directamente conectadas, para esto el transmisor descompone la estructura del datagrama y analiza específicamente la dirección IP comparándola con la porción de red de su propia dirección IP y si esta coincide, significa que el datagrama se entregará de forma directa.

1.5.1.2 Entrega indirecta

Este tipo de entrega se lo realiza cuando una estación de trabajo envía un datagrama a otra, teniendo el datagrama que atravesar por varios ruteadores para alcanzar el destino final. Explicando mas detalladamente, se debe pensar en una red físicamente grande en la que cada una de las redes se conectaran entre si por medio de ruteadores.

Cuando una estación de trabajo envía un datagrama hacia otra estación, en primer lugar lo encapsula, después busca el ruteador más cercano y este mediante software IP extrae el datagrama encapsulado como también busca y selecciona el siguiente ruteador más cercano. Nuevamente se inserta el datagrama en una trama y se lo envía a través de la siguiente red física hacia el segundo ruteador, y así sucesivamente, hasta que el datagrama llegue a su destino final.

Tanto las estaciones de trabajo como los ruteadores, para saber donde y cual es el dispositivo más idóneo a donde enviar el datagrama, se valen del ruteo IP y para esto utilizan algoritmo básico de ruteo controlado por tablas.

1.5.1.3 Ruteo IP controlado por tabla

Cada máquina tiene un algoritmo de ruteo y este emplea tablas de ruteo IP, en el cual se almacena información de los posibles destinos y en cómo alcanzarlos, es decir, cada vez que una máquina necesite enviar un datagrama, ésta consultará con la tabla de ruteo para decidir a donde enviarlo.

Estas tablas emplean el principio de ocultación de información y dejan que sean las propias máquinas las que tomen las decisiones de ruteo teniendo un mínimo de información.

Dicho principio se basa en que “aísla información sobre los anfitriones específicos del ambiente local en el que existen y hacer que las máquinas que están lejos encaminen paquetes hacia ellos sin saber dichos detalles.[35]” Para esto las tablas de ruteo IP solo contienen información de los prefijos de red y no direcciones IP completas.

1.5.1.4 Ruteo con salto al siguiente

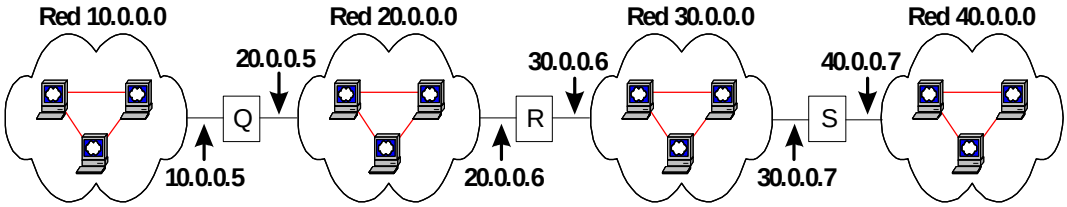
Toda tabla de ruteo contiene pares (N: dirección IP de destino y R: dirección IP del *siguiente* ruteador en el camino hacia la red N) y la utilización de la tabla de ruteo es para almacenar el siguiente salto para cada destino. Entonces, cada tabla de ruteo es solo un salto a lo largo de todo el trayecto que le conlleva a un datagrama alcanzar su destino. Además cada registro en esta tabla corresponde a un ruteador que pertenezca a una entrega directa.

Cada vez que una máquina transmite un datagrama, el software IP lo descompone y extrae la dirección IP destino y de esta toma la porción de red, con este ultimo dato el software toma la decisión de ruteo en base al ruteador al cual se pueda realizar la entrega directa. Esta explicación se la puede observar de una manera más clara en el gráfico siguiente:

[35] Fuente: COMER, Douglas. Redes Globales de Información con Internet y TCP/IP. Tercera edición. Prentice Hall. México. 1996. Página 115

GRÁFICO 1. 13

RUTEO CON SALTO AL SIGUIENTE



(a)

PARA ALCANZAR LOS ANFITRIONES EN LA RED	RUTEAR A ESTA DIRECCION
20.0.0.0	ENTREGAR DIRECTAMENTE
30.0.0.0	ENTREGAR DIRECTAMENTE
10.0.0.0	20.0.0.5
40.0.0.0	30.0.0.7

(b)

(a) Ejemplo de una red con 4 redes y 3 ruteadores, y (b) la tabla de ruteo en R

Fuente: COMER, Douglas. Redes Globales de Información con Internet y TCP/IP. Tercera edición. Prentice Hall. México. 1996. página: 116.

Como se puede observar en la figura, la tabla de ruteo solo almacena información de la dirección IP de destino al cual se realizará la entrega directa, para lograr de esta forma una optimización en el tamaño de la tabla, ocultar información de otros hosts que sean residentes de una red y por último que el software IP tome buenas decisiones en el ruteo del datagrama.

La utilización de la red IP de destino por parte de las tablas de ruteo conllevan ciertos inconvenientes como son: primero, como existe un solo camino para el tráfico destinado a una red, éste puede llegar a saturarse. Segundo, el último ruteador del camino es el delegado en informar sobre el estado operativo del anfitrión final.

1.5.1.5 Rutas asignadas por omisión

Es cuando se asocia muchos registros a un ruteador asignado por omisión, logrando de esta forma ocultar información como también mantener reducido el tamaño de las tablas de ruteo. El funcionamiento es muy sencillo, ya que si el software de ruteo IP al consultar la tabla de ruteo no encuentra una red de destino, las rutinas de ruteo envían el datagrama a un *ruteador asignado por omisión*.

Este tipo de asignación de ruteo es como regla en redes en las que tienen un solo ruteador, el cual es la puerta de acceso al resto de la red IP, debido a que toda la decisión del ruteo consiste en dos comprobaciones: una a la red local, y a un valor asignado por omisión que apunta hacia el único ruteador posible.

1.5.1.6 Rutas por anfitrión específico

Como hemos visto el ruteo se lo realiza sobre redes, pero el software de ruteo IP tiene la capacidad de especificar rutas por anfitrión como caso especial y así dar al administrador de una red local mayor control sobre el uso de la red, con el fin de hacer comprobaciones en el sentido de acceso indebido por parte de personal no autorizado (hackers).

1.5.1.7 Algoritmo de ruteo IP

Hasta el momento se ha hablado sobre el algoritmo de ruteo IP, por lo tanto se muestra su estructura a continuación:

"RutaDatagrama (Datagrama, Tabla de Ruteo).- Extraer la dirección IP de destino, D, del datagrama y computar el prefijo de red, N; si N corresponde a cualquier dirección de red directamente conectada entregar al destino D sobre dicha red (esto comprende la transformación de D en una dirección física, encapsulando el datagrama y enviando la trama).[36]"

[36] Fuente: COMER, Douglas. Redes Globales de Información con Internet y TCP/IP. Tercera edición. Prentice Hall. México. 1996.. Página: 118

“De otra forma, si la tabla contiene una ruta con anfitrión específico para D, enviar el datagrama al salto siguiente especificado en la tabla; de otra forma, si la tabla contiene una ruta para la red N, enviar el datagrama al salto siguiente especificado en la tabla; de otra forma, si la tabla contiene una ruta asignada por omisión, enviar el datagrama al ruteador asignado por omisión especificado en la tabla; de otra forma, declarar un error de ruteo.[37]“

1.5.1.8 Ruteo con direcciones IP

El ruteo IP no altera en nada el datagrama original a excepción de la disminución del tiempo de vida y el volver a computar la suma de verificación.

Al seleccionar, el algoritmo de ruteo IP, una dirección IP en realidad esta seleccionando un *salto al siguiente*, ya que con esto se sabe a donde se enviará después el datagrama. El valor de salto al siguiente, se almacena en el software de interfaz de red y este lo transforma en una dirección física, después crea una trama en base a esta dirección física, para a continuación poner el datagrama en la porción de datos de la trama y enviar el resultado. Después de utilizar la dirección de salto al siguiente para encontrar la dirección física, el software de interfaz de red la descarta.

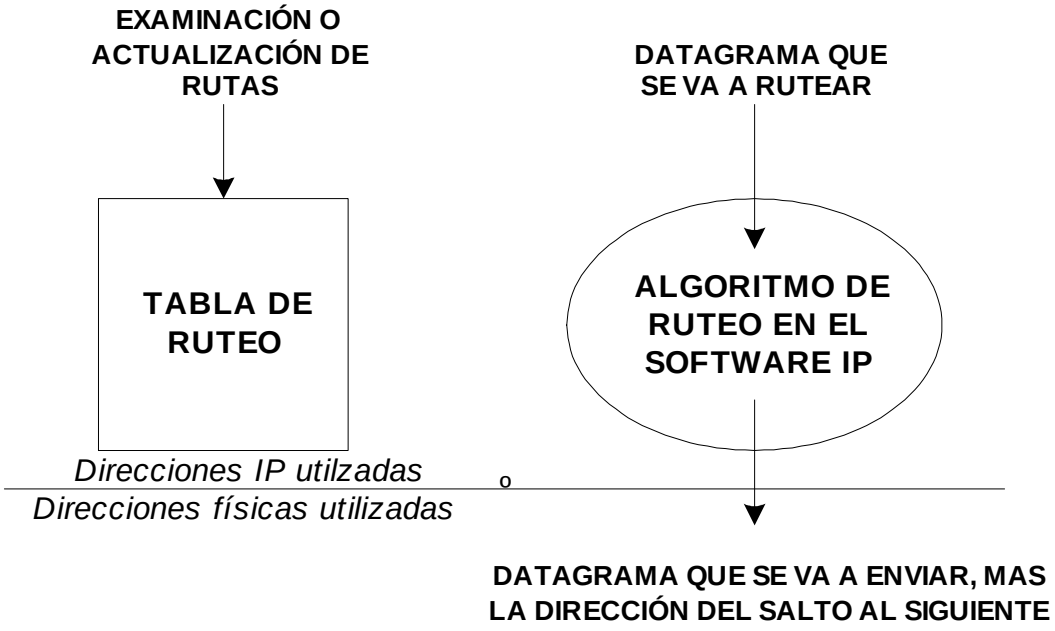
La dirección IP de salto al siguiente se almacena en la tabla de ruteo el momento en que se produce la traducción de esta dirección en dirección física y antes de que se envíe el datagrama. El software IP extrae la dirección de destino en cada uno de los datagramas y mediante la tabla de ruteo obtiene la dirección de salto siguiente, para seguidamente entregar a la interfaz de red estos dos datos, y que ésta pueda computar nuevamente la asignación para obtener una dirección física.

Esta labor sería muy ineficiente si un anfitrión enviara una serie de datagramas a la misma dirección de destino, ya que la interfaz de red tendría que computar nuevamente la misma información por cada datagrama, pero si la tabla de ruteo

[37] Fuente: COMER, Douglas. Redes Globales de Información con Internet y TCP/IP. Tercera edición. Prentice Hall. México. 1996.. Página: 118

utilizó direcciones físicas, la transformación se llevará a cabo una sola vez, evitando así costos computacionales innecesarios.

GRÁFICO 1. 14
EL SOFTWARE IP Y LA TABLA DE RUTEO QUE UTILIZA, RESIDEN ARRIBA DE LA FRONTERA DE DIRECCIÓN.



Fuente: COMER, Douglas. Redes Globales de Información con Internet y TCP/IP. Tercera edición. Prentice Hall. México. 1996. Página: 119

1.5.1.9 MANEJO DE LOS DATAGRAMAS ENTRANTES

A continuación veremos como es el procesamiento de los datagramas entrantes.

El software de interfaz de red es el encargado de enviar los datagramas al software IP, este último a su vez lo envía al software de alto nivel apropiado, para su posterior procesamiento. Si el datagrama tiene como dirección de destino la del anfitrión, entonces el software IP lo acepta, de lo contrario debe descartarlo con la restricción de que el anfitrión esta prohibido direccionar datagramas que accidentalmente se rutearon al anfitrión.

Los únicos que pueden realizar ruteo son los ruteadores y estos entregan dichos datagramas al software IP. Una vez hecho esto surgen dos alternativas: primero, que el datagrama haya llegado a su lugar de dirección destino, es decir que corresponda a la dirección IP, en este caso el software IP debe enviar el datagrama al software de protocolo de mas alto nivel para que realice su procesamiento, segundo, que el datagrama no llegue a su dirección de destino, para lo cual el software IP encaminará el datagrama utilizando el algoritmo de ruteo así como la tabla de ruteo local.

Si un anfitrión tiene muchas conexiones físicas cada una con sus respectivas direcciones IP, el momento que le llegue el datagrama tiene que comparar la dirección de destino de ésta con cada una de sus direcciones IP. Lo mismo debe realizar cuando le llegan datagramas por difusión en la red física. Si a pesar de hacer estos procedimientos la dirección de destino no corresponde a ninguna de las direcciones de la máquina local, el software IP disminuye el valor del TTL[38] en el datagrama, el cual se encuentra en el encabezado de éste, para que llegue a un valor de cero y lo descarte o computa una nueva suma de verificación y rutea el datagrama si la cuenta es positiva.

Un anfitrión puede direccionar datagramas entrantes, aun que no es su función, siempre y cuando su diseño de configuración lo permita, de lo contrario debe descartarlos.

1.5.2 TABLAS DE ENRUTAMIENTO

Todos los ruteadores que ejecutan TCP/IP tienen una tabla cuya función es dar solución a los problemas de enrutamiento.

La siguiente figura muestra una tabla de enrutamiento y los parámetros de esta los detallaremos a continuación:

---

[38] Según el c*entro de ayuda y soporte técnico Windows XP profesional*- Valor de un temporizador incluido en los paquetes enviados a través de redes basadas en TCP/IP que informa a los destinatarios de cuánto tiempo pueden mantener o utilizar el paquete o los datos incluidos en él antes de que caduquen o se descarten.

Tabla 1. 2

Tabla de enrutamiento IP

Destino	Máscara de red	Puerta de enlace	Interfaz	Métrica	Protocolo
10.57.76.0	255.0.0.0	10.57.76.1	Local Area C	1	Local
10.57.76.1	255.255.255.255	127.0.0.1	Loopback	1	Local
10.255.255.255	255.255.255.255	10.57.76.1	Local Area C	1	Local
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.45.0	255.255.255.0	192.168.45.1	Local Area C	1	Local
192.168.45.1	255.255.255.255	127.0.0.1	Loopback	1	Local
224.0.0.0	224.0.0.0	192.168.45.1	Local Area C	1	Local
224.0.0.0	224.0.0.0	10.57.76.1	Local Area C	1	Local

Ejemplo de tabla de enrutamiento.

Destino.- Este valor es la dirección IP de un host, una subred, una red o una ruta predeterminada de destino (0.0.0.0).

Máscara de red.- En esta se determina que parte identifica la red y cuales computadores en la red puede denotarse con el número de bits del comienzo de la dirección que identifican la red. Por ejemplo, una ruta de host tiene una máscara 255.255.255.255, la ruta predeterminada tiene una máscara 0.0.0.0 y una ruta de red o de subred tiene una máscara comprendida entre estos dos extremos.

Puerta de enlace.- Es la dirección IP del siguiente enrutador a través del cual se enviará los paquetes de datos.

Interfaz.- La interfaz indica la interfaz LAN o de marcado a petición que se va a utilizar para alcanzar el siguiente enrutador.

Métrica.- Es un valor relativo (costo en utilizar una ruta) que esta dado por el número de saltos que deben efectuar los paquetes hasta llegar a su destino final. Si existen varias rutas al mismo destino, la ruta con menor métrica es la ruta más adecuada.

Protocolo.- Este dato indica cómo el enrutador aprendió la ruta. Si en esta casilla se encuentra RIP u OSPF, quiere decir que el enrutador está recibiendo las rutas.

1.5.3 PRINCIPALES PROTOCOLOS DE ENRUTAMIENTO

No se debe olvidar que el enrutamiento es parte de la capa de red, pero la función principal de los protocolos de enrutamiento es que los ruteadores puedan intercambiar información entre si, llegando estos a comportarse como protocolos de aplicación.

Como se observa el ruteo IP se basa en información que esté almacenada en las tablas de ruteo. En los anfitriones finales por lo general el ingreso o la configuración de esta información, así como la dirección IP de la máquina, la red local y el default gateway es manual, y la persona encargada es el administrador de la red. A este tipo de configuración se las llaman rutas *estáticas*. Realizar esta labor en redes pequeñas no es problema, pero en casos donde existen varias redes locales es obvio que también existirá muchos ruteadores y la configuración de las tablas de ruteo por parte del administrador va a ser inmanejable, con el fin de corregir este problema, los administradores recurren a protocolos automáticos que son los que se encargaran de realizar este trabajo.

Debido a que el ruteo en Internet es complejo se han creado dos familias de protocolos que son los protocolos internos (IGP Interior Gateway Protocol) los cuales se encargan de mantener las tablas de ruteo en redes de tamaño mediano

con un solo sistema AS[39], como por ejemplo: instituciones, universidades e incluso cubre hasta un país. Y los protocolos externos (EGP Exterior Gateway Protocol) se encargan del intercambio de información entre distintos AS es decir el ruteo a escala mayor como por ejemplo: el Internet global.

Los IGPs más usados son:

- Protocolo Hello
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)

Los EGPs más usados son dos:

- Exterior Gateway Protocol (EGP)
- Border Gateway Protocol (BGP)

1.5.3.1 Protocolo Hello

Este protocolo esta descrito con más detalle en el RFC 891. La comunicación se la realiza mediante datagramas IP en los cuales se encuentran mensajes Hello, utiliza el algoritmo de ruteo vector-distancia el cual no utiliza conteo de saltos.

Un host físico DCN ("Distributed Computer Network") es un procesador que aporta un número de procesos cooperativos secuenciales. Estos host se identifican por su ID de host y cada uno de los host tienen dos tablas que son:

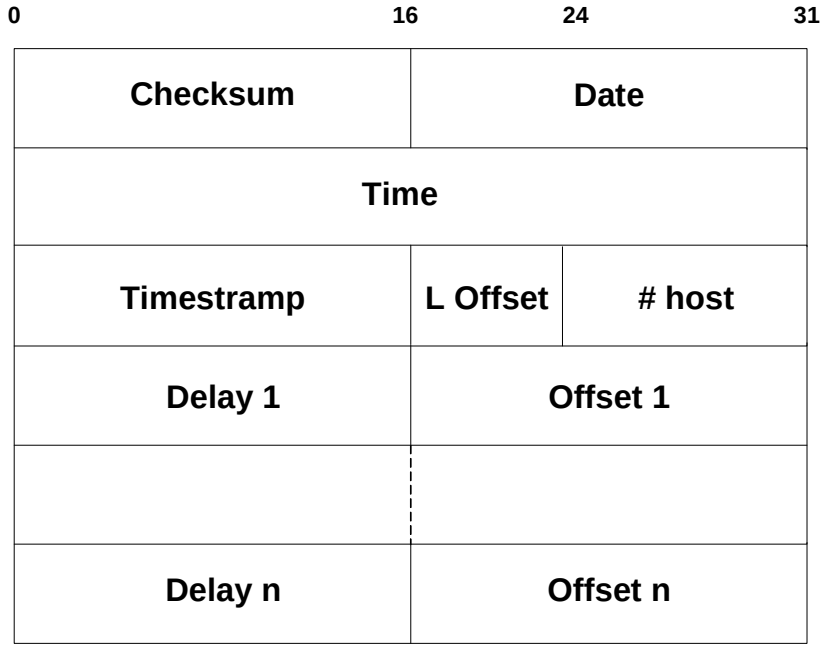
Tabla de host.- Esta contiene estimados del retardo del viaje de ida y vuelta y un desplazamiento lógico de reloj.

Tabla de red.- En esta tabla se asigna una entrada por cada red sea vecina o no a la red local.
La estructura del mensaje Hello es el siguiente:

[39] Grupo de redes que se administran como una unidad

GRÁFICO 1. 15

FORMATO MENSAJE HELLO



Fuente: Anónimo. Biblioteca personal. Capítulo 3. Protocolos de encaminamiento. Página 127.

Donde:

"Cheksum.- Contiene un checksum cubriendo los campos indicados.

Date.- Es la fecha local del host.

Time.- Es la hora local del host

Timestramp.- Usado en cálculos del tiempo de viaje

L Offset.- Contiene el desplazamiento del bloque de entradas de direcciones de Internet en la red local.

#hosts.- Contiene el número de entradas de la tabla de host siguiente

Delay n.- Retardo hasta el host n.

Offset n.- Offset hasta el host n (diferencia entre los relojes)"[40].

[40] ANÓNIMO. Biblioteca personal. Capítulo 3. Protocolos de encaminamiento. Página 127

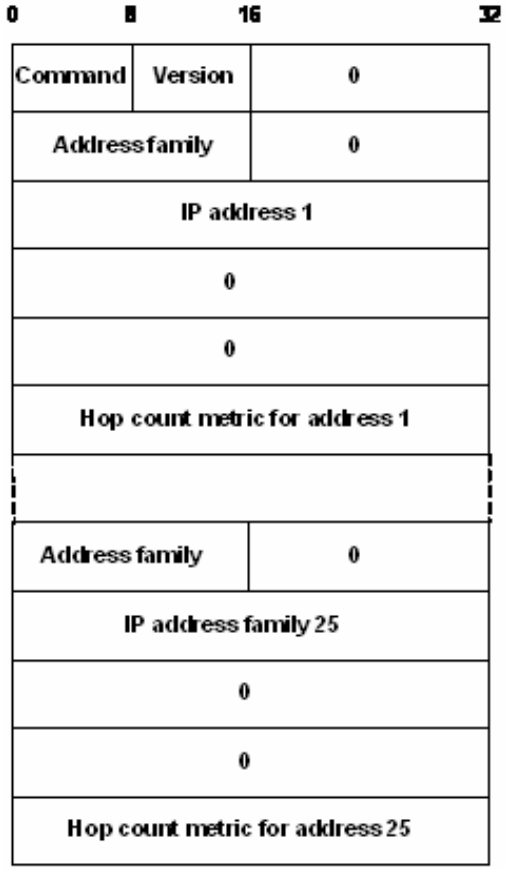
1.5.3.2 Protocolo RIP

Información más ampliada sobre este protocolo se encuentra en el RFC 1058. El RIP utiliza el demonio routed, pero también utiliza el demonio de encaminamiento gated. Este protocolo se origino tomando como base los protocolos de encaminamiento PUP y XNS de Xerox PUP, utiliza el protocolo de transporte UDP (User Datagram Protocol), el número de puerto es 520 y el algoritmo de encaminamiento vector-distancia. RIP opera en uno de los dos modos de funcionamiento: activo que es usado por los routers y pasivo que es usado por los hosts y estos escuchan todos los mensajes de broadcast.

El mensaje RIP se lo puede listar entre 1 y 25 rutas llegando a tener el datagrama un máximo de 504 bytes.

El formato del protocolo RIP es:

GRÁFICO 1. 16
ESTRUCTURA DEL MENSAJE RIP



Fuente: Anónimo. Biblioteca personal. Capítulo 3. Protocolos de encaminamiento. Página 129.

Donde:

“Command.- El valor 1 es para petición RIP o 2 para una respuesta

Versión.- El valor es de 1

Address family.- Es 2 para dirección IP.

IP address.- Es la dirección IP para esta entrada de encaminamiento: un host o una subred (caso en el que el número de host es cero)

Hop count metric.- Es el número de saltos hasta el destino[41]”.

Este protocolo no esta diseñado para resolver problemas de encaminamiento y el RFC 1720 contiene un listado amplio de todas las limitaciones técnicas de este protocolo nombradas como graves, como por ejemplo: que es inadecuado para redes grandes ya que tiene un coste máximo permitido de 16 (la cuenta de saltos solo puede ser 16), no soporta subneting variable, protocolo inseguro, usa métricas fijas para comparar rutas alternativas basados en tiempo real (el retardo, la fiabilidad o la carga), depende de la cuenta hasta el infinito, entre otros.

1.5.3.3 Protocolo OSPF

El protocolo Open Shortest Path First Protocol es un borrador, se lo describe en forma más amplia en el RFC 1583, es un protocolo de encaminamiento interior pero puede trabajar como protocolo de encaminamiento exterior en conjunto con BGP (Border Gateway Protocol), es mucho más complejo que RIP con el único propósito de asegurar que las bases de datos topológicas sean las mismas en todos los routers dentro de un área.

Su número de puerto es el 89, utiliza el protocolo IP para comunicarse, es utilizada en redes punto a punto, broadcast (Ethernet, anillo) y en redes no broadcast (X25), permite subneting de longitud variable, proporciona balance de carga, todos los intercambios entre los routers OSPF se los puede autentificar mediante el uso de passwords.

---

[41] ANÓNIMO. Biblioteca personal. Capítulo 3. Protocolos de encaminamiento. Página 129.

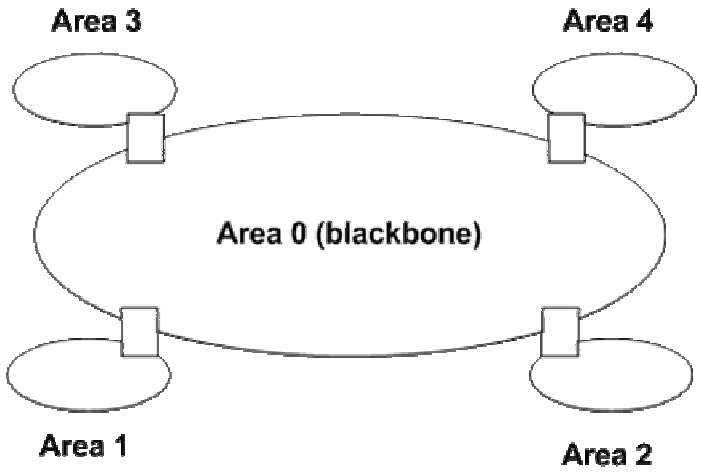
Además el protocolo OSPF realiza los siguientes trabajos:

- Descubre vecinos OSPF.
- Debe elegir al router que forme adyacencias con los demás routers de la red.
- Sincronizar bases de datos.
- Calcular la tabla de encaminamiento.
- Anunciar los estados de los enlaces.

La desventaja más predominante de este protocolo es el consumo de CPU puesto que el enlace sube y baja muy seguido trayendo consigo trastornos en el funcionamiento. Para evitar este inconveniente OSPF maneja el concepto de áreas, el cual permite dividir la red completa en varias áreas OSPF, para en estas aplicar el algoritmo de Dijkstra Shortest Path First completo. Cada una de estas áreas esta conectada a un backbone (área 0) que es una red de interconexión, permitiendo que cada área mantenga su propio estado y que los mensajes inunden sólo un área. OSPF recomienda que un área no deba contener más de 200 routers.

Esto se lo puede observar con mejor claridad en el siguiente gráfico:

GRÁFICO 1. 17
ÁREAS OSPF

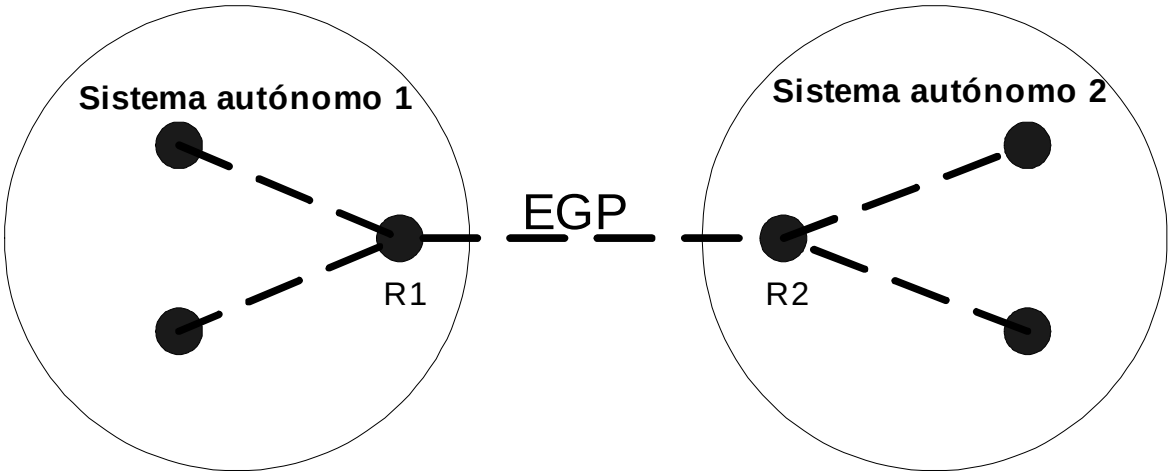


Fuente: PIQUER, José. Nivel de red.
http://www.dcc.uchile.cl/~jpiquer/Docencia/cc51c/apuntes/node5.html.
Acceso último: 06-04-2005

1.5.3.4 Protocolo EGP

Es un protocolo utilizado para el intercambio de información de encaminamiento entre ruteadores exteriores, esto significa, que no deben pertenecer al mismo sistema autónomo. Dos ruteadores pueden considerarse vecinas si están conectadas por una red, la cual es transparente para ambas, a dos sistemas autónomos diferentes, esto se lo consigue con el protocolo NAP (Neighbor Acquisition Protocol).

GRÁFICO 1. 18
ILUSTRACIÓN CONCEPTUAL DE DOS RUTEADORES EXTERIORES R1 Y R2 QUE UTILIZAN EL EGP PARA ANUNCIAR REDES EN SUS SISTEMAS AUTÓNOMOS LUEGO DE REUNIR LA INFORMACIÓN.



Fuente: COMER, Douglas. Redes Globales de Información con Internet y TCP/IP. Tercera edición. Prentice Hall. México. 1996. Página 256.

El tipo de información que se intercambian son mensajes Hello/I Hear You, para monitorear la accesibilidad de los vecinos y para sondear si hay solicitudes de actualización, esto lo hace mediante la utilización del protocolo NR (Neighbor Reachability).

EGP define los siguientes tipos de mensajes:

- Acquisition request.- Es la solicitud que una pasarela envía para convertirse en vecina.

- Acquisition Confirm.- Respuesta afirmativa a una solicitud Acquisition request.
- Acquisition Refuse.- Rechazo a una Acquisition request.
- Cease Confirm.- Confirmación de que cesen las peticiones.
- Hello.- Solicitud de respuesta a un vecino si esta vivo.
- I Hear You.- Respuesta al mensaje Hello.
- Poll Request.- Solicitud de la tabla de encaminamiento de la red.

1.5.3.5 Protocolo BGP

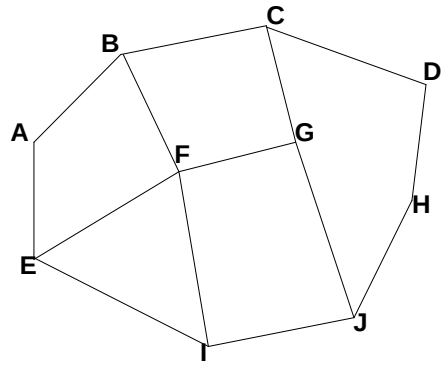
Este protocolo de encaminamiento Inter-AS, se creo en base al mejoramiento del protocolo EGP, esta orientado a conexión, es decir que utiliza el protocolo de transporte TCP, el número de puerto que trabaja es el 179, para una mayor descripción de este protocolo consultar el RFC 1267, 1268 y 1654.

BGP utiliza el protocolo vector-distancia, el cual es muy diferente al del protocolo RIP. "En lugar de mantener solo el costo a cada destino, cada enrutador BGP lleva el registro de la trayectoria seguida. Del mismo modo en lugar de dar periódicamente a cada vecino sus costos estimados de todo los destinos posibles, cada enrutador BGP le dice a sus vecinos la trayectoria exacta que está usando"[42].

A manera de ejemplo se analizará los enrutadores BGP mostrados en la figura siguiente y consideraremos la tabla de enrutamiento que tiene F para alcanzar el destino D. También se presentará la tabla de enrutamiento de los vecinos de F para llegar a D.

GRÁFICO 1. 19
ANÁLISIS DE UN ENRUTADOR QUE UTILIZA EL PROTOCOLO BGP

[42] TAENENBAUM, Andrew. Redes de computadoras. Tercera edición. Prentice Hall. México. 1997. página: 430



(a)

Información que F recibe de sus vecinos acerca de D

De B: “Yo uso BCD”
De G: “Yo uso GCD”
De I: “Yo uso IFGCD”
De E: “Yo uso EFGCD”

(b)

Figura: Grupo de enrutadores BGP, (b) Informción enviada a F

Fuente: TAENENBAUM, Andrew. Redes de computadoras. Tercera edición. Prentice Hall. México. 1997. página: 431.

Se asume que F usa la trayectoria FGCD. Una vez que f tiene las rutas de sus vecinos, las analiza y descarta las que pasan por su mismo nodo (I y E), según nuestro ejemplo entonces solo quedaría B o G. Los ruteadores BGP tienen módulo que analiza las rutas a un destino y les asigna una ponderación, entonces el ruteador toma la ruta con la distancia más corta mediante el algoritmo vector-distancia.

Si una ruta viola una restricción por política, automáticamente se le da una ponderación infinita. Cuando el algoritmo de enrutamiento vector-distancia analiza esta ruta, cae en el conteo infinito y se produce un problema el cual genera erradas decisiones al momento de elegir la ruta adecuada, afortunadamente BGP soluciona este tipo de inconvenientes.

1.5.4 SEGURIDAD, LISTAS DE ACCESO

“El problema de la seguridad consiste en lograr que los recursos de un sistema sean, bajo toda circunstancia, utilizados para los fines previstos. Para eso se utilizan mecanismos de protección.

Los sistemas operativos proveen algunos mecanismos de protección para poder implementar políticas de seguridad. Las políticas definen qué hay que hacer (qué datos y recursos deben protegerse de quién; es un problema de administración), y los mecanismos determinan cómo hay que hacerlo. Esta separación es importante en términos de flexibilidad, puesto que las políticas pueden variar en el tiempo y de una organización a otra. Los mismos mecanismos, si son flexibles, pueden usarse para implementar distintas políticas.[43]"

1.5.4.1 ¿QUÉ ES SEGURIDAD?

Según un diccionario muy conocido es: "un mecanismo que asegura el buen funcionamiento, precaviendo que este falle, se frustre o se violente[44]", en otras palabras, es una característica de cualquier sistema (informático o no), el mismo que garantiza que esta libre de peligro, daño o riesgo. También se podría decir que es un sistema infalible.

Lamentablemente, según la mayoría de los expertos, en informática y redes, es muy difícil conseguir esto, con el fin de suavizar esta negativa se habla de *fiabilidad.*

La fiabilidad es la probabilidad de que un sistema se comporte tal y como se espera de él, esto involucra tres aspectos: confiabilidad, integridad y disponibilidad.

- **Confiabilidad.-** Es que tan confiable es la calidad de un servicio determinado ofrecido.
- **Integridad.-** Es la característica en Asegurar que los objetos de un sistema se mantengan íntegros y que estos podrán ser alterados por elementos autorizados y bajo reglas de control.

---

[43] DUEÑAS, Francisco. Seguridad y protección en computación. Internet: http://monografias.com/trabajo6/sepro/sepro.shtml. Acceso último: 31/10/2004

[44] MICROSOFT. Seguridad. Diccionario Encarta® 2005.

- **Disponibilidad.-** Es la garantía que se ofrece al acceder a los objetos de un sistema por parte de los elementos autorizados.

Dependiendo del entorno en que se desenvuelva un sistema, se dará prioridad a uno de los tres aspectos antes mencionados. Por ejemplo, una entidad bancaria necesita de un medio físico de transmisión seguro y que los datos se mantengan íntegros en lugar de la disponibilidad, ya que para esta empresa no es importante que un usuario conozca los datos bancarios de otro cliente, pero si que este los pueda alterar.

En sistemas informáticos los tres elementos principales a proteger son: el hardware, el software y los datos. En *hardware* son todos los elementos físicos, claro esta, de un sistema informático; en *software* son todos los programas lógicos que hacen funcional a dichos elementos físicos y los *datos* es el conjunto de información que manejan tanto el software como el hardware.

1.5.4.2 LISTAS DE ACCESO

Las lista de control de acceso es un mecanismo que agrega una seguridad adicional a los ficheros (archivos), extendiendo de esta manera el clásico esquema de permisos Unix, ya que con este último solo se puede especificar permisos para los tres grupos de usuarios (U: propietario, G: grupo y O: otros), permitiendo de esta manera otorgar permisos a usuarios o grupos concretos; por ejemplo se puede otorgar permisos a dos usuarios sin necesidad que estos pertenezcan al mismo grupo, como usualmente no lo hace Linux. Si se requiere este servicio en Linux se debe instalar un software adicional, especialmente para los sistemas corporativos.

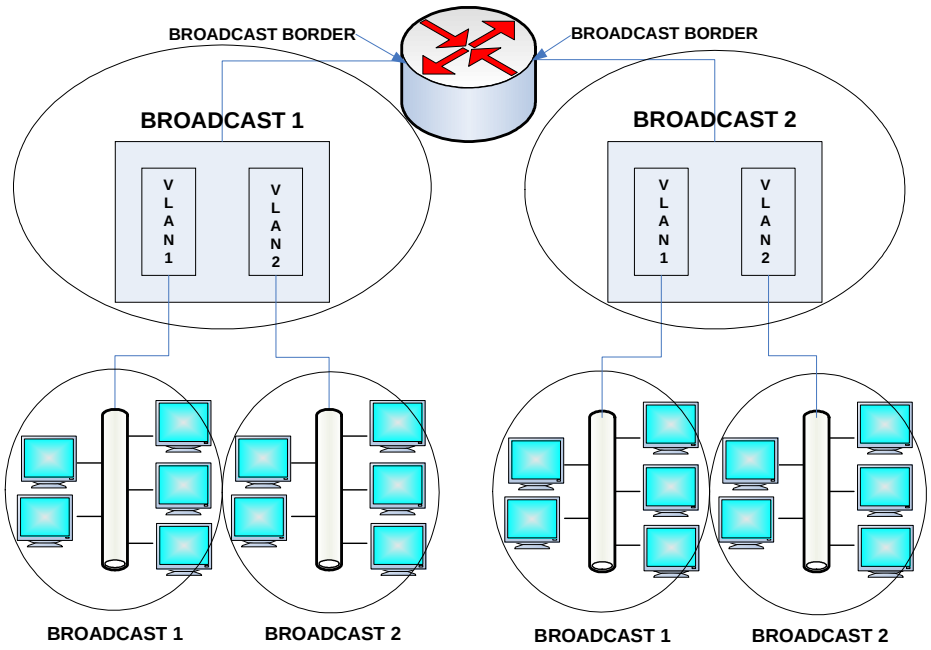
La seguridad adicional de los ficheros se basa en una lista de Entradas de Control de Acceso (ACEs), en el que cada una de estas contiene un par (usuario/grupo, permiso) que indica un tipo de acceso determinado para un usuario o grupo, y el conjunto de todas ellas forman la ACL que marca el tipo de acceso permitido en un fichero.

La lista de control de acceso se crea el instante en que se crea un fichero y tiene los mismos permisos que ese archivo tiene en el sistema. Además este sistema debido a su gran utilidad es usado en sistemas de ficheros NTFS, (Windows NT y posteriores), sistemas UFS (Solaris) y el sistema HFS (HP-UX).

1.5.4.3 DOMINIOS DE BROADCAST

Un dominio de broadcast se refiere al conjunto de dispositivos que reciben una trama de datos de broadcast desde cualquier dispositivo dentro de este conjunto. Todos los hosts que reciben una trama de datos de broadcast deben procesarla. Este proceso consume los recursos y el ancho de banda disponible del host. Los dispositivos de Capa 2 como los puentes y switches reducen el tamaño de un dominio de colisión. Estos dispositivos no reducen el tamaño del dominio de broadcast. Los routers reducen el tamaño del dominio de colisión y el tamaño del dominio de broadcast en la Capa 3.

GRÁFICO 1. 20
DOMINIOS DE BROADCAST



Ejemplo de un dominio de broadcast.

CAPITULO 2

DESARROLLO DEL PROTOTIPO DE SWITCH CAPA 3 BÁSICO BASADO EN LINUX

2.1 ESTUDIO DE LA SITUACIÓN ACTUAL DEL PROYECTO

2.1.1 ANTECEDENTES

La rápida evolución de la tecnología en el campo de las redes de información ha obligado a los diseñadores de hardware, presentar soluciones en la creación de redes virtuales, asignación dinámica de direcciones IP, velocidad de transmisión de datos, todo esto empaquetado en un solo equipo, pero con costos muy elevados para pequeñas y medianas empresas, obligándolas a que éstas se queden rezagadas en este tipo de tecnologías.

2.1.2 SITUACIÓN ACTUAL

En el medio, actualmente no existe una solución asequible, para las medianas y pequeñas empresas, en la compra de equipos de última tecnología en el ámbito de las redes de información, para esto, se presenta mediante este proyecto de tesis la solución básica a este requerimiento, mediante la utilización de equipos y dispositivos electrónicos de bajo costo, reduciendo así notablemente el valor económico de este conjunto de funciones y manteniendo su eficacia y rendimiento.

2.1.3 REQUERIMIENTOS HARDWARE

Para la implementación a esta solución, los requerimientos básicos son:

Computador personal con procesador de 1.7 Ghz

Espacio físico en disco de 5 GB

Memoria en RAM 512 Mbytes

Lector de CD`s

Slots PCI 3

3 Tarjetas de red 10/100

Cables de red UTP categoría 5

3 Switch

2.1.4 REQUERIMIENTOS SOFTWARE

Para el desarrollo del proyecto se utilizó el siguiente software:

Sistema Operativo CentOS – 4.0; Kernel V.2.4

Paquetes utilizados:

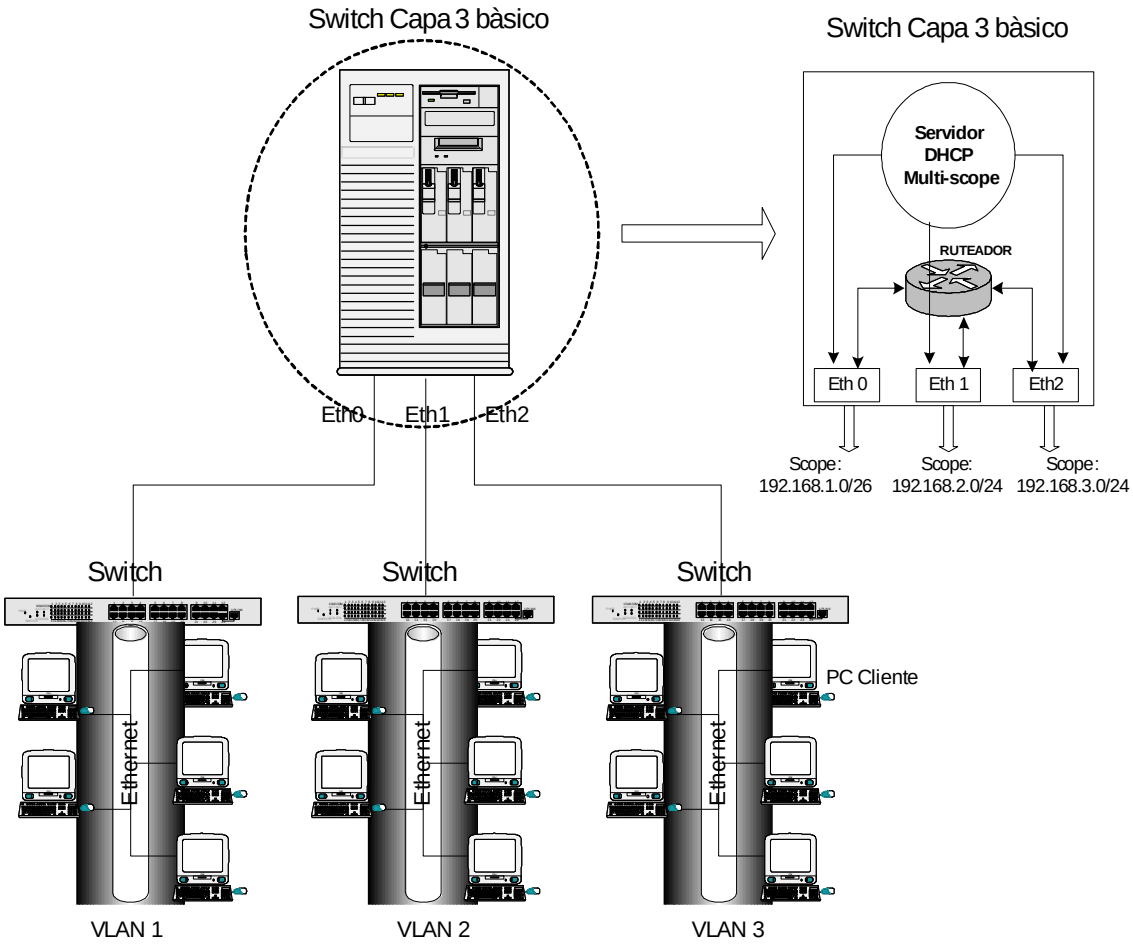
- DHCP
- BIND 9.0
- IPTABLES
- APACHE WEB SERVER
- PHP 4.3.4

Lenguajes utilizados:

- HTML
- XML
- PHP
- JAVA SCRIPT

2.2 DISEÑO DEL SWITCH CAPA 3 BÁSICO

GRÁFICO 2. 1
ESQUEMA DEL SWITCH CAPA 3 BÁSICO



Esquema funcional del switch básico capa 3 basado en Linux

Para la construcción del switch capa 3 básico se utiliza un computador el cual posee 3 slots PCI, como mínimo, en donde se insertan las interfaces de red (Eth0, Eth1, Eth2) que son las que formaran las 3 VLAN`s.

Para la creación de las VLAN`s se utiliza la tecnología DHCP Multi-Scope y para conceder permisos o ciertos privilegios a los clientes de las VLAN's, también se configura el servidor como ruteador y Firewall a la vez.

Al crear VLAN's por medio del switch se reduce dominios de colisión y el excesivo broadcast, además la utilización de los swiitches son para mantener la velocidad de la red en todos los puntos de red e incrementar el número de clientes en cada VLAN.

2.3 IMPLEMENTACIÓN DEL SWITCH CAPA 3 BÁSICO

2.3.1 LINUX COMO SERVIDOR DE RED

2.3.1.1 Introducción al Sistema Operativo Linux

Linux es la versión de código abierto de Unix y se lo distribuye bajo los términos de la GNU General Public Licency.

Este sistema operativo tiene dos ventajas en relación a otros en el mercado que son: su libre distribución y su sistema viene acompañado del código fuente. Esto es posible ya que su desarrollo va creciendo gracias a programadores voluntarios que en base a foros abiertos, investigaciones, intercambian código, comentan y analizan errores dando solución a estos inconvenientes. El sistema Linux esta formado por el núcleo del sistema llamado kernel, el shell que es la interfaz entre el usuario y el kernel, el sistema de archivos el cual organiza la forma como se almacena los archivos en los dispositivos de almacenamiento y las utilidades.

2.3.1.2 Características Principales Sistema Operativo Linux

El sistema operativo Linux posee las siguientes características:

Linux y sus Shells: Shell conocido también como interfaz de usuario es aquel que conecta las órdenes de un usuario con el Kernel de Linux (núcleo del sistema), es programable razón por la cual se puede modificar y adaptar a una necesidad específica.

Multitarea: La multitarea consiste en ejecutar múltiples programas a la vez, esto no significa que el procesador realice más de un trabajo al mismo tiempo, sino lo

que realiza es presentar las tareas de forma intercalada para que se ejecuten varias simultáneamente.

Multiusuario: Consiste en que varios usuarios pueden acceder a las aplicaciones y recursos del sistema Linux en tiempos tan cortos que a éstos les parece que es al mismo tiempo. Y, por supuesto, cada uno de ellos puede ejecutar varios programas a la vez (multitarea).

Seguridad: Linux utiliza un sistema de contraseñas que protege el acceso al sistema se basa en el algoritmo DES, que es el más probado de los algoritmos de seguridad.

Linux y su Control de Dispositivos: Los controladores de dispositivos son manejados de forma independiente al núcleo del sistema, y por lo tanto se podrá añadir tantos controladores como dispositivos nuevos se vayan añadiendo al ordenador.

Linux y las Redes de Ordenadores: Linux es un sistema operativo orientado al trabajo de redes de ordenadores. Dispone de varios protocolos para la transferencia de archivos entre plataforma. Tiene a su disposición multitud de aplicaciones de libre distribución que permiten navegar a través de Internet y enviar y recibir correo electrónico. Posee gran variedad de comandos para comunicación interna entre usuarios que se encuentren ubicados en plataformas distintas (Telnet).

Independencia de dispositivos: Linux admite cualquier tipo de dispositivo (módems, impresoras, etc.) gracias a que cada una vez instalado uno nuevo, se añade al Kernel el enlace o controlador necesario con el dispositivo, haciendo que el Kernel y el enlace se fusionen.

Comunicaciones Linux es el sistema más flexible para poder conectarse a cualquier ordenador del mundo. Internet se creó y desarrolló dentro del mundo de Unix, y por lo tanto Linux tiene las mayores capacidades para navegar, ya que

Unix y Linux son sistemas prácticamente idénticos. Con Linux podrá montar un servidor su propia casa sin tener que pagar las enormes cantidades de dinero que piden otros sistemas.

El kernel en Linux

El kernel denominado también núcleo del sistema es un programa que tiene el control de la máquina y administra los recursos. El sistema operativo es el resultado de la unión del kernel con todas las herramientas necesarias para que la máquina pueda funcionar. Su función es que el software y hardware trabajen en conjunto.

Las principales funciones que realiza el kernel son las siguientes:

- "Administración de la memoria, para todos los programas en ejecución.
- Administración del tiempo de procesador, que estos programas en ejecución utilizan.
- Es el encargado para acceder a los periféricos/elementos de nuestro ordenador de una manera cómoda.[45]"

Existe un esquema de numeración para la versión del kernel, el cual es numerado en el siguiente formato: 2.2.14, el primer dígito representa la versión primaria (actualmente sólo existen 1 y 2); el segundo dígito indica la versión secundaria que puede ser de dos tipos: estable (número par) o en producción (número impar), esto un estándar por los desarrolladores del sistema; y el tercer dígito es simplemente un incremento por cada liberación de la versión secundaria.

[45] ANONIMO. Sistema Operativo Linux. http://www.monografias.com/trabajos6/sisop/sisop.shtml. Ultimo Acceso: 02/10/2005.

2.3.1.3 Linux como servidor de red

Linux desde sus inicios se desarrolló para dotarle con capacidades de red, ofrece una gran variedad de controladores para dispositivos, así como también múltiples características avanzadas y soporte de TCP/IP.

Dentro de los protocolos estándar se incluye SLIP y PPP (para el envío de tráfico de redes sobre líneas series), PLIP (para líneas paralelas), IPX (protocolo para redes compatibles con NOVELL), Appletalk (para redes Apple), y AX.25.

Otras características que acentúan la flexibilidad de Linux están relacionadas a que incluye un sistema de ficheros, cortafuegos IP, contabilidad IP, enmascaramiento IP, soporta encapsulación IP dando lugar al encaminamiento (routing).

Soporta variedad de dispositivos de red Ethernet, así como también dispositivos FDDI, Token Ring, Frame Relay, tarjetas ISDN y ATM.

2.3.1.4 Servicios de Linux

Linux es un sistema operativo orientado a redes de computadores, el mismo que se lo configura para que trabaje con múltiples protocolos y ofrezca múltiples servicios de red, entre los más importantes listamos a continuación:

- Servidor Web
- Servidor de impresión
- Servidor de archivos (compartir archivos entre Windows, Mac, Novell, Unix y Linux)
- Servidor de correo
- Servidor DHCP
- Firewall
- Servidor de fax
- Servidor IRC
- Servidor FTP

- Servidor de bases de datos (Oracle, Informix, MySQL, PostgreSQL, etc)
- Servidor de desarrollo

2.3.1.5 El Súper Servidor inetd

"Los programas que proporcionan servicios de aplicación a través de la red se llaman demonios. Un demonio es un programa que abre un puerto, comúnmente un puerto de algún servicio bien conocido y espera conexiones entrantes en él. Si ocurre una, el demonio crea un proceso hijo que acepta la conexión, mientras que el proceso padre continúa escuchando más peticiones.

Linux ejecuta un demonio de red especial, el cual debe ser considerado como súper servidor, el mismo que crea sockets en nombre de cada uno de los servicios y escucha en todos ellos simultáneamente. Al momento que una conexión entrante es recibida en cualquiera de esos sockets el súper servidor acepta la conexión replica el servicio especificado para ese puerto, pasando el socket a gestionarse a través del proceso hijo. El servidor entonces vuelve a la escucha"[46].

El demonio inetd es el súper servidor más común, el cual se inicializa en el momento que se arranca el sistema y toma la lista de servicios (por ejemplo: dhcp, dns, proxy, etc.) que ha de gestionar de un fichero de inicialización denominado /etc./inetd.conf.

2.3.1.6 El servidor Telnet

Telnet es uno de los servicios más básicos y antiguos, es aquel que permite ingresar a un servidor remoto, con un usuario y contraseña, y acceder a ese servidor como si estuviéramos conectados desde un Terminal, el inconveniente de este servidor es que se lo considera inseguro ya que por medio de su puerto pueden personas, ajenas a la red, ingresar y causar graves perjuicios, es por eso que muchos administradores han optado cerrar dicho puerto.

---

[46] KIRCH, Olaf ; DAWSON, Terry. Guía de Administración de Redes con Linux. http://es.tldp.org/Manuales-LuCAS/GARL2/garl-2.0.pdf . Página 190. Ultimo Acceso: 05/10/2005.

2.3.1.7 El servidor Web

El servicio Web por el momento es prácticamente el más utilizado en Internet, por lo general se lo utiliza a través de un programa especialmente pensado para ello (browser o navegador), el cual conoce tanto el protocolo HTTP, como el lenguaje HTML en que recibe el contenido que muestra en pantalla. El protocolo que se utiliza en este servicio es el HTTP (Hyper Text Transfer Protocol) y normalmente utiliza el puerto 80.

2.3.1.8 El servicio FTP

El servicio FTP (File Transfer Protocol), es aquel que sirve para bajar o subir archivos a un determinado servidor, por lo general este servicio utiliza el puerto 21. Existen varios comandos para realizar diversas tareas como subir o bajar directorios completos.

2.3.1.9 El Servidor DHCP

El servidor DHCP (Dinamic Host Configuration Protocol) es utilizado para redes en donde se desea que un cliente obtenga una Dirección IP dinámica en forma automática. El demonio actúa enviando información de la red a las estaciones de trabajo, a más de la Dirección IP, envía los parámetros como Máscara de Subred, Servidores DNS, Puerta de enlace, etc.

2.3.1.10 El servicio DNS

Todas las computadoras que pertenecen a una red poseen una dirección IP única que permite identificarles a cada una, a cada dirección IP se le asigna un nombre único, cuando se asigna mas de un nombre se denomina un alias, el mecanismo para obtener la dirección IP a través del nombre se denomina resolución del nombre.

El sistema DNS es en esencia una base de datos distribuida, que realiza la traslación entre nombre y dirección IP, su estructura es en forma jerárquica o de árbol. Esto significa que se especifica dominios separados por puntos, el más alto de derecha a izquierda describe una categoría, institución o país, por ejemplo:

COM	Uso Comercial en general.
INFO	Información en general.
NET	Proveedores de Servicios de Internet.
FIN	Entidades e Instituciones de Servicios Financieros.
MED	Entidades e Instituciones Medicas, de Salud, etc.
PRO	Para profesionales en general como abogados, etc.
ORG	Solo para Entidades e Instituciones sin fines de lucro, Organizaciones no gubernamentales
.EDU	Solo para Entidades, Instituciones u Organizaciones Educativas.
.GOV	Solo para uso del Gobierno.
.MIL.	Solo para uso de las Fuerzas Armadas del Ecuador

El segundo nivel representa la organización, el tercero y restantes son departamentos o secciones dentro de una organización. Ejemplo:

www.microsoft.com
www.linux.org

A un nombre de dominio que incluye todos los nodos hasta la raíz se le denomina: nombre de dominio completamente cualificado (FQDN Full Qualified Domain Name). Existen organizaciones que controlan la asignación de nombres a direcciones IP, por ejemplo InterNIC.

2.3.1.11 El servicio de routing

En un nodo con múltiples conexiones, el routing consiste en decidir dónde hay que enviar y que se recibe. Aunque existiera un nodo simple con sólo una conexión de red es necesario de routing, ya que todos los nodos disponen de un loopback y una conexión de red, de la misma manera ocurre cuando varias computadoras que pertenezcan a una red estén conectadas directamente.

Existe la tabla denominada tabla de ruteo, la misma que contiene diversos campos, pero los tres principales son: dirección de destino, interfaz por donde saldrá el mensaje y dirección IP, que efectuará el paso siguiente en la red.

Cuando se desea interconectar varias redes entre si es necesario un equipo que se encargue de rutear la información de una red a la otra. En este equipo existirá una configuración de las rutas que deben seguir los paquetes de información dentro de cada red.

2.3.1.12 Seguridad del sistema

La seguridad es un aspecto fundamental en la administración de sistemas en un entorno de red, lo cual implica dos objetivos primordiales que es proteger al sistema en sí y a sus usuarios de intrusos.

En un sistema donde la seguridad no es administrada correctamente existen muchos huecos o vulnerabilidades los mismos que pueden causar daños desde mensajes de correos falsos hasta perdida de datos o violación de la privacidad de los usuarios.

"La seguridad del sistema comienza con una buena administración del mismo. Esto incluye comprobar las propiedades y permisos de todos los ficheros y directorios vitales, monitorizar el uso de cuentas privilegiadas, etc.[47]"

Linux ofrece varias técnicas y herramientas que aportan para obtener un sistema de seguridad estable, por ejemplo el programa COPS, sirve para comprobar el sistema de ficheros y ficheros de configuraciones generales, en busca de permisos inusuales u otras anomalías, el sistema Linux utiliza un sistema de contraseñas que se basa en el algoritmo DES que es el mas probado de los algoritmos de seguridad, las herramientas SSH usan un método de autentificación confiable, además de proporcionar otros servicios como encriptación y compresión.

Todo esto combinado con buenas técnicas de seguridad como por ejemplo dar el menor privilegio cuando un servicio se hace accesible a la red, restricción de cier-

[47] KIRCH,Olaf; DAWSON, Terry. Guía de Administración de Redes con Linux. http://es.tldp.org/Manuales-LuCAS/GARL2/garl-2.0.pdf. Página 36. Ultimo Acceso: 05/10/2005.

tos servicios a usuarios, etc., se logra un sistema estable.

2.3.1.13 El servicio de Firewall

Un aspecto fundamental en la seguridad informática es el Firewall o cortafuegos tiene por objetivo evitar o reducir los accesos no autorizados, ataques de suplantación de identidad, ataques de negación de servicio a nivel de red.

El Firewall consiste en una máquina segura y confiable que por lo general se sitúa entre una red privada y una red pública, es configurada con un conjunto de reglas que determinan que tipo de tráfico se le permitirá pasar y cual tráfico será bloqueado.

Linux proporciona un rango de características internas que le permiten funcionar bien como un cortafuegos de IP, es muy flexible para su configuración debido a que la implementación de red incluye código para realizar filtros a nivel de IP en numerosas formas y proporciona un mecanismo para configurar con precisión que tipos de reglas le gustaría imponer.

2.3.2 INSTALACIÓN Y CONFIGURACIÓN DE UNA INTERFAZ DE RED.

Para la instalación de una interfaz de Red (NIC), se recomienda insertar cada tarjeta de una manera ordenada, ascendente o descendente, con el fin de que el Administrador reconozca cada interfaz de red (eth0, eth1, eht2,… ethx) de manera visual e inmediata.

En los sistemas Linux actuales, por lo general reconocen estas tarjetas de manera automática, sin necesidad de driver alguno, ya que éstos vienen implícitamente en el Kernel. Caso contrario se procederá a instalar el driver en el Kernel. En caso de sistemas Windows se procede de la misma manera.

Para la configuración de una Interfaz de Red en Linux, se lo puede realizar de dos maneras, una en modo comando y la otra en modo gráfico.

2.3.2.1 Configuración Modo Comando en Linux

Esta configuración se lo realiza mediante la siguiente línea de comando:

ifconfig eth0 192.168.1.1 netmask 255.255.255.192

Donde:

Eth0: identifica a la primera tarjeta de red instalada
192.168.1.1: Representa la Dirección IP asignada a esta tarjeta
netmask: Representa la máscara de la red.

La verificación de la configuración realizada se utiliza el siguiente comando, el mismo que presenta una lista de todos las interfaces de red instaladas en ese equipo:

ifconfig

La segunda tarjeta está representada por la etiqueta eth1, la tercera por la eth2 y así sucesivamente.

A una misma tarjeta de red se la puede configurar con dos o más direcciones IP, con el fin de crear redes virtuales. A este procedimiento se lo denomina Alias IP y se lo hace mediante la siguiente línea de comando:

ifconfig eth0:1 192.168.2.1 netmask 255.255.255.192

2.3.2.2 Configuración Modo Gráfico en Linux

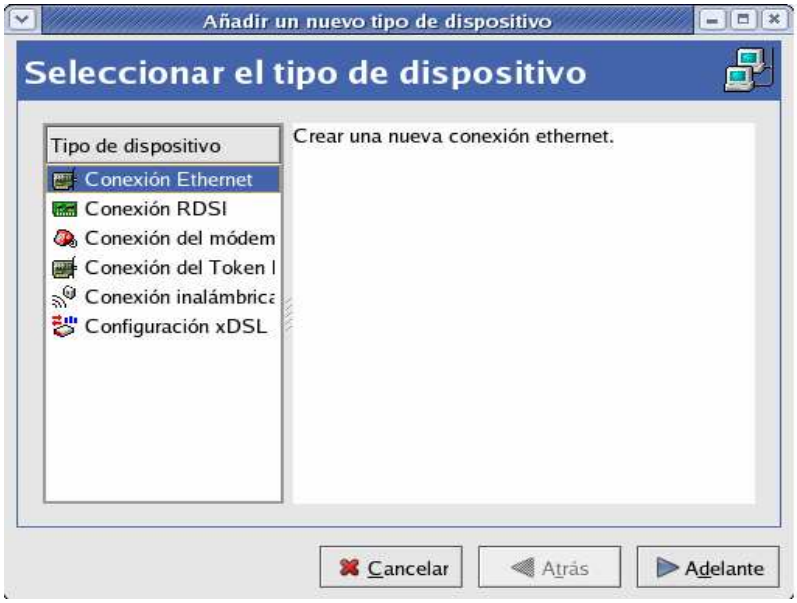
Los pasos a realizarse son los siguientes:

Navegar por el menú Aplicaciones
-> Herramientas del sistema
-> Controles de Dispositivos de Red
-> Configurar
-> Nuevo

En Tipo de Dispositivo, elegir Conexión Ethernet, pulsar Adelante

GRÁFICO 2. 2

SELECCIÓN DEL TIPO DE DISPOSITIVO



Fuente: SISTEMA OPERATIVO CENTOS. Configuración Interfaz de Red. Modo Gráfico.

En *Seleccionar el dispositivo Ethernet*, elegir la interfaz de red que se desea configurar (eth0, eth1, etc.), pulsar *Adelante*.

GRÁFICO 2. 3

SELECCIÓN DE DISPOSITIVO ETHERNET

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Configuración Interfaz de Red.

En *Configuración de las opciones de Red*, escoger *Configurar las direcciones IP de manera estática*. Pulsar Adelante.

GRÁFICO 2. 4

CONFIGURACIÓN DE LAS OPCIONES DE RED

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Configuración Interfaz de Red.

En *Configuración de las opciones de Red*, ingresar la dirección IP, Máscara de Subred, Dirección de la puerta de enlace, en los campos respectivos.

GRÁFICO 2. 5

CONFIGURACIÓN DE DIRECCIÓN EN FORMA DINÁMICA

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Configuración Interfaz de Red.

En *Creación de un dispositivo de Red*, verificar si los datos con que se configuró la tarjeta son correctos y pulsar en Aplicar.

GRÁFICO 2. 6

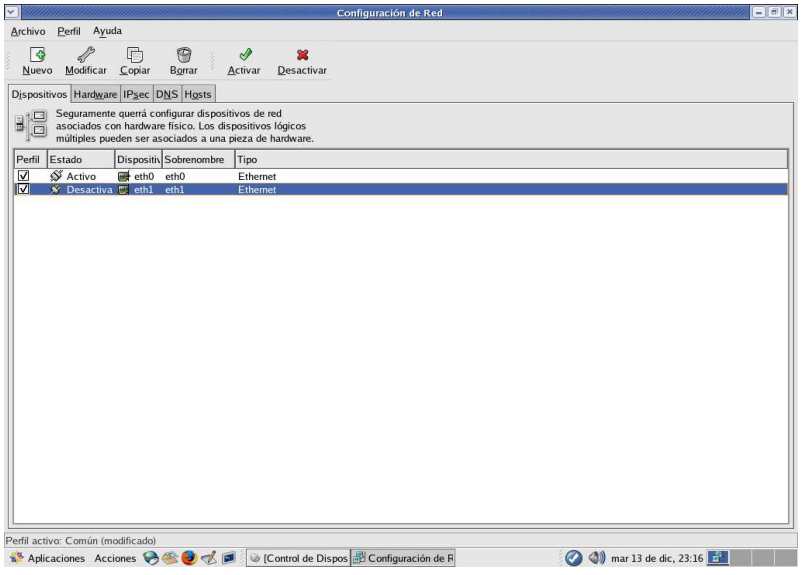
CREACION DE UN DISPOSITIVO ETHERNET

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Configuración Interfaz de Red.

Una vez configurada la interfaz de red, es necesario Activarla, para lo cual señalamos la interfaz de red específica y pulsamos el botón Activar, como muestra la siguiente pantalla:

GRÁFICO 2. 7

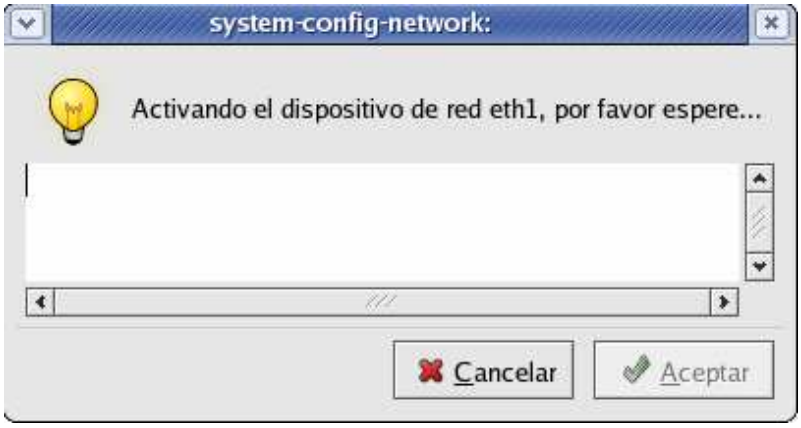
SELECCIÓN DE DISPOSITIVO ETHERNET



Fuente: SISTEMA OPERATIVO CENTOS 4.0. Configuración Interfaz de Red.

El sistema al activar el dispositivo, muestra la siguiente pantalla, la cual indica que ha finalizado la configuración y activación de la Interfaz de red.

GRÁFICO 2. 8
ACTIVANDO DISPOSITIVO DE RED



Fuente: SISTEMA OPERATIVO CENTOS 4.0. Configuración Interfaz de Red.

Aunque el Sistema Operativo Centos dentro de sus CD's de instalación tiene muchos drivers de tarjetas de red de fabricantes reconocidos con sus diferentes versiones, en ocasiones hay interfaz de red que no están dentro de estos y en este caso es necesario que obtenga el driver respectivo y se lo adhiera al kernel.

2.3.3 SERVIDOR DHCP MULTI-SCOPE

Como ya se dijo anteriormente el servidor DHCP es el encargado de asignar direcciones IP, en forma dinámica, a todos y cada uno de los host que forman parte de la LAN, siempre y cuando los clientes estén configurados para aceptar este tipo de servicio. Para este caso, se utilizará el sistema operativo CentOS, que es la versión freeware de Linux Advance Server, y tres tarjetas de red 10/100MB, las cuales servirán para crear 3 redes IP de diferente clase.

Se debe tomar en cuenta, aunque aquí no se detalle su instalación, que el computador que va a realizar la función de servidor ya debe estar instalado el sistema operativo CentOS.

Este servidor DHCP es el daemon dhcpd el mismo que se encuentra en el directorio /etc/rc.d/init.d., Para configurar el servidor se lo hará en el directorio /etc/dhcpd.conf, en este se configura los rangos de las direcciones IP que se entregaran a los clientes que pertenecen a esa subred con el siguiente comando:

range <dirección IP mínima> <dirección IP máxima>

2.3.3.1 Configuración del servidor DHCP Multi-Scope

Con el fin de guardar un orden de instalación de las interfaces de red, estos se los instalarán uno a uno comenzando desde el zócalo superior. Una vez instalado en el computador, se debe instalar el driver adecuado para que dicha tarjeta trabaje en Linux, por lo general Linux los reconoce automáticamente y no se requiere la instalación de driver alguno, seguidamente se le asignará una dirección IP con su respectiva máscara de red, para este caso se utilizarán direcciones clase C, a una de estas direcciones se particionan mediante subneting, ya que se la utilizará para la implementación de la VLAN móvil, esto es: 192.168.1.1, para esto se debe utilizar el siguiente comando:

ifconfig eth0 192.168.1.1 netmask 255.255.255.192

Para comprobar si se realizo la configuración, se utiliza el comando:

ifconfig

El resultado de esto será lo siguiente:

GRÁFICO 2. 9

RESULTADO DEL COMANDO IFCONFIG

```
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:05:5D:8B:CC:E7
          inet addr:192.168.1.1  Bcast:192.168.1.63 Mask:255.255.255.192
          inet6 addr: fe80::205:5dff:fe8b:cce7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2764 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1690 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:257095 (251.0 KiB)  TX bytes:140360 (137.0 KiB)
          Interrupt:11 Base address:0x6c00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2365 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2365 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3959768 (3.7 MiB)  TX bytes:3959768 (3.7 MiB)
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Ejecución de un comando en un Terminal.

Seguidamente se crea el archivo dhcpd.conf, el mismo que debe ser almacenado en el directorio /etc. Primeramente se tomara en cuenta que la interfaz eth0 es la VLAN móvil, para este caso, dentro de este constaran todos los hosts que van a ser declarados móviles a través de todas las interfaces de red (subredes) y que a su vez tendrán una única dirección IP por host acorde a la subred en la que se encuentre. El encargado de realizar esta función es el servidor dhcp.

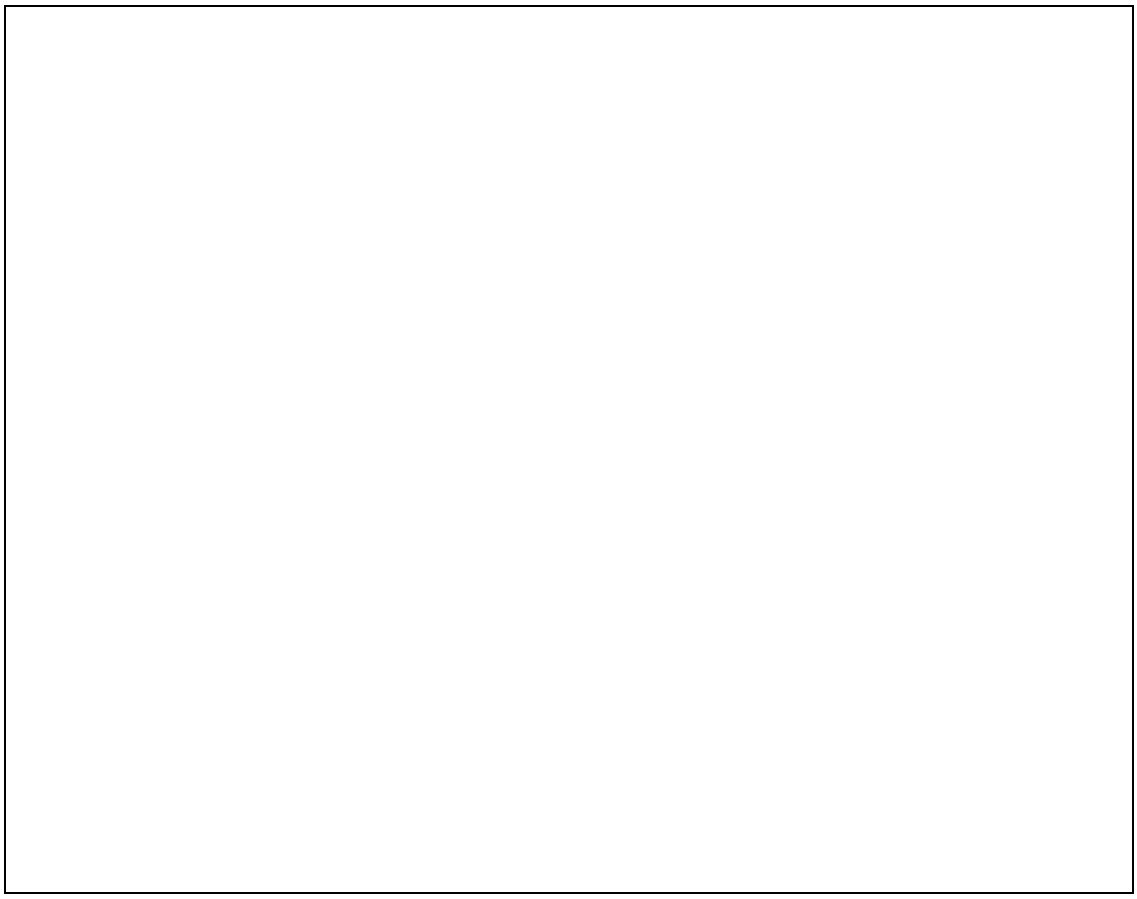
En esta parte del proyecto el servidor dhcp tendrá la capacidad de entregar direcciones IP hasta 61 hosts a través de la interfaz eth0, ya que como se indicó al principio se ha hecho subneting, pero en este caso se ha habilitado a 10 hosts.

El programa será el siguiente:

SCRIPT DE CONFIGURACIÓN 2. 1

ARCHIVO DHCPD.CONF

```
include "/etc/rndc.key";
authoritative;
ddns-update-style interim;
ddns-updates on;
update-static-leases on;
max-lease-time 3600;
#USUARIOS DE LA VLAN MOBIL, ESTOS PUEDEN TRASLADARSE A
#CUALQUIER RED FISICA PERO SIEMPRE SERAN PARTE DE LA MISMA #RED
LOGICA
# Eth0
        subnet 192.168.1.0 netmask 255.255.255.192 {
        ddns-domainname "ventas.tesis.com";
        ddns-rev-domainname "in-addr.arpa.";
        option domain-name "ventas.tesis.com";
        option domain-name-servers 192.168.1.1;
        option broadcast-address 192.168.1.63;
        option subnet-mask 255.255.255.192;
        option routers 192.168.1.1;
                host pc1 {
                hardware ethernet 00:07:95:BC:A5:9f;
                fixed-address 192.168.1.20;
                }
                host pc2 {
                hardware ethernet 00:08:02:69:96:45;
                fixed-address 192.168.1.11;
                }
                 host pc3 {
                        hardware ethernet 00:07:95:BC:A5:1f;
                        fixed-address 192.168.1.12;
                }
                 host pc4 {
                        hardware ethernet 00:02:a5:62:2f:10;
                        fixed-address 192.168.1.18;
                }
                host pc5{
                        hardware ethernet 00:07:95:BC:A5:2f;
                        fixed-address 192.168.1.19;
                }
                host pc6 {
                        hardware ethernet 00:02:a5:62:2f:20;
                        fixed-address 192.168.1.20;
                }
                host pc7 {
                        hardware ethernet 00:07:95:BC:A5:3f;
                        fixed-address 192.168.1.21;
```



```
        }
        host pc8 {
                hardware ethernet 00:02:a5:62:2f:30;
                fixed-address 192.168.1.22;
        }
        host pc9 {
                hardware ethernet 00:07:95:BC:A5:4f;
                fixed-address 192.168.1.23;
        }
        host pc10 {
                hardware ethernet 00:02:a5:62:2f:40;
                fixed-address 192.168.1.24;
        }
}

zone ventas.tesis.com. {
primary 127.0.0.1;
key "rndckey";
}

zone 1.168.192.in-addr.arpa. {
primary 127.0.0.1;
key "rndckey";
}
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Directorio /etc/dhcpd.conf

Como se observa al inicio del programa se debe insertar los parámetros siguientes:

```
include "/etc/rndc.key";
authoritative;
ddns-update-style interim;
ddns-updates on;
update-static-leases on;
max-lease-time 3600;
```

donde:

include indica al servidor dhcp que utilice el archivo rndc.key en el cual se encuentra la clave para la resolución.

authoritative.- Le da al servidor dhcp la autorización para que realice sus funciones.

ddns-update-style interim.- Método que utilizará el DNS para realizar sus actualizaciones.

ddns-updates on;.- Activa el servidor DNS dinámico.

update-static-leases on.- Activacion de los contratos dinámicos que el servidor dhcp realiza con sus clientes.

allow-client-updates.- El servidor dhcp le solicita al servidor DNS que permita a sus clientes, que utilizan el parámetro “fixed-address”, actualizar sus propias direcciones IP.

max-lease-time 3600.- Tiempo máximo de contrato que el dhcp mantiene con sus clientes, valor dado en segundos.

default-lease-time 3600.- Tiempo de contrato por default establecido por el servidor dhcp.

El programa dhcpd.conf consta de sentencias las cuales a su ves pueden contener otras sentencias.

Las sentencias se clasifican en parámetros y declaraciones. Los parámetros describen como hacer algo y que atributos se le asignan al cliente.

En las declaraciones se detalla la topología de una red, se describe un conjunto de clientes o sirve para aplicar determinados parámetros a un grupo de declaraciones. Estas tienen la siguiente estructura:

```
<nombre de la declaración> [atributos] {
        [parámetros]
        [declaraciones]
}
```

y los parámetros:

[option] <nombre del parámetro> [valores];

Los parámetros que comienzan con la palabra reservada *"option"* describen aquellos datos que brinda el servidor al cliente como parte del protocolo, y los que no, describen las características del servidor de DHCP. Entre las opciones que se ha utilizado están:

- domain-name: se refiere al nombre del dominio de la red
- domain-name-servers: Corresponde al nombre del servidor DNS
- broadcast-address: Es la dirección broadcast de la subred
- subnet-mask: Es la dirección de la mascara de la subred
- routers: Es la dirección IP del default gateway que el servidor entregará al cliente.

Las sentencias a utilizarse son:

- subnet: es donde se agrupan las características generales de los clientes que pertenecen a la misma subred. .

Sintaxis:

subnet <dirección de red> netmask <máscara de red> {
    [parámetros]
    [declaraciones]
}

- ddns-domainname: indica el dominio en el que se actualizan los DNS
- ddns-rev-domainname: nombre de dominio inverso.
- allow-client-updates: Permite el servidor dhcp que los clientes actualicen sus direcciones IP en los diferentes archivos que maneja el DNS dinámico.
- host: permite describir aquellos hosts que tengan una dirección fija. Todos los clientes que usan BOOTP deben tener asociada una sentencia *host*. Un

cliente se corresponde con una declaración *host*. De no ser así entonces se emplearía la dirección MAC del cliente especificada a través de el atributo *hardware.* .

Sintaxis:

```
host <hostname> {
  [parámetros]
  [declaraciones]
}
```

Los parámetros a utilizarse son:

- hardware <type> <address>;

  Indica la dirección física (MAC) de un cliente particular (declaraciones tipo host).

Donde:
type expresa el tipo de arquitectura de la interfaz de red, actualmente puede ser: *ethernet* o *token-ring*.
address expresa la dirección MAC en el que se utiliza seis números hexadecimales (números desde 00 hasta ff) separados por el carácter ":".

- fixed-address <address> [, <address>];

Expresa las direcciones IP que son fijas para los clientes descritos a través de las declaraciones de tipo host. Pueden utilizarse nombres de dominio en lugar de números IP.

Como parte final de esta parte del programa dhcp, se ingresaran los nombres de las zonas de red que el servidor DNS dinámico debe resolver tanto en forma directa como en forma indirecta, así como también la llave y la dirección donde se encuentra ubicado el servidor DNS.

Para este caso de proyecto la subnet es: 192.168.1.0; el nombre de dominio es: “ventas.tesis.com”; ddns-domainname corresponde al nombre del dominio de la subred a resolverse en forma directa: “ventas.tesis.com”; ddns-rev-domainname a su ves es el nombre del dominio de la subred a resolverse de manera inversa: “in-addr.arpa”; option routers es: 192.168.1.1; el valor de *host* se debe tener muy en cuenta ya que si se mantiene el mismo nombre para todos los hosts, al ejecutar el dhcp, este generará errores, es por eso que en este caso se ha dado varios valores; el valor hardware es la dirección MAC de todos los clientes que forman la subred y fixed-address es dirección IP fija que se entregara a cada host.

Al final de este código se debe agregar las zonas reversas del dominio, con el fin de que el servidor DHCP actualice, dinámicamente y automáticamente, los archivos de zonas del servidor DNS. Estas zonas a agregar son:

```
zone ventas.tesis.com. {
        primary 127.0.0.1;
        key "rndckey";
        }
        zone 1.168.192.in-addr.arpa. {
        primary 127.0.0.1;
        key "rndckey";
        }
```

En la PC cliente se debe realizar la misma operación con respecto a la instalación de la tarjeta, pero cuando llegue el momento de asignarle una dirección IP, se debe habilitar la opción: *asignación IP en forma dinámica DHCP.*

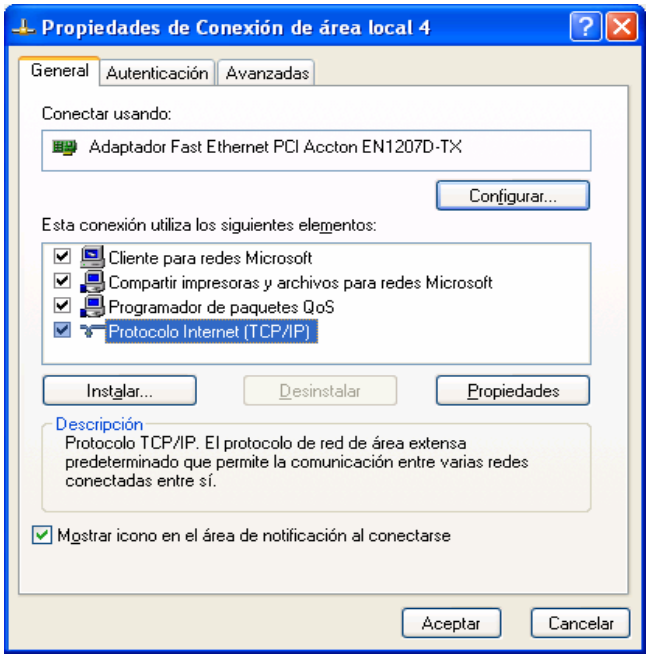
Si el sistema operativo del cliente es Windows, se debe deshabilitar y liberar las conexiones de red que éste tenga asignado, para esto se da el siguiente comando:

ipconfig /release

De igual manera se configura la tarjeta de red con dhcp escogiendo la opción: *Obtener una dirección IP automáticamente*, como se muestra en las figuras siguientes:

GRÁFICO 2. 10

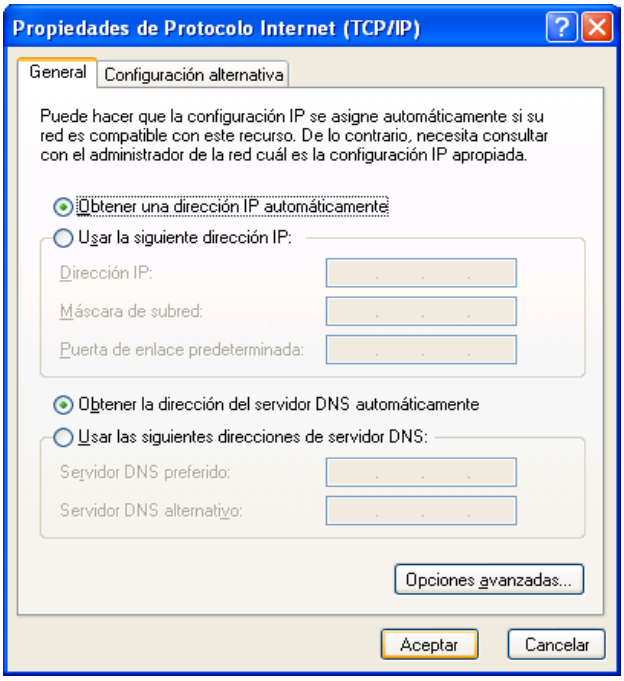
CONFIGURACION DEL CLIENTE DHCP



Fuente: SISTEMA OPERATIVO WINDOWS. Configuración de Conexión de área local.

GRÁFICO 2. 11

OBTENCIÓN DE UNA DIRECCIÓN IP AUTOMÁTICA EN EL CLIENTE



Fuente: SISTEMA OPERATIVO WINDOWS. Configuración de Conexión de área local.

Por el contrario si el cliente dhcp esta en un sistema Linux, se configura la interfaz eth0 el mismo que se encuentra en el directorio /etc/sysconfig/network-scripts/ el cual tiene un fichero etiquetado de la forma *ifcfg-x* donde *x* es el nombre de la interfaz, por ejemplo para la *loopback* es *ifcfg-lo*, para la primera interfaz de tipo Ethernet es *ifcfg-eth0* y el contenido de este es semejante a:

```
DEVICE=eth0                 # dispositivo de red asociado
ONBOOT=yes                  # se activa la interfaz durante el inicio
BOOTPROTO=dinamic           # la configuración es dinámica
IPADDR=192.168.1.1          # la dirección IP asociada a la interfaz
NETMASK=255.255.255.192     # la máscara de red
GATEWAY=192.168.1.1          # la dirección del gateway
```

Por último se reinicia la interfaz. Una vez terminado los pasos anteriores, mediante un cable de red (point-to-point) y un switch, se conectaran las computadoras, con el fin de comprobar si el servidor DHCP asigna o no direcciones IP a los clientes que formen parte de la red, para esto se habilita el demonio o servicio dhcpd con el comando:

```
service dhcpd start
starting dhcpd:                          [  OK  ]
```

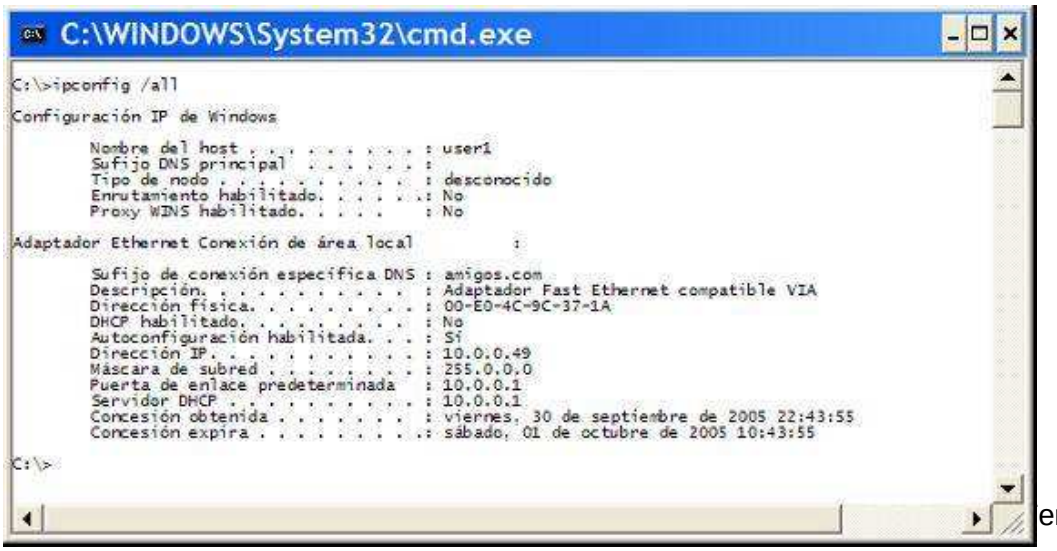
Si nuestro cliente tiene algún sistema operativo de Windows, mediante una ventana de comando se dará la siguiente instrucción:

```
ipconfig /all
```

Dando un resultado parecido al siguiente:

GRÁFICO 2. 12

RESULTADO DE LA EJECUCIÓN DEL COMANDO IPCONFIG



erminal.

Si por el contrario se tiene un sistema operativo en Linux se dará el siguiente comando:

ifconfig

Notar que la dirección IP asignada, para ambos casos, debe estar acorde con la dirección MAC que se ha impuesto en el programa servidor dhcp.

A continuación, en el servidor dhcp se instala la siguiente tarjeta de red utilizando el siguiente zócalo y se utilizan los mismos procedimientos antes mencionados, adicionalmente se asigna a esta tarjeta de red un alias, con el fin de que esta maneje y escuche dos redes diferentes, es decir, que dicha interfaz de red estará conformada por eth1:0 y eth1:1.

La eth1:0 es la que administrará la VLAN móvil cuya red es 192.168.1.64 pero su dirección IP es: 192.168.1.65 y su netmask es 255.255.255.192 (se hizo subneting), para asignar estos valores a dicha interfaz se dará el siguiente comando:

ifconfig eth1:0 192.168.1.65 netmask 255.255.255.192 up

Mientras que la eth1:1 es la que se encargará de administrar la red 192.168.2.0 cuya dirección IP para esta interfaz es: 192.168.2.1 y su máscara de red es: 255.255.255.0, al igual que en el caso anterior se utiliza el mismo comando pero con sus valores correspondientes:

ifconfig eth1:0 192.168.2.1 netmask 255.255.255.0 up

Seguidamente al dar el comando ifconfig, nos debe dar la siguiente respuesta:

GRÁFICO 2. 13

RESULTADO DE LA EJECUCIÓN DEL COMANDO IFCONFIG

```
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:05:5D:8B:CC:E7
          inet addr:192.168.1.1  Bcast:192.168.1.63
          Mask:255.255.255.192
          inet6 addr: fe80::205:5dff:fe8b:cce7/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:546 (546.0 b)
          Interrupt:11 Base address:0x6c00

eth1      Link encap:Ethernet  HWaddr 00:08:A1:62:F9:4D
          inet addr:192.168.1.65  Bcast:192.168.1.127
          Mask:255.255.255.192
          inet6 addr: fe80::208:a1ff:fe62:f94d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0
          carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:9 Base address:0xd000

eth1:1    Link encap:Ethernet  HWaddr 00:08:A1:62:F9:4D
          inet addr:192.168.2.1  Bcast:192.168.2.255
          Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:9 Base address:0xd000
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Ejecución de un comando en un Terminal.

Notar que la red eth1:1 no se hizo subneting por ende, esta red tiene la capacidad de manejar hasta 253 direcciones IP.

Seguidamente al archivo dhcpd.conf, se le agregara los datos de los hosts que pertenecen a la red VLAN móvil de la interfaz eth1:0, así como los datos de la otra red, en la cual a los clientes se les asignará una dirección IP dentro de un rango que el administrador de la red lo determine, para nuestro caso se la hizo de la 30 a la 254, mediante la sentencia *range*.

- range: mediante esta sentencia se definen los rangos de direcciones IP tanto máxima como mínima que serán entregados a los clientes dhcp que pertenecen a una misma subred. Toda declaración tipo *subnet* debe pertenecer a una declaración *range*. .

Sintaxis:
range [dynamic-bootp] <dirección IP mínima> [dirección IP maxima]

Para la VLAN móvil debe tener el mismo nombre de dominio “ventas.tesis.com”, mientras que la red 192.168.2.0 se le ha asignado el nombre de dominio: “contabilidad.tesis.com”.

Al igual que en el caso anterior se debe colocar al final de cada subred, las zonas que el DNS debe actualizarse para poder así resolver.

Notar una vez más que esta tarjeta de red maneja o gestiona dos redes diferentes, de modo que se esta compartiendo la tarjeta entre dos redes, por lo que se debe indicar esta aclaración al servidor dhcp, insertando al inicio de esta nueva configuración la siguiente sentencia:

shared-network red_1

el archivo se presentará de la siguiente manera:

SCRIPT DE CONFIGURACIÓN 2. 2

ARCHIVO DHCPD.CONF

```
shared-network red_1 {

# Eth1
     subnet 192.168.1.64 netmask 255.255.255.192 {
      ddns-domainname "ventas.tesis.com";
      ddns-rev-domainname "in-addr.arpa.";
      option domain-name "ventas.tesis.com";
      option domain-name-servers 192.168.1.65;
      option broadcast-address 192.168.1.127;
      option subnet-mask 255.255.255.192;
      option routers 192.168.1.65;

            host pc_1_1 {
                  hardware ethernet 00:07:95:BC:A5:9f;
                  fixed-address 192.168.1.70;
            }

            host pc_1_2 {
                  hardware ethernet 00:08:02:69:96:45;
                  fixed-address 192.168.1.71;
            }

            host pc_1_3 {
                  hardware ethernet 00:07:95:BC:A5:1f;
                  fixed-address 192.168.1.72;
            }

            host pc_1_4 {
                  hardware ethernet 00:02:a5:62:2f:10;
                  fixed-address 192.168.1.18;
            }
            host pc_1_5 {
                  hardware ethernet 00:07:95:BC:A5:2f;
                  fixed-address 192.168.1.19;
            }
            host pc_1_6 {
                  hardware ethernet 00:02:a5:62:2f:20;
                  fixed-address 192.168.1.20;
            }
```

```
          host pc_1_7 {
                hardware ethernet 00:07:95:BC:A5:3f;
                fixed-address 192.168.1.21;
           }
           host pc_1_8 {
                hardware ethernet 00:02:a5:62:2f:30;
                fixed-address 192.168.1.22;
           }
           host pc_1_9 {
                hardware ethernet 00:07:95:BC:A5:4f;
                fixed-address 192.168.1.23;
           }
           host pc_1_10 {
                hardware ethernet 00:02:a5:62:2f:40;
                fixed-address 192.168.1.24;
           }
     }
     zone ventas.tesis.com. {
     primary 127.0.0.1;
     key "rndckey";
     }
     zone 1.168.192.in-addr.arpa. {
     primary 127.0.0.1;
     key "rndckey";
     }

# Eth1:1

     subnet 192.168.2.0 netmask 255.255.255.0 {
     ddns-domainname "contabilidad.tesis.com";
     ddns-rev-domainname "in-addr.arpa.";
     option domain-name "contabilidad.tesis.com";
     option domain-name-servers 192.168.2.1;
     option broadcast-address 192.168.2.255;
     option subnet-mask 255.255.255.0;
     option routers 192.168.2.1;
     range 192.168.2.30 192.168.2.254;
        }

     zone contabilidad.tesis.com. {
     primary 127.0.0.1;
     key "rndckey";
       }
zone 2.168.192.in-addr.arpa. {
     primary 127.0.0.1;
     key "rndckey";
     }
}
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Directorio /etc/dhcpd.conf

Nuevamente se configura a los clientes de nuestras redes para que reciban direcciones de red en forma automática y se verifica mediante una prueba, claro que para esto se debe poner en ejecución al servidor dhcp mediante el comando:

```
service dhcpd start
starting dhcpd:                    [  OK  ]
```

Si todo esta bien debe funcionar correctamente, asignando direcciones IP según lo acordado en el archivo dhcpd.conf.

Por último se inserta la siguiente tarjeta de red en el equipo servidor y se realizan los mismos procedimientos que en la tarjeta 2, teniendo en cuenta los datos siguientes:

- VLAN móvil 192.168.1.128 eth2:0 IP: 192.168.1.129 netmask:255.255.255.192.
- Red 192.168.3.0 eth2:1 IP:192.168.3.1 netmask: 255.255.255.0.

El resultado será:

GRÁFICO 2. 14
RESULTADO DE COMANDO IFCONFIG

```
root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:05:5D:8B:CC:E7
          inet addr:192.168.1.1  Bcast:192.168.1.63
          Mask:255.255.255.192
          inet6 addr: fe80::205:5dff:fe8b:cce7/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0
          carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:546 (546.0 b)
          Interrupt:11 Base address:0x6c00

eth1      Link encap:Ethernet  HWaddr 00:08:A1:62:F9:4D
          inet addr:192.168.1.65  Bcast:192.168.1.127
          Mask:255.255.255.192
          inet6 addr: fe80::208:a1ff:fe62:f94d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

```
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
           TX packets:8 errors:0 dropped:0 overruns:0
           carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:9 Base address:0xd000

eth1:1    Link encap:Ethernet  HWaddr 00:08:A1:62:F9:4D
           inet addr:192.168.2.1  Bcast:192.168.2.255
           Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
           TX packets:0 errors:0 dropped:0 overruns:0
           carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:9 Base address:0xd000

eth2      Link encap:Ethernet  HWaddr 00:10:B5:67:50:AE
           inet addr:192.168.1.129  Bcast:192.168.1.191
           Mask:255.255.255.192
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
           TX packets:0 errors:0 dropped:0 overruns:0
           carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:5 Base address:0xde00

eth2:1    Link encap:Ethernet  HWaddr 00:10:B5:67:50:AE
           inet addr:192.168.3.1  Bcast:192.168.3.255
           Mask:255.255.255.0
          inet6 addr: fe80::210:b5ff:fe67:50ae/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
           TX packets:9 errors:0 dropped:0 overruns:0
           carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:618 (618.0 b)
          Interrupt:5 Base address:0xde00

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
           RX packets:1948 errors:0 dropped:0 overruns:0
           frame:0
           TX packets:1948 errors:0 dropped:0 overruns:0
           carrier:0
          collisions:0 txqueuelen:0
RX bytes:3794364 (3.6 MiB)  TX bytes:3794364 (3.6 MiB)
```

Fuente: SISTEMA OPERATIVO WINDOWS. Ejecución de un comando en un Terminal.

Al archivo dhcpd.conf de la misma manera se tendrá que insertar los datos de los hosts que va a administrar por medio de las interfaces de red, teniendo en cuenta que la interfaz eth2:0 es la VLAN móvil cuyo nombre de dominio es “ventas.tesis.com” y ésta entregará direcciones fijas de acuerdo a la dirección MAC de cada cliente, mientras que la eth2:1 es la red 192.168.3.0 su nombre de dominio es: “rrhh.tesis.com” y entregará direcciones IP en forma automática dentro del rango IP que el administrador disponga, esta subnet tampoco se la hizo subneting.

El archivo dhcpd.conf final será:

SCRIPT DE CONFIGURACIÓN 2. 3
ARCHIVO DHCPD.CONF

```
include "/etc/rndc.key";
authoritative;
ddns-update-style interim;
ddns-updates on;
update-static-leases on;
max-lease-time 3600;

#USUARIOS DE LA VLAN MÓVIL, ESTOS PUEDEN TRASLADARSE A
CUALQUIER RED FISICA PERO SIEMPRE SERAN PARTE DE LA MISMA RED
LÓGICA

# Eth0
      subnet 192.168.1.0 netmask 255.255.255.192 {
       ddns-domainname "ventas.tesis.com";
      ddns-rev-domainname "in-addr.arpa.";
      option domain-name "ventas.tesis.com";
      option domain-name-servers 192.168.1.1;
      option broadcast-address 192.168.1.63;
      option subnet-mask 255.255.255.192;
      option routers 192.168.1.1;

            host pc1 {
            hardware ethernet 00:07:95:BC:A5:9f;
                  fixed-address 192.168.1.20;
            }

            host pc2 {
            hardware ethernet 00:08:02:69:96:45;
            fixed-address 192.168.1.11;
            }
```

```
            host pc_0_3 {
            hardware ethernet 00:07:95:BC:A5:1f;
            fixed-address 192.168.1.12;
            }
            host pc4 {
                  hardware ethernet 00:02:a5:62:2f:10;
                  fixed-address 192.168.1.18;
            }
            host pc5 {
                  hardware ethernet 00:07:95:BC:A5:2f;
                  fixed-address 192.168.1.19;
            }
            host pc6 {
                  hardware ethernet 00:02:a5:62:2f:20;
                  fixed-address 192.168.1.20;
            }
            host pc7 {
                  hardware ethernet 00:07:95:BC:A5:3f;
                  fixed-address 192.168.1.21;
            }
            host pc8 {
                  hardware ethernet 00:02:a5:62:2f:30;
                  fixed-address 192.168.1.22;
            }
            host pc9 {
                  hardware ethernet 00:07:95:BC:A5:4f;
                  fixed-address 192.168.1.23;
            }
            host pc10 {
                  hardware ethernet 00:02:a5:62:2f:40;
                  fixed-address 192.168.1.24;
            }
      }

      zone ventas.tesis.com. {
      primary 127.0.0.1;
      key "rndckey";
      }

      zone 1.168.192.in-addr.arpa. {
      primary 127.0.0.1;
      key "rndckey";
      }



shared-network red_1 {

# Eth1
       subnet 192.168.1.64 netmask 255.255.255.192 {
      ddns-domainname "ventas.tesis.com";
      ddns-rev-domainname "in-addr.arpa.";
      option domain-name "ventas.tesis.com";
      option domain-name-servers 192.168.1.65;
```

```
      option broadcast-address 192.168.1.127;
      option subnet-mask 255.255.255.192;
      option routers 192.168.1.65;

            host pc11 {
                  hardware ethernet 00:07:95:BC:A5:9f;
                        fixed-address 192.168.1.70;
            }

            host pc12 {
                  hardware ethernet 00:08:02:69:96:45;
                  fixed-address 192.168.1.71;
            }

            host pc13 {
                  hardware ethernet 00:07:95:BC:A5:1f;
                  fixed-address 192.168.1.72;
            }

            host pc14 {
                  hardware ethernet 00:02:a5:62:2f:10;
                  fixed-address 192.168.1.18;
            }
            host pc15 {
                  hardware ethernet 00:07:95:BC:A5:2f;
                  fixed-address 192.168.1.19;
            }
            host pc16 {
                  hardware ethernet 00:02:a5:62:2f:20;
                  fixed-address 192.168.1.20;
            }
            host pc17 {
                  hardware ethernet 00:07:95:BC:A5:3f;
                  fixed-address 192.168.1.21;
            }
            host pc18 {
                  hardware ethernet 00:02:a5:62:2f:30;
                  fixed-address 192.168.1.22;
            }
            host pc19 {
                  hardware ethernet 00:07:95:BC:A5:4f;
                  fixed-address 192.168.1.23;
            }
            host pc20 {
                  hardware ethernet 00:02:a5:62:2f:40;
                  fixed-address 192.168.1.24;
            }

      }

      zone ventas.tesis.com. {
      primary 127.0.0.1;
      key "rndckey";
      }
```

```
      zone 1.168.192.in-addr.arpa. {
      primary 127.0.0.1;
      key "rndckey";
      }


# Eth1:1

      subnet 192.168.2.0 netmask 255.255.255.0 {
      ddns-domainname "contabilidad.tesis.com";
      ddns-rev-domainname "in-addr.arpa.";
      option domain-name "contabilidad.tesis.com";
      option domain-name-servers 192.168.2.1;
      option broadcast-address 192.168.2.255;
      option subnet-mask 255.255.255.0;
      option routers 192.168.2.1;
      range 192.168.2.30 192.168.2.254;
         }

      zone contabilidad.tesis.com. {
      primary 127.0.0.1;
      key "rndckey";
        }

      zone 2.168.192.in-addr.arpa. {
      primary 127.0.0.1;
      key "rndckey";
      }
}


shared-network red_2 {

# Eth2

      subnet 192.168.1.128 netmask 255.255.255.192 {
      ddns-domainname "ventas.tesis.com";
      ddns-rev-domainname "in-addr.arpa.";
      option domain-name "ventas.tesis.com";
      option domain-name-servers 192.168.1.129;
      option broadcast-address 192.168.1.191;
      option subnet-mask 255.255.255.192;
      option routers 192.168.1.129;

            host pc21 {
            hardware ethernet 00:07:95:BC:A5:9f;
                  fixed-address 192.168.1.133;
            }

            host pc22 {
                  hardware ethernet 00:08:02:69:96:45;
                  fixed-address 192.168.1.134;
            }
```

```
            host pc23 {
                  hardware ethernet 00:07:95:BC:A5:1f;
                  fixed-address 192.168.1.135;
            }

            host pc24 {
                  hardware ethernet 00:02:a5:62:2f:10;
                  fixed-address 192.168.1.18;
            }
            host pc25 {
                  hardware ethernet 00:07:95:BC:A5:2f;
                  fixed-address 192.168.1.19;
            }
            host pc26 {
                  hardware ethernet 00:02:a5:62:2f:20;
                  fixed-address 192.168.1.20;
            }
            host pc27 {
                  hardware ethernet 00:07:95:BC:A5:3f;
                  fixed-address 192.168.1.21;
            }
            host pc28 {
                  hardware ethernet 00:02:a5:62:2f:30;
                  fixed-address 192.168.1.22;
            }
            host pc29 {
                  hardware ethernet 00:07:95:BC:A5:4f;
                  fixed-address 192.168.1.23;
            }
            host pc30 {
                  hardware ethernet 00:02:a5:62:2f:40;
                  fixed-address 192.168.1.24;
            }

      }

      zone ventas.tesis.com. {
      primary 127.0.0.1;
      key "rndckey";
      }

      zone 1.168.192.in-addr.arpa. {
      primary 127.0.0.1;
      key "rndckey";
      }


# Eth2:1

      subnet 192.168.3.0 netmask 255.255.255.0 {
      ddns-domainname "rrhh.tesis.com";
      ddns-rev-domainname "in-addr.arpa.";
      option domain-name "rrhh.tesis.com";
      option domain-name-servers 192.168.3.1;
```

```
      option broadcast-address 192.168.3.255;
      option subnet-mask 255.255.255.0;
      option routers 192.168.3.1;
       range 192.168.3.30 192.168.3.254;
      }

     zone rrhh.tesis.com. {
      primary 127.0.0.1;
      key "rndckey";
        }

      zone 3.168.192.in-addr.arpa. {
      primary 127.0.0.1;
      key "rndckey";
      }
}
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Directorio /etc/dhcpd.conf

Por último se realiza una prueba, en el cual cada interfaz de red debe entregar direcciones IP a sus clientes de acuerdo a la red en la que se encuentren.

2.3.4 DNS (DOMAIN NAME SYSTEM)

2.3.4.1 Sistema de resolución de nombres

El Sistema de resolución de nombres, es un servicio que permite referir a una dirección IP utilizando nombres significativos y semánticos, por ejemplo www.epn.edu.ec

Este mecanismo realiza una conversión entre un nombre de una máquina por ejemplo localhost.tesis.com y el número IP de la máquina 192.168.1.1,

Existen dos formas que permiten traducir nombres a direcciones:

a) Utilizando una tabla llamada *host tabla*
b) Utilizando un sistema de base de datos distribuida llamada Domain Name Service (Servicio de Nombre de Dominio)

Archivo host.- La tabla host, es un archivo de texto que almacena direcciones IP y las asocia con nombres. En Linux este archivo se encuentra en el siguiente directorio /etc/hosts. Esta técnica es estática y es recomendada cuando existen pocas máquinas ya que carece de escalabilidad y de un proceso automático de actualización.

DNS (Sistema de dominio de nombres).- es una base de datos distribuida, la misma que forma un sistema jerárquico para traducir de nombres a direcciones IP.

La información es distribuida por todo el mundo en cientos de servidores de nombres y este sistema utiliza el mecanismo cliente – servidor de DNS. Los servidores de nombres contienen la información de un segmento de la base de datos y la ponen a disposición de los clientes.

Un servidor DNS está en la capacidad de recibir y resolver peticiones relacionadas con el sistema de nombres, permite traducir su nombre de dominio a una dirección IP, asignar nombres a las máquinas de una red y trabajar con nombres de dominio en lugar de direcciones IP. Su funcionamiento e implementación está descrito en las RFC's 1034[1] y 1035[2].

2.3.4.2 Funcionamiento

En el momento que un programa cliente intenta acceder a los recursos de Internet, o cualquier recurso de Red que sean invocados por nombres, el servidor DNS procesa la consulta, intentando buscar el dominio en su tabla de registros, si la operación es fallida envía la petición a otro servidor DNS situado a un nivel superior de la jerarquía de nombres de dominio, este proceso se repite hasta que se obtiene como resultado la dirección IP correspondiente al dominio buscado.

2.3.4.3 Implementación.

Para la aplicación de este proyecto, se configura un Servidor Local de Nombre de Dominio Secundario, el cual es la fuente autorizada de toda la información acerca

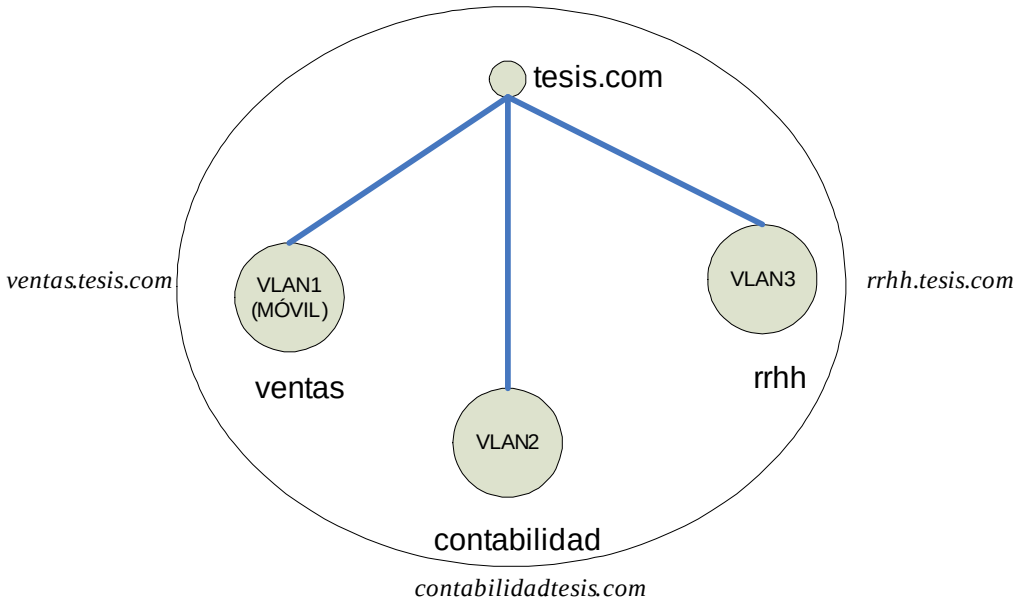
de un dominio específico, en este caso son tres dominios que se crean para satisfacer a cada VLAN.

RED	**DOMINIO**
VLAN 1 ->	ventas.tesis.com (vlan móvil)
VLAN 2 ->	contabilidad.tesis.com
VLAN 3 ->	rrhh.tesis.com

2.3.4.4 Diagrama de Jerarquía

El diagrama de jerarquía es representado como un árbol invertido, en donde el punto donde parten es denominado dominio raíz en este caso es “tesis.com”, a partir de éste nacen tres subdominios que se asocian a cada vlan, por ejemplo representan a tres departamentos o secciones diferentes: “ventas”, ”contabilidad”, ”rrhh”.

GRÁFICO 2. 15
DIAGRAMA DE JERARQUIA DNS



Ejemplo de jerarquías DNS

2.3.4.5 Instalación del software

En Linux el Servicio de nombres es un programa llamado *named*, el cual forma parte del paquete bind[48], el mismo que viene preparado para su instalación en las distribuciones Linux actuales (kernel 2.4 en adelante), o a su vez se instala a través de RPM o como otra opción que es compilando e instalando directamente desde el código fuente.

En Centos 4.0 con interfaz gráfica, el primer paso es agregar un componente del sistema operativo, Se inicia en el menú principal del escritorio y se continúa con el siguiente submenú:

→ Aplicaciones
→ Herramientas Administrativas
→ Añadir o quitar componentes
→ Servicios de Red
→ Bind 9.0

Seguir los pasos del asistente de Instalación, una vez culminado este proceso el paquete se instala en el siguiente directorio /usr/sbin/named.

2.3.4.6 Configuración del DNS

Se inicia la configuración del DNS con los archivos básicos de configuración.

2.3.4.7 Archivos básicos de configuración

Existe un fichero de configuración para el servicio *named,* el cual se denomina named.conf y se encuentra ubicado en el directorio /etc. Al momento de la instalación este archivo se crea automáticamente y ya viene configurado para que la máquina localhost resuelva su dirección IP.

El archivo /etc/named.conf es el siguiente:

[48] Paquete DNS coordinado por Paul Vixie para The Internet Software Consortium http://www.isc.com

SCRIPT DE CONFIGURACIÓN 2. 4

ARCHIVO NAMED.CONF

```
// Este es un ejemplo de fichero de configuración de name para
bind 9
// named.conf for Red Hat caching-nameserver
//

options {
// Aquí se define el nombre del directorio de trabajo

     directory "/var/named";

// La opción allow- query contiene una lista de redes o
direcciones IP para aceptar las peticiones
     allow-query
{192.168.1.0/24;192.168.2.0/24;192.168.3.0/24;127.0.0.1;};

dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
     //draft-ietf-dhc-fqdn-option-fully-qualified.txt;
     //allow-client-updates;

// Por defecto el DNS funciona en el Puerto 53, este número de
puerto se puede cambiar
      // query-source address * port 53;
};

//
// a caching only nameserver config
//

controls {
     inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};


//Las siguientes definiciones no necesitan ninguna
modificación.
// La siguiente es la definición zona de los servidores raíz.


zone "." IN {
     type hint;
               // En la siguiente línea invoca al archivo
named.ca, el cual  es buscado en el directorio de trabajo.
     file "named.ca";
};

//Define la zona ‘localhost’
zone "localhost" IN {
     type master;
     file "localhost.zone";
```

```
      allow-update { none; };
};

// Define la zona inversa para ‘localhost’
zone "0.0.127.in-addr.arpa" IN {
      type master;
      file "named.local";
      allow-update { none; };
};

zone
"0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
ip6.arpa" IN {
         type master;
      file "named.ip6.local";
      allow-update { none; };
};

zone "255.in-addr.arpa" IN {
      type master;
      file "named.broadcast";
      allow-update { none; };
};

zone "0.in-addr.arpa" IN {
      type master;
      file "named.zero";
      allow-update { none; };
};

//En las siguientes líneas se introduce las definiciones de
zona para los propios dominios de este proyecto


// Define la zona de la VLAN1 (móvil) ventas.tesis.com

zone "ventas.tesis.com" IN {
      type master;
      allow-update { 127.0.0.1;key "rndckey"; };
      file "ventas.tesis.com";
};

// Define la zona inversa de la VLAN1
zone "1.168.192.in-addr.arpa" IN {
      type master;
      allow-update { 127.0.0.1;key "rndckey"; };
      file "192.168.1.reverso";
};

// Define la zona de la VLAN 2 contabilidad.tesis.com

zone "contabilidad.tesis.com" {
      type master;
      allow-update { 127.0.0.1;key "rndckey"; };
```

```
      file "contabilidad.tesis.com";
};

// Define la zona inversa de la VLAN 2

zone "2.168.192.in-addr.arpa" {
      type master;
      allow-update { 127.0.0.1;key "rndckey"; };
      file "192.168.2.reverso";
};

// Define la zona de la Vlan 3 rrhh.tesis.com
zone "rrhh.tesis.com" IN {
      type master;
      allow-update { 127.0.0.1;key "rndckey"; };
      file "rrhh.tesis.com";
};

// Define la zona inverse de la Vlan 3
zone "3.168.192.in-addr.arpa" IN {
      type master;
      allow-update { 127.0.0.1;key "rndckey"; };
      file "192.168.3.reverso";
};
include "/etc/rndc.key";
```

Directorio /etc/named.conf

Adicionalmente y de la misma manera automática se crea un directorio de trabajo con los archivos necesarios para que el servicio named funcione adecuadamente. Este directorio está ubicado en el path /var/named/

En el directorio /var/named, se encuentran los archivos de las zonas a las cuales hace referencia el archivo named.conf, se listan a continuación:

Los siguientes archivos se crean automáticamente y no hay que realizar ninguna modificación:

- localdomain.zone
- localhost.zone
- named.broadcast
- named.ca
- named.local
- named.zero

- localhost.zone.rpmsave
- localdomain.zone.rpmsave
- named.local.rpmsave

Los siguientes archivos se crean manualmente y son almacenados en el mismo directorio /var/named.

- 192.168.1.reverso
- 192.168.2.reverso
- 192.168.3.reverso
- ventas.tesis.com
- contabilidad.tesis.com
- rrhh.tesis.com

SCRIPT DE CONFIGURACIÓN 2. 5
ARCHIVO LOCALDOMAIN.ZONE

localdomain.zone

```
$TTL  86400
@           IN SOA      localhost root (
                              42          ; serial (d. adams)
                              3H          ; refresh
                              15M         ; retry
                              1W          ; expiry
                              1D )        ; minimum
              IN NS           localhost
localhost   IN A        127.0.0.1
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0.
Directorio /var/etc/named/chroot/var/named/localdomain.zone

SCRIPT DE CONFIGURACIÓN 2. 6

ARCHIVO LOCALHOST.ZONE

localhost.zone

```
$TTL  86400
@           IN SOA      @       root (
                                42          ; serial (d. adams)
                                3H          ; refresh
                                15M         ; retry
                                1W          ; expiry
                                1D )        ; minimum

              IN NS             @
            IN A        127.0.0.1
            IN AAAA           ::1
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0.
Directorio /var/etc/named/chroot/var/named/localhost.zone

SCRIPT DE CONFIGURACIÓN 2. 7

ARCHIVO NAMED.BROADCAST

Named.broadcast

```
$TTL    86400
@               IN SOA  localhost       root (
                                        42              ; serial (d.
adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
      IN    NS    localhost
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0.
Directorio /var/etc/named/chroot/var/named/named.broadcast

SCRIPT DE CONFIGURACIÓN 2. 8

ARCHIVO NAMED.CA

named.ca

; Este archivo contiene la información de los servidores raíz.

```
;       This file holds the information on root name servers needed
to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:    Jan 29, 2004
;       related version of root zone:   2004012900
;
;
; formerly NS.INTERNIC.NET
;
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     192.228.79.201
;
; formerly C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
;
; formerly TERP.UMD.EDU
;
.                        3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     128.8.10.90
;
; formerly NS.NASA.GOV
;
.                        3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
;
; formerly NS.ISC.ORG
;
.                        3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.      3600000      A     192.5.5.241
;
; formerly NS.NIC.DDN.MIL
;
.                        3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.      3600000      A     192.112.36.4
```

```
;
; formerly AOS.ARL.ARMY.MIL
;
.                        3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.      3600000      A     128.63.2.53
;
; formerly NIC.NORDU.NET
;
.                        3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000      A     192.36.148.17
;
; operated by VeriSign, Inc.
;
.                        3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.      3600000      A     192.58.128.30
;
; operated by RIPE NCC
;
.                        3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.      3600000      A     193.0.14.129
;
; operated by ICANN
;
.                        3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.      3600000      A     198.32.64.12
;
; operated by WIDE
;
.                        3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.      3600000      A     202.12.27.33
; End of File
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0.
Directorio /var/etc/named/chroot/var/named/named.ca

SCRIPT DE CONFIGURACIÓN 2. 9

ARCHIVO NAMED.LOCAL

```
named.local

$TTL                    86400
@                       IN          SOA     localhost. root.localhost.  (
                                            1997022700 ; Serial
                                             28800      ; Refresh
                                            14400      ; Retry
                                            3600000    ; Expire
                                            86400 )    ; Minimum
                        IN          NS      localhost.
1                       IN          PTR     localhost.
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0.
Directorio /var/etc/named/chroot/var/named/named.local

SCRIPT DE CONFIGURACIÓN 2. 10

ARCHIVO NAMED.CERO

```
named.cero
$TTL    86400
@           IN SOA  localhost       root (
                                42              ; serial (d. adams)
                                3H              ; refresh
                                15M             ; retry
                                1W              ; expiry
                                1D )            ; minimum
        IN      NS      localhost
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0.
Directorio /var/etc/named/chroot/var/named/named.cero

SCRIPT DE CONFIGURACIÓN 2. 11

ARCHIVO LOCALHOST.ZONE.RPMSAVE

```
Localhost.zone.rpmsave
$TTL  86400
@           IN SOA      @       root.tesis.com (
                                42          ; serial (d. adams)
                                3H          ; refresh
                                15M         ; retry
                                1W          ; expiry
                                1D )        ; minimum
              IN NS             @
            IN A        127.0.0.1
            IN AAAA           ::1
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0.
Directorio /var/etc/named/chroot/var/localhost.zone.rpmsave

SCRIPT DE CONFIGURACIÓN 2. 12

ARCHIVO LOCALDOMAIN.ZONE.RPMSAVE

```
Localdomain.zone.rpmsave
$TTL  86400
@           IN SOA      byron root (
                                42          ; serial (d. adams)
                                3H          ; refresh
                                15M         ; retry
                                1W          ; expiry
                                1D )        ; minimum
              IN NS             byron
byron IN A        127.0.0.1
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0.
Directorio /var/etc/named/chroot/var/ localdomain.zone.rpmsave

SCRIPT DE CONFIGURACIÓN 2. 13

ARCHIVO NAMED.LOCAL.RPMSAVE

```
named.local.rpmsave
$TTL  86400
@       IN      SOA     localhost. root.localhost  (
                                      1997022700 ; Serial
                                      28800      ; Refresh
                                      14400      ; Retry
                                      3600000    ; Expire
                                      86400 )    ; Minimum
              IN      NS      localhost.

1       IN      PTR     localhost.
```

Fuente: SISTEMA OPERATIVO CENTOS 4.0.
Directorio /var/etc/named/chroot/var/ named.local.rpmsave

2.3.4.8 Archivo de configuración de zona

SCRIPT DE CONFIGURACIÓN 2. 14

ARCHIVO VENTAS.TESIS.COM

ventas.tesis.com

```
$TTL 86400
@       IN SOA        localhost.ventas.tesis.com.
root.localhost.ventas.tesis.com. (
                              61        ; serial
                              10800     ; refresh (3 hours)
                              900       ; retry (15 minutes)
                              604800    ; expire (1 week)
                              86400     ; minimum (1 day)
                              )
@               IN NS         localhost.ventas.tesis.com.
localhost               IN A          192.168.1.1
localhost               IN A          192.168.1.65
localhost               IN A          192.168.1.129
```

Directorio /var/etc/named/chroot/var/ ventas.tesis.com

El formato de un fichero de zona es el siguiente:

nombrederegistro IN tipodeentrada valor

Los registros de DNS que más se utilizan son:

SOA:

Comienzo de Zona con Autoridad (Start Of zone Authority)

NS :

Un servidor de nombres con autoridad para una determinada zona

A :

Una dirección IP de una máquina

CNAME:

El nombre canónico de una máquina para definir un alias. (este parámetro no es utilizado en esta configuración.

MX :

Servidor de Correo (este parámetro no es utilizado en esta configuración)

PTR :

Un puntero a un nombre de dominio (utilizados para definir el DNS inverso)

ventas.tesis.com.:

Nombre de dominio, también el origen para el fichero de zona

localhost.ventas.tesis.com.:

Servidor de nombres primario/autoritario para esta zona

root.localhost.ventas.tesis.com.:

La persona responsable de esta zona; observe que la dirección de correo electrónico aparece con la @ sustituida por un punto.

61

Número de serie del fichero, el cual se incrementa cada vez que se modifique el fichero de zona. El número de serie es importante ya que para avisar a los servidores de nombres esclavos de que se ha actualizado la zona.

@ IN NS localhost.ventas.tesis.com.

Esta es una entrada de tipo NS. Cada servidor de nombres que contesta de forma autoritaria a las consultas de un determinado dominio debe tener una de estas entradas. El carácter @ se sustituye por el origen, es decir ventas.tesis.com

localhost IN A 192.168.1.1

El registro de tipo A hace referencia a nombres de computadores. Como se puede ver localhost.ventas.tesis.com se resuelve a 192.168.1.1, así sucesivamente.

Otros archivos de configuración de zonas

SCRIPT DE CONFIGURACIÓN 2. 15

ARCHIVO CONTABILIDAD.TESIS.COM

contabilidad.tesis.com

```
$TTL 86400
@     IN SOA      localhost.contabilidad.tesis.com.
root.localhost.contabilidad.tesis.com. (
                        105         ; serial
                        10800       ; refresh (3 hours)
                        900         ; retry (15 minutes)
                        604800      ; expire (1 week)
                        86400       ; minimum (1 day)
                        )
@                  IN NS        localhost.contabilidad.tesis.com.
Localhost          IN A         192.168.2.1
```

Directorio /var/etc/named/chroot/var/ contabilidad.tesis.com

SCRIPT DE CONFIGURACIÓN 2. 16

ARCHIVO RRHH.TESIS.COM

rrhh.tesis.com

```
$TTL 86400
@     IN SOA      localhost.rrhh.tesis.com.
root.localhost.rrhh.tesis.com. (
                        48          ; serial
                        10800       ; refresh (3 hours)
                        900         ; retry (15 minutes)
                        604800      ; expire (1 week)
                        86400       ; minimum (1 day)
                        )
@                  IN NS        localhost.rrhh.tesis.com.
localhost          IN A         192.168.3.1
```

Directorio /var/etc/named/chroot/var/ rrhh.tesis.com

2.3.4.9 Archivo de configuración de zona in-addr.arpa (DNS inverso)

Este archivo proporciona las asociaciones de direcciones IP con nombres de computadoras.

SCRIPT DE CONFIGURACIÓN 2. 17

ARCHIVO 192.168.1.REVERSO

192.168.1.reverso

```
$TTL  86400
1.168.192.in-addr.arpa  IN SOA      localhost.ventas.tesis.com.
root.localhost.ventas.tesis.com. (
                        1997022714 ; serial
                        28800      ; refresh (8 hours)
                        14400      ; retry (4 hours)
                        3600000    ; expire (5 weeks 6 days 16 hours)
                        86400      ; minimum (1 day)
                        )
@       IN      NS      localhost.ventas.tesis.com.
1       IN      PTR     localhost.ventas.tesis.com.
65      IN      PTR     localhost.ventas.tesis.com.
129     IN      PTR     localhost.ventas.tesis.com.
```

Directorio /var/etc/named/chroot/var/ 192.168.1.reverso

En este tipo de configuración de zona inversa se utiliza el mismo formato excepto que se especifican registros *PTR* en lugar de registros *A* o *CNAME*.

Otros archivos de configuración de zona inversa

SCRIPT DE CONFIGURACIÓN 2. 18

ARCHIVO 192.168.2.REVERSO

192.168.2.reverso

```
$TTL  86400
@     IN SOA      localhost.contabilidad.tesis.com.
root.localhost.contabilidad.tesis.com. (
                        1997022726 ; serial
                        28800      ; refresh (8 hours)
                        14400      ; retry (4 hours)
                        3600000    ; expire (5 weeks 6 days 16 hours)
                        86400      ; minimum (1 day)
                        )
@       IN      NS      localhost.contabilidad.tesis.com.
1       IN      PTR     localhost.contabilidad.tesis.com.
```

Directorio /var/etc/named/chroot/var/ 192.168.2.reverso

SCRIPT DE CONFIGURACIÓN 2. 19

ARCHIVO 192.168.3.REVERSO

192.168.3.reverso

```
$TTL 86400
@     IN SOA      localhost.rrhh.tesis.com.
root.localhost.rrhh.tesis.com. (
                        1997022704 ; serial
                        28800      ; refresh (8 hours)
                        14400      ; retry (4 hours)
                        3600000    ; expire (5 weeks 6 days 16 hours)
                        86400      ; minimum (1 day)
                        )
@       IN      NS      localhost.rrhh.tesis.com.
1       IN      PTR     localhost.rrhh.tesis.com.
```

Directorio /var/etc/named/chroot/var/ 192.168.3.reverso

Como última configuración, como el servidor de nombres en este proyecto va a ser local es necesario añadir una línea para indicar que el propio computador va a ser el servidor de nombres.

En el archivo /etc/resolv.conf

Insertar la siguiente línea:

nombre_servidor dirección_ip

localhost 127.0.0.1

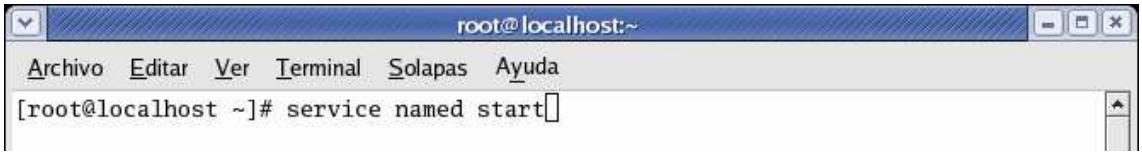
2.3.4.10 Inicio del Servicio

El servicio named (DNS) se encuentra ubicado en el directorio ** /etc/sbin/named.

Para iniciar el servicio named ejecutar el comando, desde cualquier ubicación.

service named Start

GRÁFICO 2. 16
COMANDO DE INICIO DEL SERVICIO DNS



Fuente: SISTEMA OPERATIVO CENTOS 4.0. Ventana de un Terminal

Para iniciar el servicio DHCP ejecutar el comando.

service dhcpd start

GRÁFICO 2. 17
COMANDO DE INICIO DEL SERVICIO DHCP

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Ventana de un Terminal

Para parar la ejecución del servicio named ejecutar el siguiente comando:

service named stop

Para parar la ejecución del servicio dhcpd ejecutar el siguiente comando:

service dhcpd stop

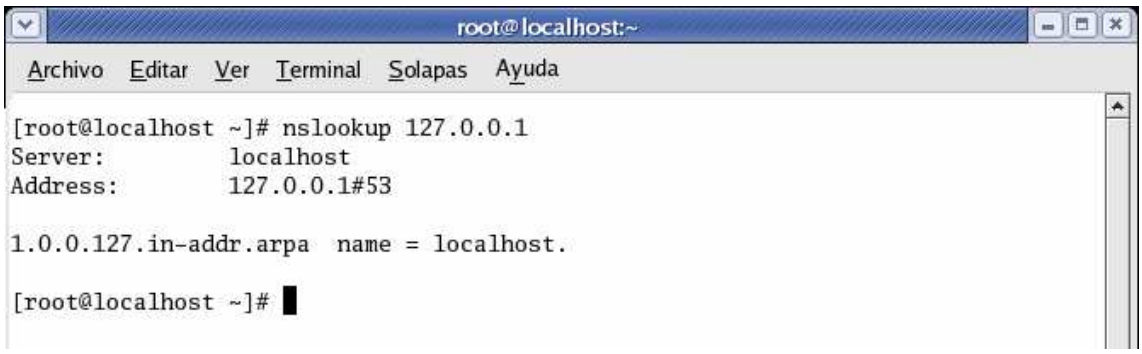
Una vez iniciado los servicios, se comprueba si el dns resuelve por nombre del servidor local, con la ayuda del comando nslookup, como se muestra en la siguiente pantalla:

GRÁFICO 2. 18
RESULTADO DE UNA CONSULTA AL DNS DE LOCALHOST

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Ventana de un Terminal

Se comprueba la resolución de nombres inversa de la dirección local.

GRÁFICO 2. 19
RESULTADO DE UNA CONSULTA DNS POR IP



Fuente: SISTEMA OPERATIVO CENTOS 4.0. Ventana de un Terminal

De acuerdo al diseño del proyecto el servidor posee tres tarjetas de red físicas (eth0, eth1, eth2) y dos tarjetas de red virtuales (eth1:1, eth2:1) que se asocian a cada VLAN, y a cada una de éstas se las asocia con una zona.

TABLA 2. 1

DISTRIBUCION DE LAS ZONAS EN CADA INTERFAZ DE RED

INTERFAZ	DIRECCION IP	RED	DOMINIO
eth0	192.168.1.1/26	VLAN 1 ->	ventas.tesis.com (vlan móvil)
eth1	192.168.1.65/26	VLAN 1 ->	ventas.tesis.com (vlan móvil)
eth2	192.168.1.129/26	VLAN 1 ->	ventas.tesis.com (vlan móvil)
eth1:1	192.168.2.1/26	VLAN 2 ->	contabilidad.tesis.com
eth2:1	192.168.3.1/26	VLAN 3 ->	rrhh.tesis.com

Ejemplo de la distribución de las zonas DNS en cada interfaz de red

2.3.4.11 Consultas de zona directa

Se verifica la resolución de la zona directa, realizando una consulta al servidor dns por nombre.

Se realiza una consulta al servidor de nombres local del subdominio rrhh.tesis.com:

GRÁFICO 2. 20

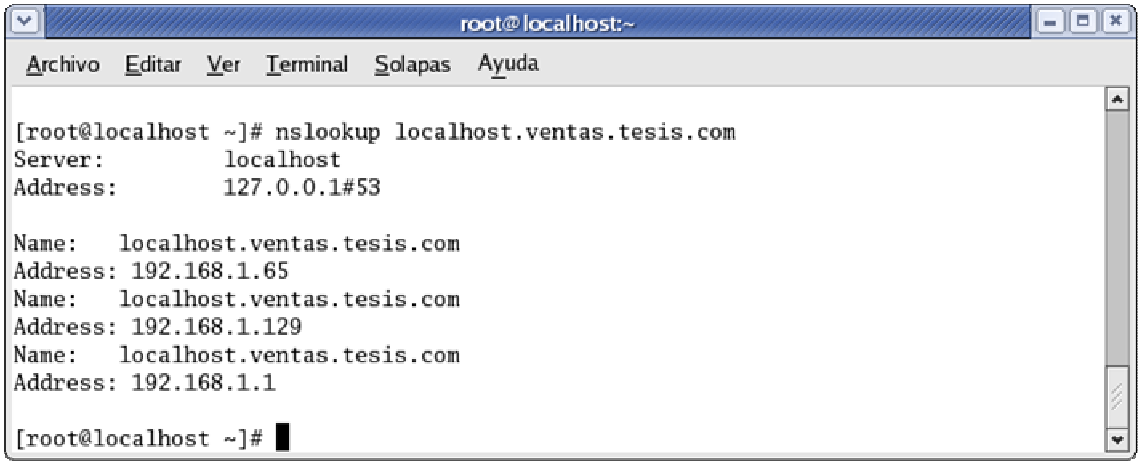
RESULTADO DE UNA CONSULTA DE UN SUBDOMINIO AL DNS

Fuente: SISTEMA OPERATIVO CENTOS 4.0. Ventana de un Terminal

Por último se consulta al servidor local de nombres acerca del subdominio ventas.tesis.com:

GRÁFICO 2. 21

RESULTADO DE UNA CONSULTA DE UN SUBDOMINIO AL DNS



Fuente: SISTEMA OPERATIVO CENTOS 4.0. Ventana de un Terminal

El resultado anterior es diferente a los dos primeros debido que hay que tomar en cuenta que este subdominio (ventas.tesis.com) tiene asociado 3 direcciones IP's.

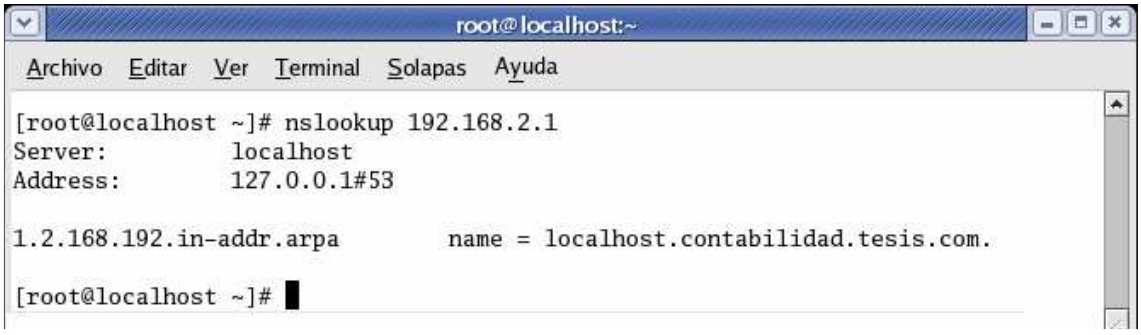
2.3.4.12 Consultas de zona inversa

Se verifica la resolución de la zona inversa, realizando una consulta al servidor dns por dirección IP.

Consulta a la zona inversa la dirección IP 192.168.2.1 (vlan 2), el resultado debe corresponder al subdominio contabilidad.tesis.com, comprobamos mediante la siguiente pantalla:

GRÁFICO 2. 22

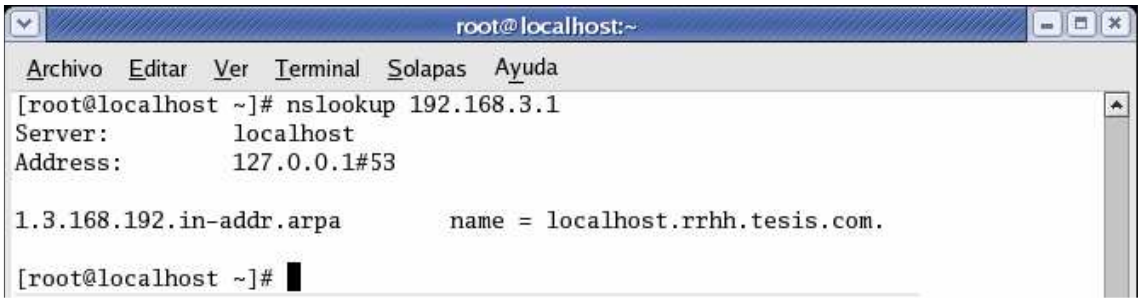
RESULTADO DE UNA CONSULTA INVERSA DE UN SUBDOMINIO AL DNS



Fuente: SISTEMA OPERATIVO CENTOS 4.0. Ventana de un Terminal

De la misma manera se comprueba con la direcciones IP del localhost que tenemos asociadas al subdominio rrhh.tesis.com en la vlan 3.

GRÁFICO 2. 23
RESULTADO DE UNA CONSULTA INVERSA DE UN SUBDOMINIO AL DNS



Fuente: SISTEMA OPERATIVO CENTOS 4.0. Ventana de un Terminal

El mismo resultado anterior se tendrá si se consulta las direcciones IP`s de la VLAN 1 (móvil), la cual tiene asociado 3 direcciones IP's, por ejemplo la dirección IP 192.168.1.1.

2.3.4.13 Interacción con los clientes

Cuando un computador cliente arranca, el servidor realiza varios procesos para atenderlo, a continuación se listan los principales:

Se asume que el servidor tiene los servicios dhcpd y named levantados y el cliente tiene configurado para obtener automáticamente los parámetros de red y físicamente se conecta a la interfaz eth0.

2.3.4.14 Obtención de una Dirección IP

El computador cliente puede forzar una nueva obtención de una dirección IP con el siguiente comando:

ipconfig /renew

Desde el computador cliente:

GRÁFICO 2. 24

EJECUCIÓN DEL COMANDO PARA RENOVAR UNA DIRECCION IP

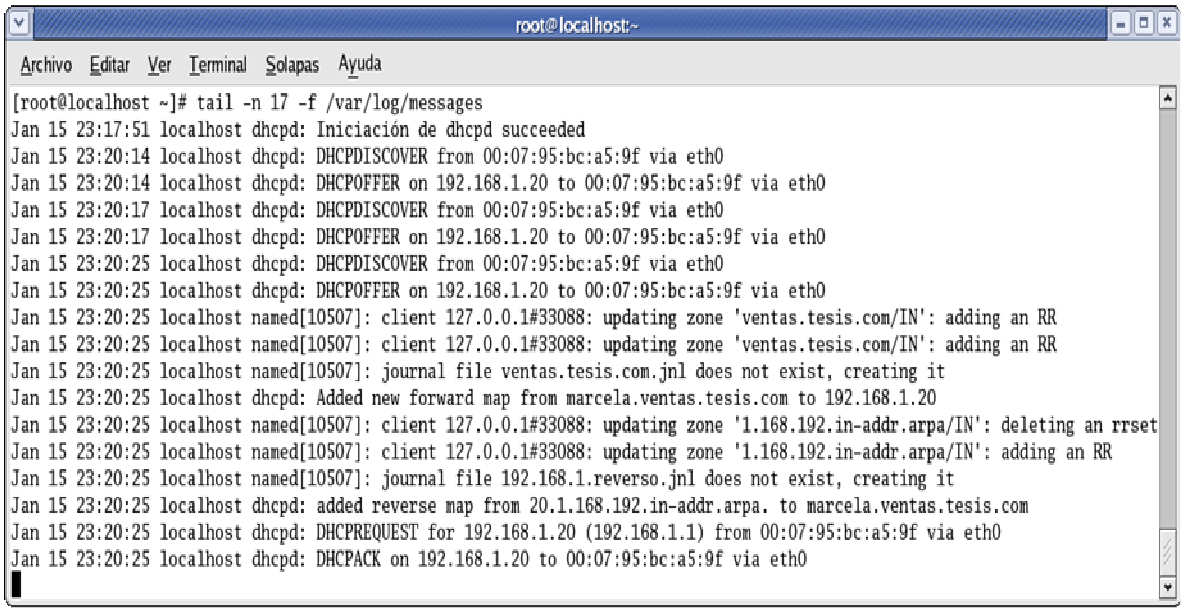
Fuente: SISTEMA OPERATIVO CENTOS 4.0. Ventana de un Terminal

El computador cliente arranca y solicita al servidor DHCP sus datos TCP/IP, el servidor le ofrece una dirección IP y el dhcpd comunica al DNS que actualiza sus tablas, el ordenador cliente le comunica al dhcpd que acepta los datos y el dhcpd le contesta que está conforme. Este hecho genera varias líneas de registros que se almacenan en el archivo /var/log/messages, a los cuales pueden ser visualizados con el comando:

tail –n 17 – f /var/log/messages
-n = número de líneas a ser visualizadas
-f = especifica el camino y nombre de la carpeta.

GRÁFICO 2. 25

VISTA DE LOS LOGS DEL SISTEMA CUANDO EL CLIENTE SOLICITA EL SERVICIO DHCP Y DNS DINAMICO



Fuente: SISTEMA OPERATIVO CENTOS 4.0. Directorio /var/log/messages

Explicación:

Como se observa en la pantalla anterior los mensajes que se intercambian como parte del protocolo DHCP, a continuación se lista una pequeña explicación de cada uno, vale recalcar que el servicio dhcp interactúa con el servicio dns dinámico.

DHCPDISCOVER from 00:07:95:bc:a5:9f via eth0
Este es un mensaje de broadcast de un cliente con dirección MAC 00:07:95:bc:a5:9f realiza para detectar el servidor DHCP, el servidor lo atiende por la interfaz eth0.

DHCPOFFER on 192.168.1.20 to 00:07:95:bc:a5:9f via eth0
Este es un mensaje en donde el servidor DHCP realiza una oferta de configuración a un cliente, le ofrece la dirección IP 192.168.1.20 a la dirección MAC 00:07:95:bc:a5:9f y lo realiza vía la interfaz eth0.

Client 127.0.0.1#3308:updating zone 'ventas.tesis.com/IN' adding an RR
Este es un mensaje del servicio named (DNS), el cual comunica que la zona 'ventas.tesis.com', esta siendo actualizada automáticamente. Esto es lógico ya que el computador se conectó físicamente a la interfaz eth0 la cual está asociada con el subdominio ventas.tesis.com.

journal file ventas.tesis.com.jnl does not exist, creating it
El servicio dns dinámico cuando está en ejecución trabaja con un archivo tipo journal (archivo de trabajo) por cada zona que esté configurada que realice la actualización dinámicamente. El archivo journal se crea la primera vez que un cliente realice una petición de actualización.

Added new forward map from marcela.ventas.tesis.com to 192.168.1.20
En este mensaje el DHCP comunica al DNS que actualice sus tablas con el nombre de host marcela.ventas.tesis.com y la IP 192.168.1.20

Client 127.0.0.1#3308:updating zone '1.168.192.in-addr.arpa/IN' adding an RR
Este es un mensaje del servicio named (DNS), el cual comunica que la zona inversa '1.168.192.in-addr.arpa/IN', esta siendo actualizada.

Added reverse map from 20.1.168.192.in-addr.arpa to marcela.ventas.tesis.com
En este mensaje el DHCP comunica al DNS que actualice sus tablas con la dirección IP 192.168.1.20 y el nombre de host marcela.ventas.tesis.com.

DHCPREQUEST for 192.168.1.20 (192.168.1.1) from 00:07:95:bc:a5:9f via eth0
En este mensaje el cliente que posee la MAC 00:07:95:bc:a5:9f comunica al servidor que acepta la oferta IP 192.168.1.20 de un servidor determinado 192.168.1.1, vía la interfaz de red eth0.

DHCPACK on 192.168.1.20 to 00:07:95:bc:a5:9f via eth0
En este mensaje el servidor hacia el cliente le envía la configuración asignada excluyendo la dirección IP que ya fue aceptada.

2.3.4.15 Liberación de la Dirección IP

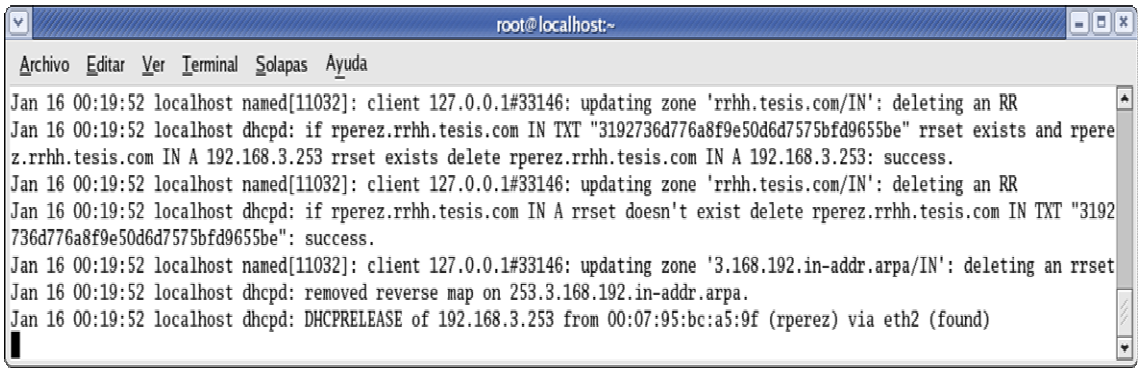
Cuando un computador desea liberar la dirección IP, por alguna razón, en este caso es cuando un computador móvil desea conectarse físicamente de una VLAN a otra VLAN, es necesario que la dirección IP se libere y en la próxima VLAN que se conecte le asigne una nueva dirección IP y actualice el DNS de manera automática. Para comprobar este hecho se puede forzar en el cliente a liberar la IP con el siguiente comando:
Desde el computador cliente:

GRÁFICO 2. 26
EJECUCIÓN DEL COMANDO PARA LIBERAR UNA DIRECCION IP

Fuente: SISTEMA OPERATIVO WINDOWS. Ventana de un Terminal

En el proceso de la liberación IP en el Servidor se observa en el log /var/log/message de la siguiente manera:

GRÁFICO 2. 27
VISTA DE LOS LOGS DEL SISTEMA CUANDO EL CLIENTE LIBERA EL SERVICIO DHCP Y DNS DINAMICO



Fuente: Sistema Operativo CentOS. Ventana de comando.

El ordenador rperez.rrhh.tesis.com que corresponde a la VLAN3 libera la dirección IP.

client 127.0.0.1#33146: updating zone 'rrhh.tesis.com/IN':deleting an RR
Este mensaje se refiere a que se está actualizando la zona rrhh.tesis.com eliminando el registro que enlaza el nombre del computador que solicitó la liberación con la dirección IP.

If rperez.rrhh.tesis.com IN TXT "3192736d776a8f9e50d6d757bfd9655be" reset exists and rperez.rrhh.tesis.com IN A 192.168.3.253 rrset exists delete rperez.rrhh.tesis.com IN A 192.168.3.253: success.
Este es un mensaje que realiza el dhcpd el cual mediante una sentencia condicional comprueba si existe dentro de las zonas el registro que se va a liberar.

client 127.0.0.1#33146: updating zone '3.168.192.in-addr.arpa/IN':deleting an rrset

Este mensaje se refiere a que se está actualizado la zona '3.168.192.in-addr.arpa/IN', eliminando el registro que enlaza la dirección IP con el nombre del computador que solicitó la liberación.

removed reverse map on 253.3.168.192.in-addr.arpa.
Este mensaje confirma que ha sido eliminado en la zona inversa la dirección IP 192.168.3.253.

DHCPRELEASE of 192.168.3.253 from 00:07:95:bc:a5:pf (rperez) via eth2 (found)
Este mensaje se origina del cliente al servidor para indicar que renuncia a la dirección otorgada y cancela lo que queda del contrato establecido anteriormente.

2.3.5 CONFIGURACIÓN DE FIREWALL

2.3.5.1 IPtables

IPTABLES es un sistema de Firewall que está integrado al kernel de Linux (a partir del kernel 2.4) y forma parte del sistema operativo. Consiste en un script de shell en el que se va ejecutando las diversas reglas de Firewall.

Existen tres tipos de reglas de filtrado:

Filtrado de Entradas (INPUT).- las reglas de entradas son aplicadas a los datagramas recibidos en un dispositivo de red.

Filtrado de Salidas (OUTPUT).- Las reglas de salidas son aplicadas a los datagramas que va a transmitir un dispositivo de red.

Filtrado de Reenvíos (FORWARD).- Las reglas de reenvíos se aplican a datagramas que reciben pero que no son para esta máquina, como por ejemplo datagramas que entran por una interfaz para ser encaminada por otra.

Además de la reglas de filtrado, es posible aplicar reglas de NAT (Network Address Resolution) que se utilizan para realizar redirecciones de puertos o

cambios en las direcciones IP's de origen /destino; y reglas de tipo MANGLE que son destinadas a modificar los paquetes.

2.3.5.2 Maneras de implementar un Firewall

Existen dos maneras para implementar un Firewall:

La primera se refiere a una política por defecto ACEPTAR, donde todo lo que entra y sale por el Firewall se acepta y solo se denegará lo que se diga.

La segunda es una política por defecto DENEGAR, donde todo está denegado y solo se admitirá pasar por el Firewall lo que explícitamente se permita. Este tipo de configuración se implementa en este Proyecto.

Hay que tomar muy en cuenta el orden de las reglas de un Firewall, ya que éste va comparando cada regla de arriba hacia abajo hasta que coincida que afecte a el paquete, aplica esa regla y no mira más reglas.

2.3.5.3 Implementación

Se crea un archivo que es un script de shell, el mismo que va a contener todas las reglas de filtrado:

SCRIPT DE CONFIGURACIÓN 2. 20
ARCHIVO IPTABLES.SH

"iptables.sh"

Al interior de este fichero se escribe las siguientes líneas, que son las reglas que se aplica al Firewall. El símbolo "#" indica que es un comentario.

```
#!/bin/sh

# FLUSH de reglas, limpieza de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

echo -n Aplicando reglas de Firewall
```

```
#Establecimiento de políticas por defecto DROP (negamos todo)

#iptables -t nat -P PREROUTING DROP
#iptables -t nat -P POSTROUTING DROP

iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

#HABILITAR LAS REDES VIRTUALES
iptables -A INPUT -s 192.168.1.0/26 -i eth0 -j ACCEPT
iptables -A OUTPUT -d 192.168.1.0/26 -j ACCEPT
iptables -A INPUT -s 192.168.1.64/26 -i eth1 -j ACCEPT
iptables -A OUTPUT -d 192.168.1.64/26 -j ACCEPT
iptables -A INPUT -s 192.168.1.128/26 -i eth2 -j ACCEPT
iptables -A OUTPUT -d 192.168.1.128/26 -j ACCEPT

#HABILITAR LAS REDES FISICAS eth1 y eth2
iptables -A INPUT -s 192.168.2.0/24 -i eth1 -j ACCEPT
iptables -A OUTPUT -d 192.168.2.0/24 -j ACCEPT
iptables -A INPUT -s 192.168.3.0/24 -i eth2 -j ACCEPT
iptables -A OUTPUT -d 192.168.3.0/24 -j ACCEPT


#LINEA QUE SIGNIFICA QUE VA A EXISTIR RUTEO ENTRE TODAS LAS
REDES
echo 1 > /proc/sys/net/ipv4/ip_forward

#DESHABILITAR LA CONEXION ENTRE LA eth0 Y LA eth1
#iptables -A FORWARD -s 192.168.1.0/26 -d 192.168.2.0/26 -j
DROP
#iptables -A FORWARD -s 192.168.2.0/26 -d 192.168.1.0/26 -j
DROP
#iptables -A INPUT -s 192.168.1.15 -d 192.168.3.1 -j DROP
#iptables -A OUTPUT -s 192.168.1.15 -d 192.168.3.1 -j DROP

#ENLAZAR LA eth0 CON LA eth1:1
iptables -A FORWARD -s 192.168.1.0/26 -d 192.168.1.64/26 -j
ACCEPT
iptables -A FORWARD -s 192.168.1.64/26 -d 192.168.1.0/26 -j
ACCEPT
iptables -A INPUT -s 192.168.1.70 -j ACCEPT
iptables -A OUTPUT -d 192.168.1.70 -j ACCEPT
iptables -A FORWARD -s 192.168.1.70 -d 192.168.1.20 -j ACCEPT
iptables -A FORWARD -s 192.168.1.20 -d 192.168.1.70 -j ACCEPT

#ENLAZAR LA eth0 CON LA eth2:1
iptables -A FORWARD -s 192.168.1.0/26 -d 192.168.1.128/26 -j
ACCEPT
iptables -A FORWARD -s 192.168.1.128/26 -d 192.168.1.0/26 -j
ACCEPT
```

```
#ENLAZAR LA eth2:1 CON LA eth1:1
iptables -A FORWARD -s 192.168.1.64/26 -d 192.168.1.128/26 -j
ACCEPT
iptables -A FORWARD -s 192.168.1.128/26 -d 192.168.1.64/26 -j
ACCEPT

#HABILITAR SERVICIOS ENTRE LOS HOST DE REDES DIFERENTES
#ACCESO DESDE UN HOST MOVIL A UN SERVIDOR WEB (192.168.2.5)
iptables -A FORWARD -s 192.168.1.0/26 -d 192.168.2.5 -p tcp --
dport 8080 -j ACCEPT
iptables -A FORWARD -s 192.168.2.5 -d 192.168.1.0/26 -p tcp --
sport 8080 -j ACCEPT
iptables -A FORWARD -s 192.168.1.64/26 -d 192.168.2.5 -p tcp --
dport 8080 -j ACCEPT
iptables -A FORWARD -s 192.168.2.5 -d 192.168.1.64/26 -p tcp --
sport 8080 -j ACCEPT
iptables -A FORWARD -s 192.168.1.128/26 -d 192.168.2.5 -p tcp -
-dport 8080 -j ACCEPT
iptables -A FORWARD -s 192.168.2.5 -d 192.168.1.128/26 -p tcp -
-sport 8080 -j ACCEPT



#ACCESO DESDE UN HOST MOVIL A UNA BASE DE DATOS (192.1068.2.6)
iptables -A FORWARD -s 192.168.1.0/26 -d 192.168.2.6 -p tcp --
dport 5432 -j ACCEPT
iptables -A FORWARD -s 192.168.2.6 -d 192.168.1.0/26 -p tcp --
sport 5432 -j ACCEPT
iptables -A FORWARD -s 192.168.1.64/26 -d 192.168.2.6 -p tcp --
dport 5432 -j ACCEPT
iptables -A FORWARD -s 192.168.2.6 -d 192.168.1.64/26 -p tcp --
sport 5432 -j ACCEPT
iptables -A FORWARD -s 192.168.1.128/26 -d 192.168.2.6 -p tcp -
-dport 5432 -j ACCEPT
iptables -A FORWARD -s 192.168.2.6 -d 192.168.1.128/26 -p tcp -
-sport 5432 -j ACCEPT
```

Ejemplo reglas de Firewall en base a iptables

Este archivo puede variar debido a que depende del Administrador que decida paquetes o puertos se va a permitir entre las diferentes VLANS.

Antes de ejecutar el archivo hay que dar permisos de ejecución, con el comando chmod.

chmod 750 iptables.sh

Para ejecutar el archivo con la ayuda del comando “sh”, ya que es un script de shell y se realiza de la siguiente manera:

#sh iptables.sh

En este momento el Firewall ya está corriendo por lo que las reglas se están aplicando.

2.3.6 INTERFAZ DE APLICACIÓN

Para facilitar las tareas de configuración e inicio del servicio del switch capa 3 que debe realizar el Administrador de la Red se construyó una Aplicación que permite configurar y poner en marcha el sistema de una manera gráfica y amigable.

2.3.6.1 Software utilizado

La aplicación está desarrollada en ambiente Web, para esto se utilizó lo siguiente:

- Lenguaje HTML
- Lenguaje XML
- Lenguaje PHP 4.3.4
- Servidor Web Apache.

2.3.6.2 Principales Funciones

La aplicación consiste en manipular el archivo de configuración del servicio DHCP y FIREWALL, lo cual me permite:

- Ingresar los datos de configuración de red de las tres vlans.
- Tener un control de los host que se utilizan en la vlan móvil.
- Ver la configuración que en ese momento se esté corriendo.
- Manejar las reglas del Firewall.
- Iniciar, reiniciar el servicio.

Además de todas las opciones necesarias para tener un control apropiado del switch capa 3 básico.

La aplicación se desarrolló en base a una consideración, que es ingresar direcciones de red de Clase C, debido a que la el proyecto está destinado a empresas pequeñas y medianas. Si el Administrador pretende configurar redes de otra clase, lo podrá hacer modificando directamente el script de configuración de los servicios.

A pesar de que este proyecto posee un servidor DNS, en la aplicación no se contempló interfaces para manipular los archivos de configuración de este servicio, ya que éste no es un objetivo específico del proyecto. Además es posible cambiar la configuración como así desee el Administrador modificando directamente el código.

Para ver un detalle de la aplicación, junto a una explicación de las pantallas gráficas Ver el Anexo No 1.

2.3.7 PRUEBAS

2.3.7.1 Objetivos de las pruebas

Realizar un ambiente de pruebas real que demuestre el funcionamiento de este proyecto

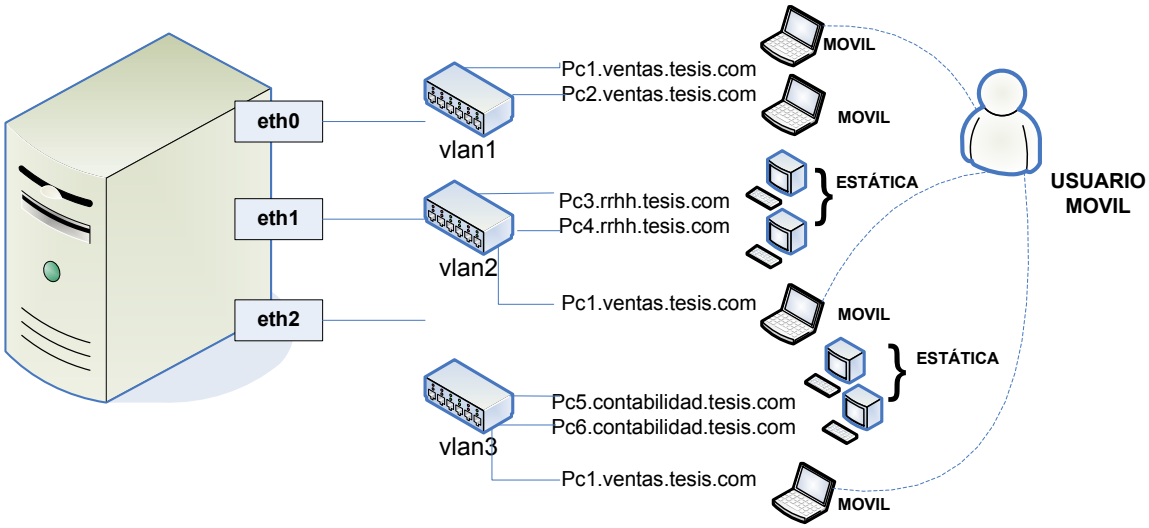
Dentro de las actividades que se realiza consta la configuración de las 3 VLAN, configuración de equipos móviles que están rotando en todas las VLAN´s y que estos host sean visibles a través de su nombre de dominio completamente expresado (FQDN).

2.3.7.2 Requerimientos

- El switch capa 3 en Linux encendido.
- Tres computadores clientes, uno para cada VLAN.
- Dos computadoras clientes, que cumplen la función de usuarios móviles, en lo posible computadores portátiles para que exista mayor facilidad al movilizarse.

- Tres switch convencionales, en donde cada uno se conecta a una interfaz de red del switch capa 3 y por otro lado se conecta a una VLAN.
- Cables punto a punto, para cada computador y conexión de los switch.

GRÁFICO 2. 28
ESQUEMA DE PRUEBAS



Ejemplo esquema de un ambiente de pruebas real

2.3.7.3 Resultados

Cada computador que se conecta a una VLAN, recibe automáticamente la dirección IP, nombre de dominio junto a los demás parámetros de configuración de red correspondientes. Ejemplo:

VLAN1:
pc1.ventas.tesis.com
pc2.ventas.tesis.com

VLAN2
pc3.rrhh.tesis.com
pc4.rrhh.tesis.com

VLAN3
pc5.rrhh.tesis.com
pc6.rrhh.tesis.com

El host pc1.ventas.tesis.com de la VLAN1, es un computador móvil, el mismo que físicamente se traslada a cualquier otra VLAN. Se verifica que un computador distinto, también perteneciente a la VLAN1 por ejemplo pc2.ventas.tesis.com tiene conexión al computador móvil, sin importar a que red esté conectado físicamente, siempre lo ubicará mediante su nombre de dominio completamente expresado (FQDN). Por ejemplo, se realiza un comando ping a pc1.ventas.tesis.com, desde pc2.ventas.tesis.com obteniendo resultados.

En el otro sentido, el computador móvil pc1.ventas.tesis.com que está conectado físicamente a otra red tiene respuesta a través del comando ping de su compañero pc2.ventas.tesis.com.

Un computador que pertenece a la VLAN2, por ejemplo pc3.rrhh.tesis.com que está adyacente al computador móvil pc1.ventas.tesis.com, incluso están conectados físicamente al mismo switch no se ven, a menos que se habilite una regla en el Firewall por algún servicio que tengan en común.

Es importante notar que un computador móvil siempre recibirá el nombre de dominio correspondiente a la VLAN móvil (ejemplo ventas.tesis.com), sin importar en que red físicamente esté conectada, por lo que siempre mantendrá su nombre completo de dominio cuando se traslade de una red a otra.

CAPITULO 3

ANALISIS COSTO-BENEFICIO

3.1 INTRODUCCIÓN

Debido al interés de las empresas pequeñas y medianas en obtener un dispositivo electrónico de red que resuelva sus problemas de dominios de colisión excesivos y permita mejorar el rendimiento de su red a través de técnicas de conmutación y enrutamiento de paquetes, es necesario realizar un análisis costo-beneficio a soluciones alternas a la compra de hardware especializados en realizar las funciones antes descritas. Una solución que se recomienda a estas empresas, es implementar el switch básico capa 3, presentado como tema de tesis de este proyecto.

3.2 ANÁLISIS ECONÓMICO

En la Tabla 3.1 se detallan los valores de los componentes hardware necesarios para la implementación del switch básico capa 3, estos se han descrito en base a costos que los proveedores comerciales de hardware de red publican.

TABLA 3. 1

DISPOSITIVOS Y ELEMENTOS DE HARDWARE PARA EL SWITCH BÁSICO CAPA 3

Cantidad	Descripción	P. Unit	Total
1	Procesador Intel Pentium IV de 2 GHz		180.00
1	Tarjeta madre Intel con mínimo 4 slots PCI		150.00
1	Memoria RAM de 512 MB		30.00
1	Disco duro de 60 GB		95.00
1	Monitor de 15 pulgadas		100.00
1	Teclado		10.00
1	Mouse ps/2		8.00
3	Tarjetas de red 10/100 MB	30.00	90.00
3	Switch de 8 puertos	18.00	60.00
1	Regulador de voltaje		15.00
1	Case TX		60.00
3	Cables de red UTP categoría 5 punto a punto	5.00	15.00
	Subtotal		813.00
	IVA 12%		97.50
	Total		**910.50**

Fuente: Compañía Megachips

El costo total para la adquisición del equipo hardware necesario para la implementación del switch básico capa 3 es de: $910.5 (novecientos diez dólares con cinco centavos).

En la siguiente tabla se detalla el valor necesario para la compra de un switch capa 3, indispensable para el manejo y la creación de las vlan’s.

TABLA 3. 2

COSTO DE UN SWITCH CAPA 3 EN EL MERCADO COMERCIAL

Cantidad	Descripción	P. Unitario ($)	Total ($)
1	Switch capa 3 serie 4500 marca Cisco WS-C3560-24TS-E	5010.00	5010.00
3	Cables de red UTP categoría 5 punto a punto	5.00	15.00
	Subtotal		5025.00
	IVA 12%		603.00
	Total		**5628.00**

Fuente: Compañía Uniplex S.A.

El costo total para la adquisición de un switch capa 3 marca 3com es de: $5628.00 (cinco mil seis cientos veinte y ocho dólares).

En la Tabla 3.2 se detallan el valor de los paquetes de software necesarios en la implementación del switch básico capa 3.

TABLA 3. 3

DESCRIPCIÓN DEL SOFTWARE UTILIZADO

Cantidad	Descripción	P. Unitario ($)	Total ($)
1	Sistema operativo CentOS	0.00	0.00
1	Servidor DHCP	0.00	0.00
1	Servidor DNS	0.00	0.00
1	Paquete PHP	0.00	0.00
1	Servidor WEB	0.00	0.00
	Descarga por internet	2.5	25.00
	Subtotal		0.00
	12% IVA		3.00
	Total		**28.00**

El costo total para la adquisición del software necesario en el switch básico es de: $28.00 (veinte y ocho dólares), ya que solo se necesita descargar de internet.

En la tabla siguiente se especifica un listado del software equivalente a los servicios que presta el switch capa 3 básico, necesarios para la creación y administración de las vlan's.

TABLA 3. 4
DESCRIPCIÓN DEL SOFTWARE UTILIZADO

Cantidad	Descripción	P. Unitario ($)	Total ($)
1	Sistema operativo Windows 2003 Server (incluye servidor DHCP y DNS)	400.00	400.00
1	Intérprete PHP	0	0
1	Servidor WEB	0	0
	Subtotal		400.00
	12% IVA		48.00
	Total		**448.00**

Fuente: Compañía MAINT S.A, para el primer producto.

El valor total para la compra del software es de: $448.00 (cuatro cientos cuarenta y ocho dólares).

Gastos incurridos en la consumación de un Firewall para administración de las vlan's, se los describe en la Tabla 3.5 siguiente:

TABLA 3. 5

VALOR ADQUISICIÓN DE UN FIREWALL PARA EL SWITCH BÁSICO CAPA 3

Cantidad	Descripción	P. Unitario ($)	Total($)
1	Kernel ver. 2.4 para manejo de Iptables	0.00	0.00
	Subtotal		0.00
	12% IVA		0.00
	Total		**0.00**

El total de gastos que demandan la incorporación de un Firewall al sistema switch básico capa 3 es de: $ 0 (cero dólares).

A continuación se muestra la Tabla 3.6, en la que se indica el valor que debe invertir una empresa en la adquisición de un Firewall.

TABLA 3. 6

VALOR ADQUISICIÓN DE UN FIREWALL

Cantidad	Descripción	P. Unitario ($)	Total($)
1	Firewall ISA de Microsoft	180.00	180.00
	Subtotal		180.00
	12% IVA		21.60
	Total		201.60

Fuente: Compañía MAINT S.A

Valor para la compra de Firewall ISA, $201.60 (dos cientos un dólares con sesenta centavos).

En la tabla 3.7 se muestra el valor del costo recurso humano para la implementación del switch básico capa 3.

TABLA 3. 7

DESCRIPCIÓN COSTO RECURSO HUMANO PARA EL SWITCH BÁSICO CAPA 3

Cantidad	Descripción	P. Unitario/mes ($)	Nº meses	Total ($)
2	Prestación de servicios profesionales de técnicos especialistas en redes	100.00	4	800.00
	Subtotal			800.00
	12% IVA			96.00
	Total			896.00

El valor total para el pago de servicios profesionales a los técnicos especialistas en la implementación del switch básico capa 3 es de: $896.00 (ocho cientos noventa y seis dólares).

En la presente tabla se describe el valor presupuestado para la contratación de señores técnicos con certificado Microsoft.

TABLA 3. 8

COSTO RECURSO HUMANO PARA EL SWITCH BÁSICO CAPA 3

Cantidad	Descripción	P. Unitario/hora ($)	Nº horas	Total ($)
1	Prestación de servicios profesionales de técnico Mycrosoft	40.00	5	200.00
	Subtotal			200.00
	12% IVA			24.00
	Total			224.00

Fuente: Expertech S.A. profesional especialista de Microsoft

Valor necesario para contratación de los servicios del técnico especialista Microsoft es de: $224.00 (dos cientos veinte y cuatro dólares).

Según los valores obtenidos, a continuación se realiza un análisis costos implementación switch básico capa 3 vs compra switch capa 3 Cisco

Los valores obtenidos en las diferentes tablas del análisis económico llegan a la siguiente conclusión:

TABLA 3. 9
SWITCH BÁSICO CAPA 3 VS SWITCH CAPA 3 CISCO

Descripción	SWITCH BÁSICO CAPA 3 (cantidad en dólares)	SWITCH CAPA 3 CISCO (cantidad en dólares)
Valor dispositivos y componentes Hardware	910.50	5628.00
Valor de Software utilizado	28.00	448.00
Valor adquisición de Firewall	0.00	201.60
Valor Recursos Humanos	896.00	224.00
Total	1834.50	6501.60

Como se puede observar existe un ahorro sustancial en la implementación del switch básico capa 3, ya que al restar $6501.60 de $1834.50, la empresa tendría $4667.10 (cuatro mil seis cientos sesenta y siete dólares con diez centavos) a favor suyo para disponer en otros proyectos.

3.3 ANÁLISIS LEGAL

El proyecto presentado en esta tesis posee componentes de hardware y software, los mismos que son sujetos a un análisis legal, el cual no viole los derechos de autor de los productos.

En los componentes de Hardware cada dispositivo por ser un bien tangible, al momento de la adquisición el proveedor cede todos los derechos sobre él, pasando así como único propietario la empresa o persona que adquirió.

En los componentes de Software la situación varía un poco respecto a la anterior, ya que se trata de bienes intangibles, los mismos que tienen derecho de propiedad intelectual. A continuación se muestra una lista del software utilizado junto con el licenciamiento de cada una.

TABLA 3. 10
DESCRIPCIÓN DEL SOFTWARE UTILIZADO

Paquete	Descripción	Tipo de licencia
CentOS	Sistema operativo	GNU
DHCP	Servidor DHCP de Linux	GNU
BIND	Servidor DNS de Linux	GNU
PHP	Lenguaje interpretador	GNU
APACHE	Servidor WEB	GNU

Como se observa en la tabla anterior todos los productos poseen licencia GNU (General Public Licency), la cual indica que no posee licenciamiento pagado y su uso es público e ilimitado para el número de usuarios, además su código es abierto, si desea más información acerca de los términos de la licencia GNU.

En el caso de utilizar el switch capa 3 del mercado comercial se aplica los mismos conceptos, en los componentes de hardware al momento de adquirir el dispositivo el nuevo propietario ejerce derecho sobre él.

Como el proyecto de tesis que se plantea en este documento ejerce funciones de servicio de DNS, DHCP, FIREWALL, es necesario comparar con la tecnología Windows que también provee todos estos servicios.

En Microsoft Windows toda licencia tiene un valor intelectual representado en costo, y existen diferentes tipos de licenciamiento, ejemplo el número de conexiones clientes en el servidor, etc.

En la Tabla 3.2 se detallan las condiciones legales en las que se encuentran todos y cada uno de los paquetes de software utilizados.

3.4 ANÁLISIS TÉCNICO

Una de las maneras de reducir gastos al máximo en la implementación de un dispositivo electrónico que realice las mismas funciones que un hardware capa 3 comercial específico, es el desarrollo de un módulo, que maneje de forma lógica todas esas labores de configuración de red, mediante la utilización tanto de componentes electrónicos de bajo costo comercial como de software, en base a esto se decidió crear esta solución alternativa con el sistema operativo Linux versión CentOS y kernel versión 2.4 en el cual se puede incorporar ya sea en el momento de la instalación o después la descarga de los paquetes para el configuración del servidor DHCP, servidor DNS (BIND), el Firewall, el servidor WEB, lenguaje de etiquetas XML y lenguaje HTML.

Además de que el sistema operativo Linux es de distribución libre, es muy estable y robusto en el manejo, distribución y administración de paquetes IP, es la solución más apta en reducción de gastos de las pequeñas y medianas empresas.

Es conveniente pensar sobre el tema de las actualizaciones en los sistemas de distribución libre como es el caso de Linux versión Centos, ya que en toda empresa grande se requiere que, éstas actualizaciones o soluciones a los problemas, lleguen inmediatamente y a tiempo, pero para las empresas que son pequeñas, es una mínima desventaja que deben correr a cambio de lo que se

dijo, el factor dinero, ya que estas actualizaciones se darán pero tal vez no con la misma prontitud.

3.5 ANÁLISIS OPERATIVO

La empresa interesada en la utilización de este proyecto de tesis debe tener a su disposición una persona entrenada en el manejo del sistema Linux, y si no lo tiene, debe solicitar un entrenamiento previo para la persona delegada al manejo de este por parte de los diseñadores del proyecto, para que el sistema funcione a su máxima capacidad.

En lo posible los dispositivos electrónicos que conforman el switch básico capa 3 deben ser de marcas prestigiosas y reconocidas, como por ejemplo las tarjetas de red 10/100 Mb, a fin de garantizar su óptimo desenvolvimiento, aunque en la elaboración de este proyecto se utilizaron tarjetas de diferentes fabricantes y su desarrollo fue exitoso.

Tener muy presente que este proyecto de tesis desarrollado solo esta diseñado para la creación y administración de subredes tipo C, así que se debe tener muy en cuenta los datos ingresados en esta etapa de configuración, aunque el sistema operativo Linux esta en la capacidad de aceptar cualquier tipo de clase de red, pero el administrador, si en un momento lo necesitara, debe configurarlo en forma manual todos los archivos necesarios. De igual forma, el servidor DNS (BIND) se lo ha configurado para que los nombres de dominio y las zonas de resolución de nombres tanto directa como inversa se los cree automáticamente en sus respectivos archivos de configuración, pero con los nombres ya establecidos previamente en cada una de las subredes por parte de los diseñadores, pero si el administrador necesita crear otros o cambiarlos, igual que en el caso anterior lo debe realizar de forma manual.

Hay que recordar que el switch básico capa 3 que se ha diseñado solo se estableció para crear hasta 3 VLAN’s, en las cuales dos de ellas son fijas y una es móvil, puesto que eso es lo que se estableció en el alcance de este tema de tesis.

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Como resultado de este proyecto de tesis se ha logrado implementar un switch básico capa 3, mediante la utilización de dispositivos de red comunes, el cual realiza sus funciones de trabajo, como son administrar y gestionar redes pero de manera lógica, al igual que cualquier otro switch capa 3 comercial.

- La meta final de este proyecto de tesis, es la creación de un switch capa 3 de costos bajos, con el único propósito de que las empresas medianas y pequeñas no se queden rezagadas al acceso de estas tecnologías, so pretexto de su costo comercial, es por eso que se implementó este switch mediante la utilización de sencillos dispositivos de red y la utilización efectiva de varias de la potencialidades del sistema operativo Linux, los cuales se los puede conseguir en cualquier casa comercial relacionadas con este tema.

- Para reducir aún más el valor comercial del switch básico capa 3 se utiliza software cuya licencia es gratuita, pero la labor potencial que este realiza, no lo desacredita en comparación con un switch capa 3 comercial.

- Este prototipo básico de switch esta en la capacidad de crear hasta 3 redes, debido a que físicamente utiliza 3 tarjetas de red, ya que ese fue el alcance propuesto en el proyecto, el sistema en sí, no tiene restricción alguna en esta funcionalidad, a no ser de la capacidad del hardware (número de slots PCI en el mainboard).

- En este proyecto se implementó una interfaz básica de aplicación que permite generar automáticamente los archivos de configuración del servicio DHCP y manejar las reglas del Firewall, de acuerdo a los parámetros que el administrador requiera (ver anexo 1).

- Al realizar un análisis costo beneficio en la creación e implementación de este proyecto, se observa de manera clara que su ahorro es muy aceptable y que de ninguna manera, involucra el menor desempeño del dispositivo en comparación con otro switch capa 3.

- Como función adicional, este proyecto de tesis esta configurado para entregar direcciones IP en forma dinámica para redes de rangos diferentes, es decir, tiene un servidor DHCP multi-scope, cuya técnica permite manejar una VLAN móvil a través de las diferentes interfaces de red.

- Otra función que el switch cuenta es que tiene incorporado un servidor DNS, con el propósito de que el administrador conozca si un computador es parte o no de una subred y a que subred pertenece, ya sea dando un comando ping a su dirección IP o su nombre de PC.

- También se pensó en las políticas de seguridad que deben manejarse entre las subredes, es por eso que el proyecto cuenta con un Firewall básico, mediante el cual el administrador puede conceder o negar servicios a las subredes a través de puertos o protocolos de transporte.

- La definición de los nombres de zonas de servidor DNS están ya establecidas de acuerdo al criterio del diseño de este proyecto, sin opción a que éstas puedan ser alteradas a través del software de aplicación. Sin embargo pueden ser alteradas directamente en los archivos de configuración respectivos.

- Un computador que pertenece a la VLAN móvil podrá trasladarse por cualquier otra VLAN, a este computador siempre se lo identificará por su FQDN sin importar en que red esté conectado físicamente.

4.2 RECOMENDACIONES

- Se recomienda que la instalación de este prototipo de switch básico capa 3, propuesto en este tema de tesis, se la realice con soporte de los diseñadores originales a fin de que los administradores se familiaricen con el sistema y tengan a la vez un asesoramiento técnico del manejo del software de aplicación.

- Debido a que el proyecto de tema de tesis sugerido, como una solución alternativa al excesivo gasto por parte de las empresas, en la compra de un switch capa 3, y todo su contenido esta enfocado en la administración y gestión de redes, se recomienda que la persona (técnico) que esté a cargo de dicha labor, conozca el manejo del Sistema Operativo Linux, conocimientos sólidos de redes TCP/IP y servicios planteados, y si no lo tiene, se debe solicitar un entrenamiento previo para la persona delegada al manejo de éste por parte de los diseñadores del proyecto, para que el sistema funcione a su máxima capacidad.

- Para modificar las zonas de dominio en el Servidor DNS, el administrador lo debe realizar directamente en los diferentes archivos de configuración que administra el DNS, ya que el software de Aplicación no está diseñado para permitir esta funcionalidad.

- El administrador de red en coordinación con las gerencias, son los encargados de realizar políticas informáticas para controlar el acceso de los usuarios a los diferentes servicios que preste cada VLAN.

- En el software de aplicación el administrador debe ingresar los parámetros de configuración de red correctos (máscara de red, broadcast, puerta de enlace, etc) para cada red, ya que de esto depende el correcto funcionamiento del Sistema, puesto que este tiene la capacidad de manejar subneting en cada red.

- Se recomienda que la interfaz de red tenga la primera dirección IP del rango de direcciones IP, la misma que sirve como puerta de enlace con las otras redes, con el fin de facilitar la administración en si de las VLAN`s.

- En el diseño de este Sistema se planteó la posibilidad de utilizar switch convencionales para crear las diferentes redes, se recomienda la utilización de switch debido a que su rendimiento es superior, además que el hub es un hardware con tecnología obsoleta y que incorpora dominios de colisión entre otros.

- Se recomienda la utilización de tarjetas de red de marcas reconocidas, caso contrario puede restar rendimiento en el sistema.

CAPITULO 5

REFERENCIAS BIBLIOGRÁFICAS

5.1 LIBROS

Anónimo. Protocolos de encaminamiento. Biblioteca personal.

Comer D. (1996). Redes Globales de Información con Internet y TCP/IP. México. Prentice Hall.

Jamsa K, y Cope K. (1996). Programación en Internet. McGraw-Hill.

Samaniego G. (2003). Apuntes de Redes de Computadores, Quito.

Taenenbaum A. (1997). Redes de computadoras. México. Prentice Hall.

Anónimo. (2005). Redes Virtuales (vLANs): Un nuevo concepto en Redes Computacionales. http://www.ibw.com.ni/~alanb/tecno/thpage.htm.

5.2 INTERNET

Anónimo. (2005). Redes Locales Virtuales. Microsoft. http://polaris.lcc.uma.es/~eat/services/rvirtual/rvirtual.html.

Anónimo. (2005). Redes TCP/IP. http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-087-2-intro.tcpip.html.

Soto A. (2005). Protocolos TCP/IP. http://usuarios.lycos.es/janjo/janjo1.html.

Moreno L. (2005). Tipos de redes.
http://www.htmlweb.net/redes/topologia/topologia_3.html.
Anónimo. (2005). Tutorial y descripción técnica de TCP/IP.
http://ditec.um.es/laso/docs/tut-tcpip.

Anónimo. (2005). Protocolos de Internet. http://www.zator.com/Internet/A3_7.htm.

Castellanos A. (2002). El servicio DHCP. http://www.linux.cu/maual/avanzado-html/node29.html.

Piquer J. (2005). Nivel de red.
http://www.dcc.uchile.cl/~jpiquer/Docencia/cc51c/apuntes/node5.html.

Dueñas F. (2004). Seguridad y protección en computación. Monografías.com.
http://monografias.com/trabajo6/sepro/sepro.shtml.

Anónimo. (2005). Sistema Operativo Linux. Monografías.com.
http://www.monografias.com/trabajos6/sisop/sisop.shtml.

Kirch O y Dawson T. (2005). Guía de Administración de Redes con Linux.
http://es.tldp.org/Manuales-LuCAS/GARL2/garl-2.0.pdf.

5.3 SOFTWARE

MICROSOFT. Seguridad. Diccionario Encarta® 2005.

ANEXOS

ANEXO N. 1

INTERFAZ DE APLICACIÓN

Las opciones que presenta la Interfaz de Aplicación están ligadas a las principales configuraciones que requiere el prototipo de switch básico capa 3 basado en Linux para su administración.

El objetivo de la aplicación es modificar automáticamente los archivos de configuración de los servicios que presta el switch capa 3, según los parámetros que ingrese el usuario. Estos archivos de configuración son:

a. Servicio DHCPD (Archivo: dhcpd.conf)
b. Servicio FIREWALL: (Archivo: iptables.sh)

La aplicación se ha creado para dar facilidad al usuario Administrador de la red ya que permite controlar el servicio del switch de una manera sencilla y amigable.

El desarrollo de esta aplicación es básico, está estructurado para que trabaje con direcciones de clase C, debido a que esta clase de direcciones están enfocadas a las pequeñas y medianas empresas.

En la primera pantalla muestra una vista global de todas las opciones que brinda la interfaz:

1. **Nueva Configuración.-** Esta opción permite realizar una configuración desde cero iniciando el proceso de ingreso de datos para el archivo dhcpd.conf de las nuevas subredes.

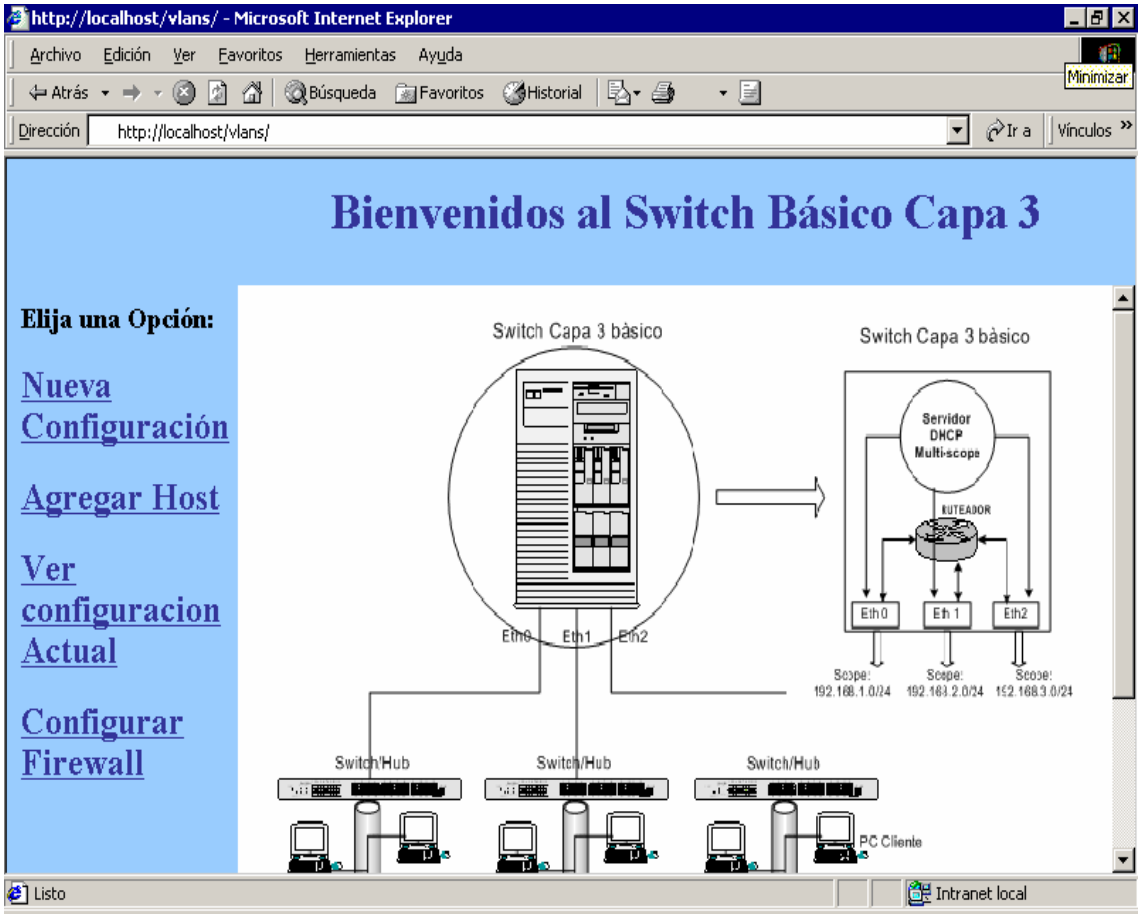
2. **Agregar Host.-** Esta opción es utilizable cuando de antemano ya se tiene hecha la configuración del switch capa 3 y se desea agregar un nuevo Host a la VLAN móvil, a través de su dirección MAC.

3. **Ver configuración Actual.-** En esta opción se despliega una lista con las configuraciones de las tres subredes. No incluye las reglas de Firewall.

4. **Configurar Firewall.-** Como su nombre lo expresa, esta opción permite configurar las opciones para generar el archivo iptables. sh

Gráfico 1

Pantalla Inicial de la Aplicación



Fuente: Interfaz de aplicación

1.- Nueva Configuración

Al ingresar a esta opción, cualquier contenido de los archivos de configuración existentes se borra y empieza nuevamente el ciclo de configuración A continuación una lista con todo el submenú que contiene este punto

a. Vlan1

b. Agregar Host

c. Vlan2

d. Vlan3

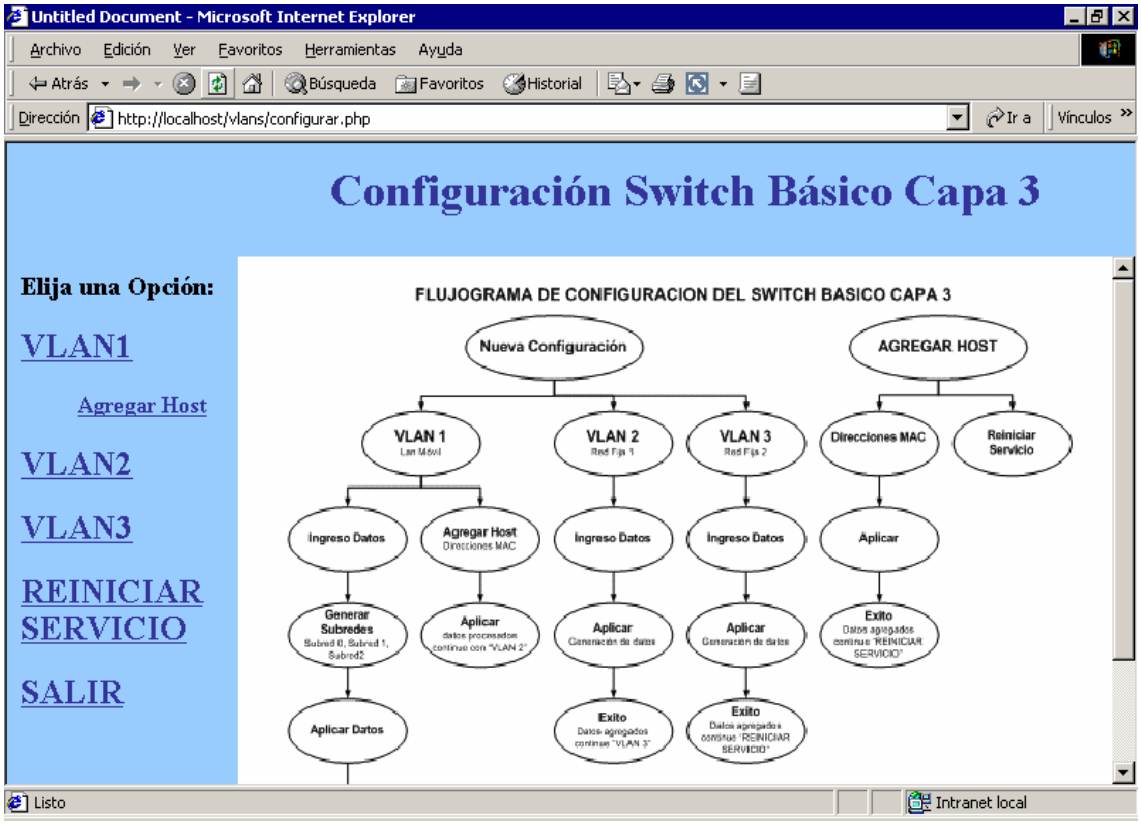
e. Reiniciar el servicio

f. Salir

Cada submenú se explica más adelante.

Gráfico 2

PANTALLA NUEVA CONFIGURACIÓN



Fuente: Interfaz de aplicación

En la parte central existe un flujograma de configuración del switch capa 3, el mismo que ayuda de una manera visual a seguir los pasos para tener una exitosa configuración.

En la parte izquierda la lista de las diferentes opciones, las mismas que se detallan a continuación:

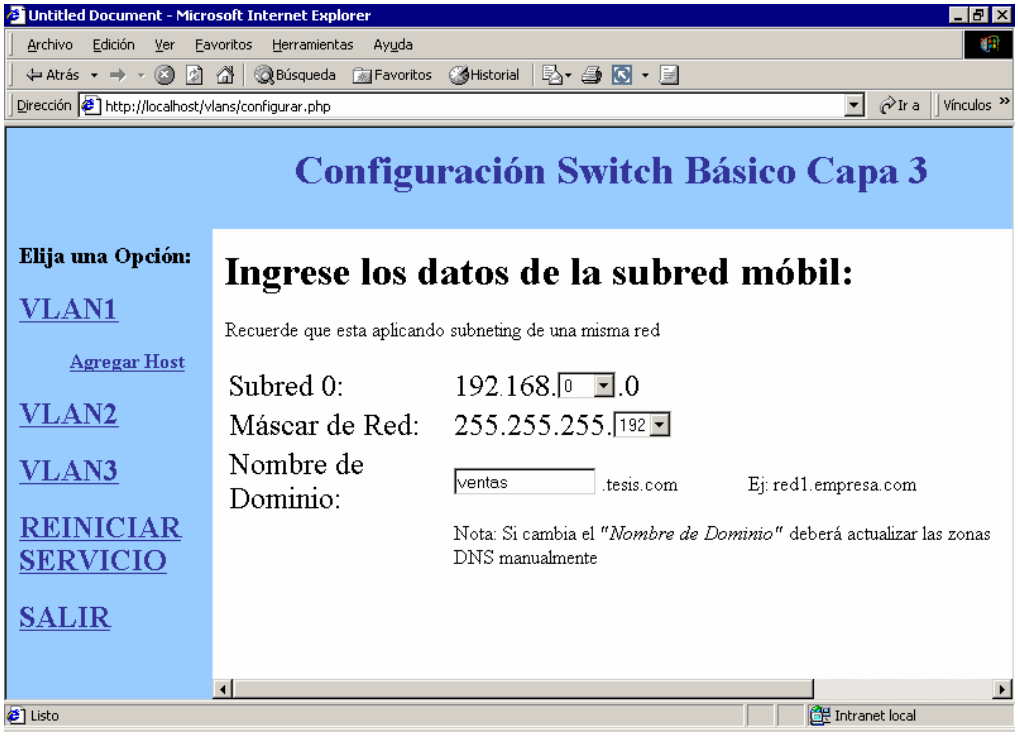
a. VLAN1

La pantalla que se refiere a la VLAN1 está asociada directamente con la VLAN móvil, razón por la cual requiere datos de las tres subredes en forma de subneting. Estas subredes pertenecen a la VLAN Móvil.

Es muy importante tomar en cuenta que si cambia la zona de configuración del DNS, debe cambiar directamente las zonas en código fuente como parte de la configuración de un servidor DNS

La dirección de red escogida como estándar de configuración es la 192.168.x.x, debido a que pertenece a un grupo de direcciones IP privadas y es de clase C.

Gráfico 3
PANTALLA DE CONFIGURACIÓN DE LA VLAN1

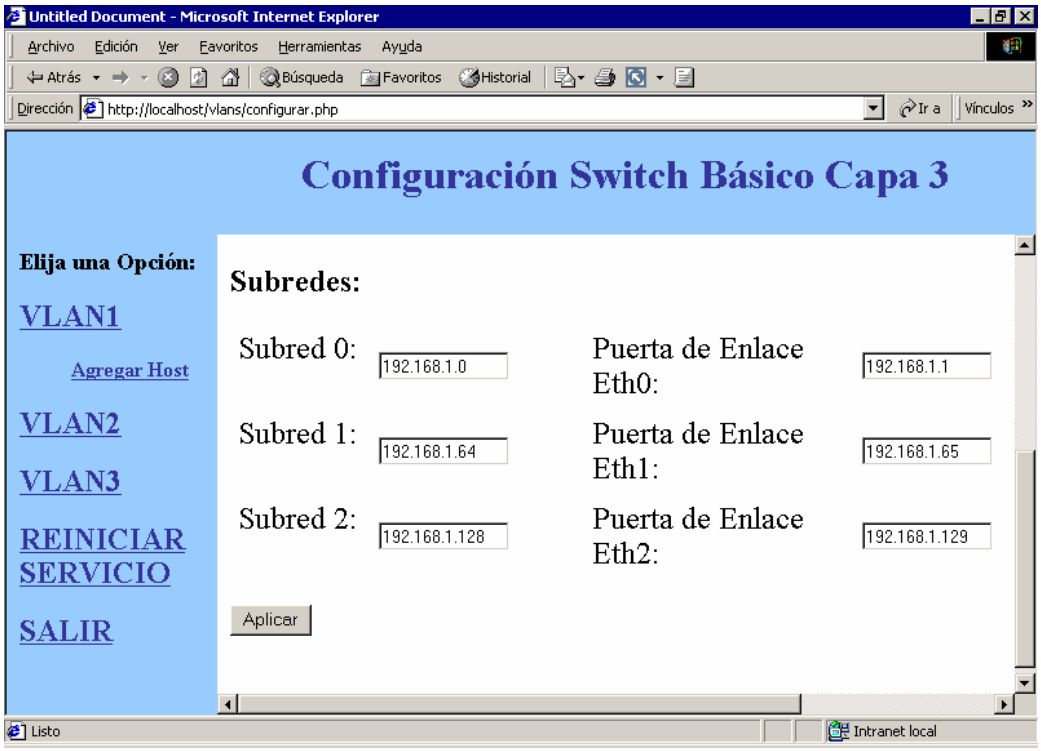


Fuente: Interfaz de aplicación

Los datos que se ingresan en esta pantalla son los parámetros básicos de configuración de red.

En la siguiente pantalla, la interfaz de aplicación genera automáticamente las tres subredes, y muestra al usuario Administrador los datos de configuración de red que pertenecen a la VLAN1 (o móvil)

Gráfico 4
GENERACIÓN DE SUBREDES DE LA VLAN1

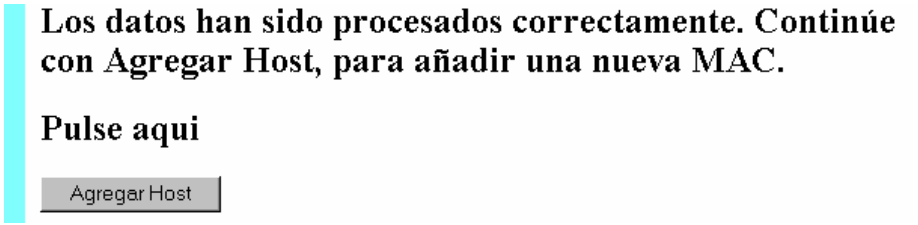


Fuente: Interfaz de aplicación

En el instante de Aplicar las configuraciones, la aplicación procesa estos datos y si los campos están correctos emite un mensaje al Usuario:

Gráfico 5

MENSAJE EXITOSO DE LA CONFIGURACIÓN DE LA VLAN1



Fuente: Interfaz de aplicación

b. Añadir un nuevo host

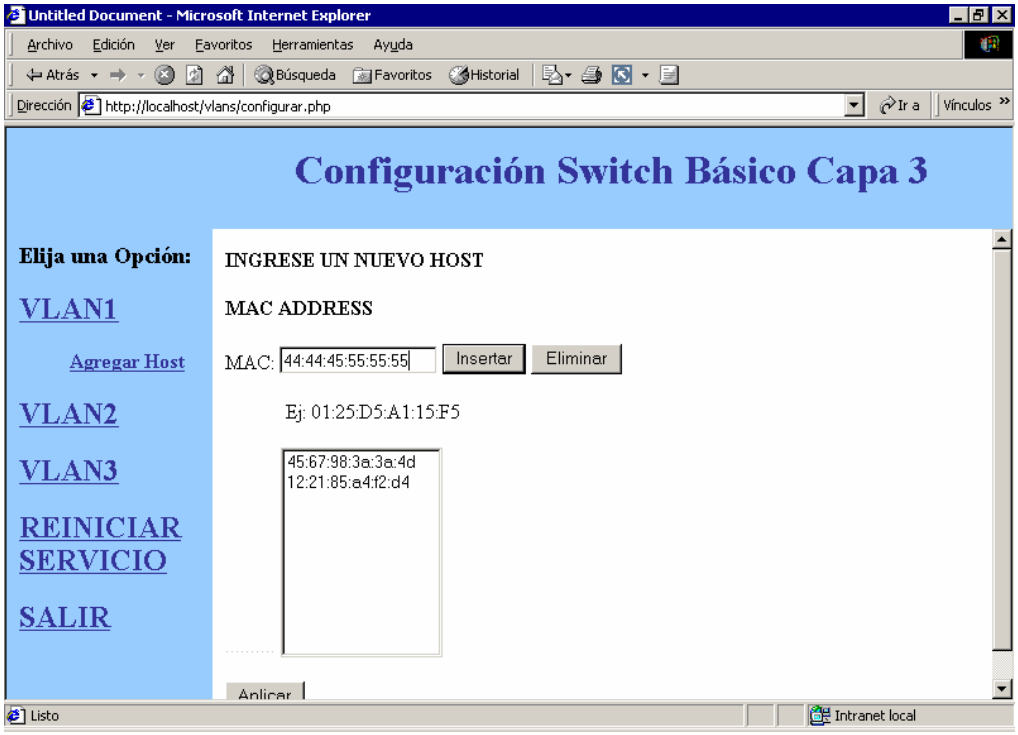
En esta pantalla se tiene un control de los Host que pertenecen a la VLAN móvil a través de la dirección MAC.

Existe un listado de las direcciones MAC que se encuentran configuradas en ese momento y para dar flexibilidad, la aplicación ofrece las opciones de insertar o eliminar un ítem de esta lista.

Vale indicar que todas estas configuraciones primero se almacenan en archivos de tipo xml, los mismos que funcionan como contenedor de datos, para de una manera posterior extraer nuevamente estos datos e imprimirlos en el archivo de configuración.

Gráfico 6

Ingresar host por medio de la MAC



Fuente: Interfaz de aplicación

Una vez realizado este procedimiento, seleccionar Aplicar y como se procedió en el caso anterior, la aplicación genera un mensaje de éxito.

c. VLAN 2

La siguiente pantalla recoge todos los parámetros necesarios para la configuración de red de la VLAN2 y se aplica el mismo concepto que la VLAN1 móvil, es decir ésta plantilla se basa en direcciones de clase C

Gráfico 7

GENERACIÓN DE SUBREDES DE LA VLAN2

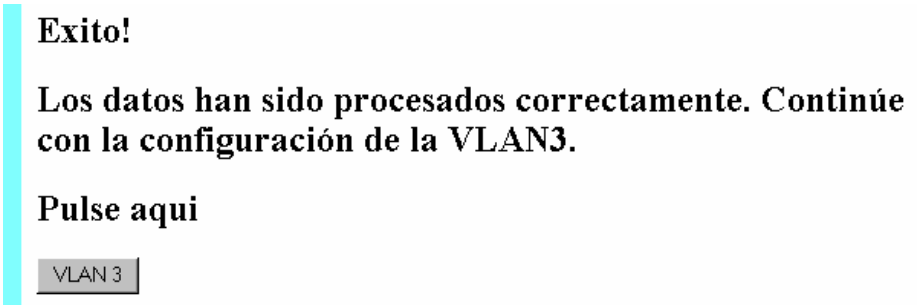
Fuente: Interfaz de aplicación

La pantalla de configuración de la VLAN3 es muy similar a la VLAN2, razón por la cual no se incluye una explicación respecto a la VLAN3.

Una vez realizadas las configuraciones y si no existe algún problema, la aplicación genera un mensaje de éxito.

Gráfico 8

MENSAJE EXITOSO DE LA CONFIGURACIÓN DE LA VLAN1



Fuente: Interfaz de aplicación

d. Reiniciar el Servicio

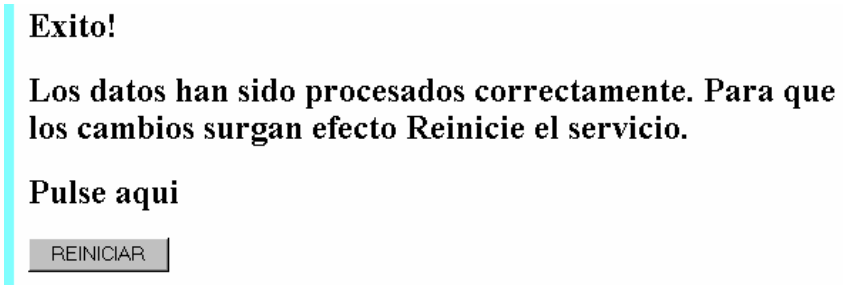
Cuando ha culminado el ingreso de datos de las tres subredes en los formularios es necesario reiniciar el servicio para que todos los cambios surjan efecto.

Reiniciar el Servicio consiste en reiniciar el servicio dhcp, dns iptables, leyendo de los archivos de configuración que se generaron anteriormente.

A continuación se muestra la pantalla que indica que la operación ha surgido con éxito.

Gráfico 9

MENSAJE EXITOSO DE LA CONFIGURACIÓN DE LA VLAN1

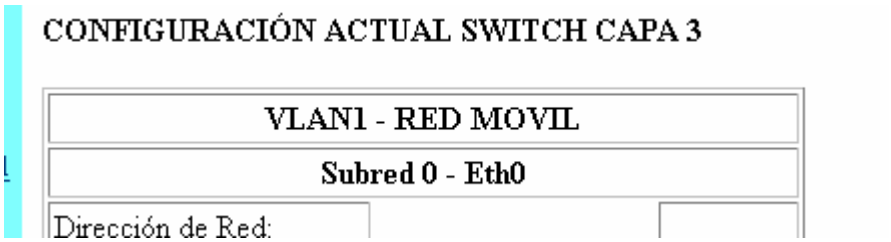


Fuente: Interfaz de aplicación

3. Ver configuración actual

Esta opción permite ver de una manera ordenada, los parámetros de configuración de red de la VLAN1 (móvil), VLAN2 y VLAN3 que se encuentra en ese momento funcionando, facilitando así una visión general del Administrador.

Gráfico 10
VER LA CONFIGURACIÓN ACTUAL DEL SWITCH CAPA 3



Fuente: Interfaz de aplicación

4. Configurar Firewall

La aplicación maneja la configuración del Firewall, presentando una lista de las reglas que se encuentran configuradas, además que da la posibilidad de agregar o quitar una regla.

Una vez configurada estas reglas a través de la interfase de aplicación, se genera automáticamente el archivo de IPTABLES, según los requerimientos del usuario.

A continuación se muestra la pantalla de inicio de la Configuración de Firewall, la misma genera una tabla dinámicamente de las reglas que está almacenadas en un archivo xml. Los campos que posee la tabla son los esenciales para crear una regla de seguridad:

- Origen (host específico o red)
- Destino (host específico o red)
- Servicio (los principales http, ftp, telnet, https, etc.)

- Puerto (según el servicio ingresado)
- Acción (Aceptar o Negar)

Gráfico 11

CONFIGURACIÓN REGLAS DEL FIREWALL

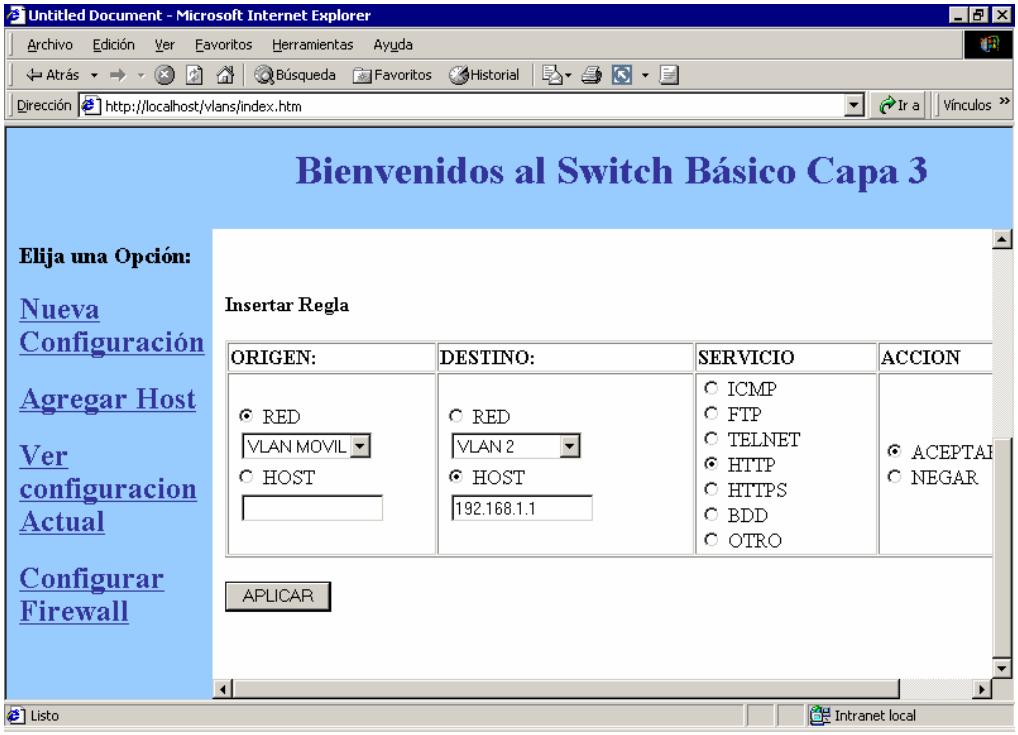
Fuente: Interfaz de aplicación

a. Añadir una Regla en el Firewall

Al insertar / eliminar una regla, la aplicación presenta una interfaz que permite realizar esta acción sin complejidad, ya que se ha desarrollado una aplicación básica.

Gráfico 12

INSERTAR UNA REGLA EN EL FIREWALL



Fuente: Interfaz de aplicación

La interfaz de aplicación que se ha desarrollado es muy intuitiva para el Administrador de la Red, a la vez que es básica y posee sólo las opciones necesarias para configurar e iniciar el servicio del switch capa 3 básico.

Si el Administrador desea realizar una configuración extra posee la opción de dirigirse directamente al código fuente y modificar, ya que en este caso no existe ningún tipo de limitaciones respecto al tema.