VIABILIDAD DEL USO DEL PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST (DHCP) PARA LA RED DE DATOS DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

JOSE MIGUEL AGUILERA GIL
ANGÉLICA MARÍA ANAYA CALA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2005

VIABILIDAD DEL USO DEL PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST (DHCP) PARA LA RED DE DATOS DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER

JOSE MIGUEL AGUILERA GIL
ANGÉLICA MARÍA ANAYA CALA

Este proyecto es presentado como requisito para optar al título de Ingeniero Electrónico

Director
PhD. OSCAR GUALDRÓN GONZÁLEZ
Codirector
ING. BENJAMÍN PICO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FÍSICO-MECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2005

AGRADECIMIENTOS

Los autores expresan su agradecimiento y reconocimiento a :

Nuestras familias por su apoyo incondicional.

Doctor Oscar Gualdrón González, director del proyecto por su valiosa orientación y colaboración.

Ingeniero Benjamín Pico, codirector del proyecto y a la División de Servicios de Información, por su excelente disposición al prestarnos su colaboración.

Los integrantes del Grupo de Investigación en Conectividad y Procesado de Señal – CPS, por su colaboración durante la realización de las pruebas.

La Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones.

La Universidad Industrial de Santander.

A Dios por las oportunidades que me ha brindado cada día.
A mis padres, Alfonso y Zoraida por su amor y apoyo incondicional.
A mi hermana Laura, porque a pesar de la distancia siempre está a mi lado.
A José por su compañía y su amor.
A Jose Miel.
A mis amigos por los buenos momentos.
Angélica María

A Dios por iluminarme y fortalecerme todos los días de mi vida.
A mi madre María Angélica por su total amor y comprensión.
A mi padre José Ignacio, por enseñarme a vivir tempranamente.
A mis hermanos Nidia, Pedro y Henry por su cariño y apoyo incondicional.
A mi sobrino Steven por inspirarme en situaciones difíciles.
A Mayerli por su amor y paciencia en todo este tiempo.
A Pocahontas.
A mis amigos por los momentos compartidos.
José Miguel

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

TÍTULO: VIABILIDAD DEL USO DEL PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST (DHCP) EN LA RED DE DATOS DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER*

AUTORES: JOSE MIGUEL AGUILERA GIL
ANGELICA MARÍA ANAYA CALA **

PALABRAS CLAVES: cliente DHCP, servidor DHCP, agente relay

DESCRIPCIÓN

Actualmente todas las estaciones de la red de datos de la UIS están configuradas estáticamente, el proceso de gestión de direcciones IP no es el más adecuado, se presentan conflictos de suplantación, cualquier usuario puede hacer uso de la red, no se garantiza la movilidad para equipos portátiles y no existe un registro actualizado de los hosts que están conectados a la red. Con este proyecto se determinó la viabilidad de implementar DHCP y se plantearon las políticas de administración, gestión y control que contribuirán a mejorar la labor de administración de la red.

Se estableció que la infraestructura de red ofrece un buen nivel de soporte para el servicio, y con las pruebas de tráfico ejecutadas, se concluyó que las transacciones generadas por DHCP no tendrán impacto significativo en el funcionamiento de la red y que es suficiente utilizar un servidor y un agente relay, configurado en el switch central; sin embargo serán clientes DHCP las estaciones de la sede principal y del área metropolitana, las sedes regionales mantendrán la configuración estática.

La asignación y administración de direcciones se realizará desde un servidor DHCP centralizado utilizando la asignación manual, lo cual permitirá ejercer un mayor control sobre las estaciones, mantener un inventario actualizado de las mismas, efectuar un crecimiento controlado, restringir el uso de la red a usuarios registrados, flexibilizar cambios a la configuración de red, implementar políticas y ofrecer movilidad a dispositivos móviles. El proyecto representa una solución integral soportada en la optimización de recursos y el trabajo en equipo.

* Trabajo de grado
** Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones
Director: PhD. Oscar Gualdrón González

TITLE: POSSIBILITY OF USAGE OF THE DYNAMICS CONFIGURATION HOST PROTOCOL (DHCP) IN THE UNIVERSIDAD INDUSTRIAL DE SANTANDER DATA BASE*

AUTHORS: JOSE MIGUEL AGUILERA GIL
ANGELICA MARÍA ANAYA CALA **

KEY WORDS: Relay Agent, DHCP client, DHCP server

DESCRIPTION

Currently, all the UIS database stations are configured staticly, the IP process is not quite appropriate, there are impersonation conflicts, any user can use the network, the movility for portable equipment is not guaranteed, and there is not a current record of the hosts that are connected to the net. With this proyect, the possibility to implement DHCP is determined and the administration policies were planned , this procedure and its control will contribute to improve the database administration job.

It is established that the network's foundation offers a good service support, and with the traffic samples executed, it is concluded that the transactions generated by DHCP will not have any meaningful impact in how the net is working and it is enough to use a server and a relay agent; nevertheless the stations of the headquarters y and the metropolitan area will be DHCP clients, the regional stations will keep the static configuration.

The assignment and administration of addresses will be made from a centralized DHCP server using the manual assignment, which will allow it to obtain a bigger control over the stations, to keep a current inventory of these addresses, to carry out a controlled increasemet, to restrict the net usage to just registered users, to be flexible with changes when configuring the database, to implement policies, and to offer movility to portable devices. This project represents a total solution which is supported by the resources improvement and teamwork.

*Graduation work
**Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones
Director Phd. Oscar Gualdrón González

INTRODUCCIÓN

Dentro de una red de datos existen identificadores con los que se reconoce cada dispositivo, sea activo o pasivo, que facilitan el intercambio de paquetes entre las distintas entidades; las direcciones IP desarrollan dicho papel de una manera sencilla y universal que permite la comunicación entre equipos de diversos fabricantes los cuales pueden utilizar diferentes tecnologías y sistemas operativos.

La Red de datos de la Universidad Industrial de Santander está conformada actualmente por cerca de 2000 estaciones de trabajo, agrupadas en 80 subredes que incluyen indistintamente dependencias, sedes, escuelas y departamentos, las cuales presentan condiciones cambiantes que complican la labor de administración de direcciones y pueden vulnerar la seguridad de la red. Ello hace necesario adoptar mecanismos que contribuyan a mejorar las políticas de gestión.

Para adelantar dicha tarea, se evalúa el uso del Protocolo de Configuración Dinámica de Host (DHCP), el cual asigna automáticamente información TCP/IP a equipos cliente. Cada cliente DHCP se conecta a un servidor DHCP el cual suministra la configuración de red del cliente, incluida la dirección IP, la máscara de subred, el gateway y los servidores DNS, entre otros.

El estudio realizado permitirá identificar los requerimientos para implementar DHCP en la red de datos de la Universidad, así como los múltiples beneficios que traerá consigo este servicio.

Además, la viabilidad de la implementación se fundamentará en la estimación del impacto de dicho servicio en el tráfico de la red, así como en la efectividad del proceso de configuración y el nivel de soporte del protocolo que presenta la estructura actual de la red de datos institucional.

El producto final de este proyecto constituye un gran aporte investigativo del Grupo de Investigación en Conectividad y Procesado de Señal al mejoramiento de uno de los recursos más útiles que proporciona la Institución a la comunidad universitaria, para lo cual se contó con la colaboración de la División de Servicios de Información.

1. PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST (DHCP)

1.1 GENERALIDADES DEL PROTOCOLO

El Protocolo de Configuración Dinámica de Host (DHCP[1]) es un protocolo de red construido sobre el modelo cliente-servidor para asignar automáticamente información TCP/IP a equipos cliente. Cada cliente DHCP se conecta a un servidor DHCP centralizado, el cual suministra la configuración de red del cliente.

DHCP es considerado como la versión mejorada de BOOTP[2] (BOOTstrap Protocol), el cual asigna direcciones IP a partir de una tabla que contiene una correspondencia entre estas direcciones y las direcciones físicas de los clientes. Dicha tabla necesita ser creada manualmente por el administrador de red en el servidor de BOOTP.

A pesar de que DHCP es un protocolo diseñado para superar las carencias de BOOTP, mantiene el mismo formato de mensaje y también necesita la implementación de un Agente DHCP Relay[3] dentro de la LAN, el cual permite el intercambio de mensajes entre cliente y servidor cuando éstos se encuentran ubicados en diferentes segmentos de red, evitando así la implementación de un servidor DHCP para cada subred.

El DHC Working Group[4] planteó la posibilidad de que las configuraciones dadas por el servidor al cliente, incluyeran no sólo la asignación de una dirección de red, sino también la transmisión de otros parámetros, tales

[1] En adelante se nombrará al Protocolo de Configuración Dinámica de Host como DHCP.

[2] Para mayor información sobre BOOTP, referirse al RFC 951.

[3] Puede encontrar más información en el capítulo 2, sección 2.4.3.

[4] DHC WG, Grupo perteneciente al Internet Engineering Task Force (IETF). Es el encargado de diseñar las especificaciones de DHCP en el RFC 2131 y el RFC 2132. Mayor información en http://www.dhcp.org

como la máscara de subred, el servidor DNS[5] y la puerta de enlace. Además, este grupo de trabajo también sugirió el mejoramiento de varias limitaciones presentes en el diseño inicial de DHCP. Entre estas mejoras se destacan:

- Realizar el diseño de DHCP como un mecanismo a través del cual los administradores de red pudieran implementar políticas de administración en la red.
- Usar DHCP para proporcionar una dirección de red y otros parámetros de configuración a cada cliente.
- Limitar el alcance de DHCP para configuración de hosts TCP/IP.
- Evitar la necesidad de implementar un servidor en cada segmento de red.
- Usar uno o varios servidores centralizados.
- Garantizar la coexistencia de DHCP con configuraciones estáticas en host no participantes de la implementación del servicio.

Para desarrollar sus funciones, un servidor DHCP puede identificar a cada cliente a través de dos formas fundamentales:

- Por medio de la dirección MAC (Media Access Control) de la tarjeta de red del cliente, o
- A través de un identificador que le indique el cliente.

El identificador seleccionado por el cliente DHCP debe ser único dentro de la subred a la cual él está conectado. Si el cliente usa un determinado identificador en un mensaje, éste también debe ser usado en los mensajes

[5] DNS: Domain Name System.

subsecuentes de la transacción para asegurar que todos los servidores lo identifiquen correctamente.

Basándose en la forma de identificación del cliente, DHCP soporta tres mecanismos para la asignación de direcciones:

- **Asignación automática**: en la cual el servidor DHCP selecciona una dirección IP que esté disponible y la asigna permanentemente al cliente.

- **Asignación dinámica**: el servidor DHCP asigna una dirección IP a un cliente durante un tiempo limitado o hasta que ésta sea liberada por el cliente.

- **Asignación Manual**: Una dirección IP que haya sido configurada manualmente en el servidor es permanentemente asignada al cliente por medio de la identificación de su dirección MAC.

El mecanismo de asignación dinámica es una gran ventaja que presenta DHCP sobre BOOTP, ya que éste permite reutilizar las direcciones que no están siendo usadas por los clientes a los cuales ya les habían sido asignado determinadas IPs, por lo tanto este mecanismo se considera útil en casos como en los que un cliente solicite una dirección por un período de tiempo reducido o para poder compartir un grupo limitado de direcciones IP entre una cantidad mayor de clientes.

Y aunque la idea central del servicio DHCP es la dinamicidad de las direcciones IP asignadas, no se excluye la posibilidad de utilizar direcciones fijas para algunos hosts que por sus características lo requieran, ejemplo de ello son las máquinas proveedoras de servicios como el correo electrónico o el DNS. Este tipo de host podría utilizar las ventajas del servicio para obtener el resto de los datos que se pueden proveer mediante DHCP.

1.2 OPERACIÓN DE DHCP

La forma en que un cliente DHCP obtiene su configuración de red es bastante sencilla, ya que generalmente este proceso se hace por medio del intercambio de 4 mensajes entre el cliente y el servidor.

Si el cliente que desea hacer uso del servicio DHCP por primera vez se encuentra en el mismo segmento de red donde está ubicado el servidor, y éste posee la información necesaria para que los clientes que accedan a él puedan adquirir su configuración de red, el proceso inicia cuando el cliente contacta el servidor para obtener su dirección IP y demás parámetros, para lo cual envía un mensaje (DHCP Discover) en broadcast en búsqueda de los servidores DHCP disponibles en ese momento. Al recibir este mensaje, los servidores responden al cliente con un mensaje (DHCP Offer), enviado en unicast, con el que se identifican como servidores DHCP y ofrecen la configuración de red seleccionada para el cliente; dicha configuración debe ser asignada de acuerdo al segmento de red en el que se encuentra el cliente.

Una vez el cliente ha recibido las propuestas de los servidores, envía un mensaje en broadcast (DHCP Request) donde solicita los parámetros de configuración ofrecidos por un servidor y rechaza las otras ofertas. Al recibir dicho mensaje, una vez se confirma que la dirección IP aún está disponible[6] y que los otros parámetros ofrecidos son los apropiados, el servidor envía al cliente sus parámetros de configuración en el último mensaje de la transacción (DHCP ACK[7]), el cual va también direccionado en unicast; además el servidor también almacena la dirección asignada, para evitar que sea concedida posteriormente a otro cliente.

---

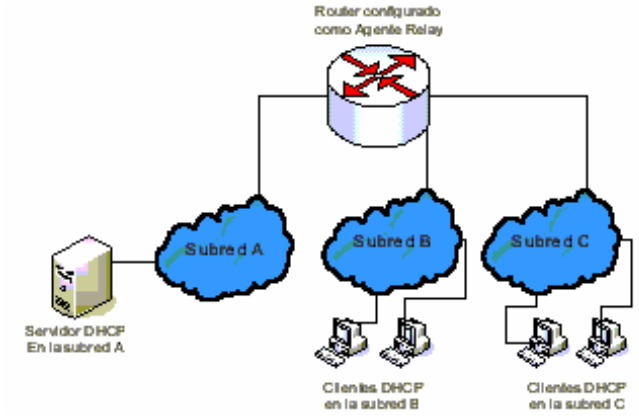
[6] Para hacer esta confirmación, el servidor envía mensajes ICMP Echo Request a las direcciones IP definidas en sus rangos de asignación, si no recibe ningún ICMP Echo Reply, asume que ésta aún es válida y la asigna al cliente.

[7] Después de recibir el mensaje de finalización de la transacción o DHCP ACK, el cliente realiza otra verificación de la disponibilidad de la dirección IP que le ha sido asignada; para esto, envía un mensaje ARP a las estaciones de su misma subred, si alguna de éstas responde, el cliente envía al servidor un mensaje DHCP Decline.

Si después de esto, el cliente es movido a cualquier otra subred dentro de la misma LAN mientras se encontraba apagado, cuando se encienda, contactará nuevamente al servidor con un mensaje (DHCP Request) para verificar si la dirección que le había asignado aún es válida; en respuesta, el servidor establece con la intervención y soporte del agente DHCP relay que la dirección adjunta al mensaje es inapropiada para el segmento de red en el que se encuentra el cliente, por lo tanto, le envía un mensaje denegando el uso de la dirección antigua (DHCP NACK). Posteriormente, el cliente descarta esta dirección e inicia nuevamente el proceso.

Si un cliente nuevo es incorporado en un segmento de red diferente al que contiene el servidor DHCP, resulta indispensable la presencia de un agente relay para que se lleve a cabo el intercambio de mensajes entre el servidor y los clientes. La anterior situación se representa en la figura 1, donde múltiples segmentos de red se encuentran conectados a un mismo router.

Figura 1. Implementación de un switch-router como agente relay en una LAN.



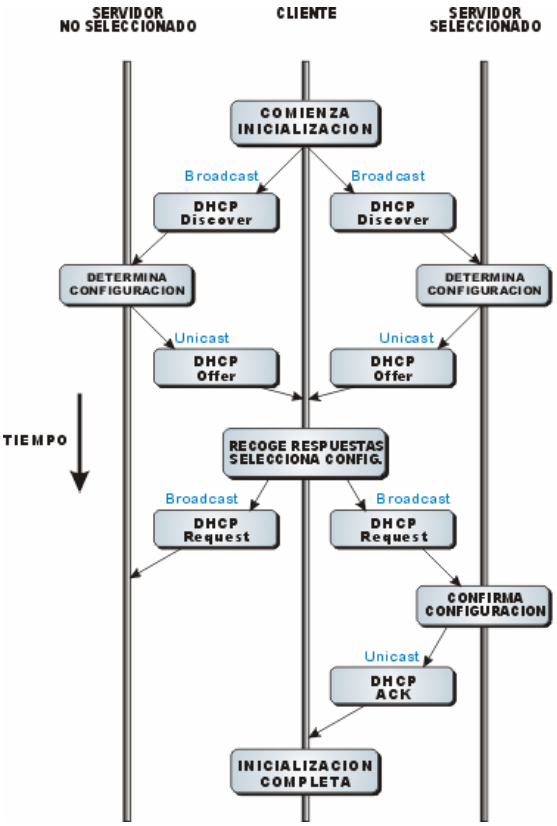
Fuente: Los autores

Cuando el agente relay recibe un mensaje que ha sido enviado por el cliente (broadcast), almacena la dirección de la interfaz de red a través de la cual el mensaje se recibió. El agente relay entonces, redirecciona en unicast

dicho mensaje hacia el servidor DHCP y de esta misma manera, el servidor envía su respuesta a la dirección de red del agente relay, el cual lo reenvía hacia el segmento de red en el que se encuentra el cliente.

La figura 2 sintetiza el proceso descrito anteriormente donde ocurre el intercambio de mensajes entre el cliente y el servidor, de esta manera se presentan las líneas de tiempo para cuando existe más de un servidor activo en la red.

Figura 2. Diagrama de tiempos para el intercambio de mensajes entre el cliente y servidores DHCP.



Fuente: RFC 2131

La información otorgada por el servidor se mantiene asociada al cliente mientras éste no desactive su interfaz de red (posiblemente porque se

apague el equipo) o no expire el tiempo del contrato o lease time[8]. Una vez vencido el plazo del contrato el servidor puede renovar la información del cliente, fundamentalmente su dirección IP, y asignarle otra nueva o extender el plazo, manteniendo la misma información. Cada vez que el cliente solicite renovar sus parámetros de configuración de red, el servidor en lo posible le asignará la misma dirección IP.

1.3 MENSAJES DHCP

El intercambio de información entre cliente y servidor utiliza UDP[9] como protocolo de transporte, donde los mensajes DHCP desde el cliente hacia el servidor son enviados al puerto 67 del servidor y los del servidor hacia el cliente son enviados al puerto 68 del cliente DHCP.

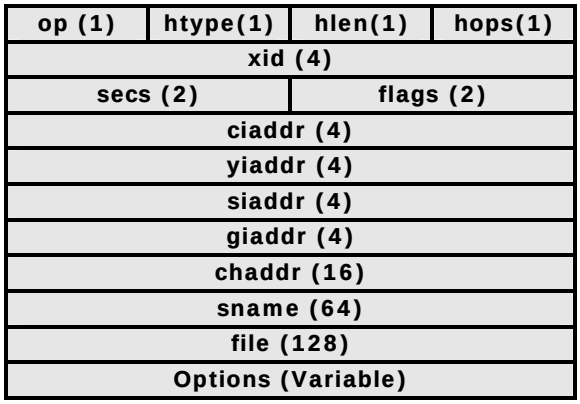
1.3.1 Formato de los mensajes DHCP.

Debido a la relación entre BOOTP y DHCP, estos dos protocolos presentan gran similitud en el formato de sus mensajes, permitiendo interoperabilidad de clientes BOOTP existentes con servidores DHCP sin requerir cambios en la inicialización del software del cliente.

La figura 3 presenta el formato de los mensajes DHCP en el que cada uno de los campos permite identificar los parámetros de las entidades involucradas en cada instante del proceso; los valores entre paréntesis representan el tamaño de los campos, los cuales son expresados en bytes.

[8] El lease time es el periodo de tiempo durante el cual el cliente ha sido autorizado para mantener asociada su configuración de red.
[9] UDP, Protocolo de Datagramas de Usuario

Figura 3. Formato de un mensaje DHCP.



Fuente: RFC 2131

La descripción detallada de cada uno de los campos del formato de mensaje se presenta en la tabla 1.

Tabla 1. Campos de un mensaje DHCP.

CAMPO	DESCRIPCION
op	Tipo de mensaje (1:REQUEST, 2:REPLY).
htype	Tipo de dirección de hardware (ethernet).
hlen	Longitud en bytes de la dirección hardware. Ethernet y Token Ring usan 6.
hops	El cliente lo pone a 0. Cada router que retransmite la solicitud a un servidor lo incrementa en 1.
xid	Número aleatorio elegido por el cliente para asociar mensajes y respuestas.
secs	Utilizado por el cliente. Segundos desde que el cliente comenzó el proceso.
flags	El bit más significativo de este campo se usa como flag de broadcast. Todos los demás bits deben estar en 0; están reservados para usos futuros.
ciaddr	Dirección IP del cliente. Fijada por el cliente, o bien es su dirección IP real al iniciar el proceso de solicitud (0.0.0.0)
yiaddr	Dirección IP Fijada por el servidor si el valor del campo anterior es 0.0.0.0
siaddr	Server IP address, Fijada por el servidor en mensajes DHCPOFFER y DHCPACK.
giaddr	Dirección IP del agente relay.
chaddr	Dirección de harware del cliente. Fijada por el cliente y usada por el servidor para identificar cuál de los clientes registrados está arrancando.
sname	Nombre de host del servidor opcional. Cadena terminada con un nulo (00).

file	El cliente puede dejar este campo vacío o especificar un nombre genérico, indicando el tipo de archivo de arranque a usar. En la solicitud de DHCPDISCOVER se pone al valor nulo. El servidor devuelve la ruta de acceso completa del archivo en una respuesta DHCPOFFER.
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.

Fuente: RFC 2131

El campo options es de longitud variable y depende de los parámetros de configuración que el cliente pueda solicitar, además especifica detalles importantes del cliente o del servidor en cada parte del proceso; también les puede proporcionar el resto de información a los clientes para que obtengan su completa configuración de red, la cual les permite interactuar entre ellos y lograr el acceso a la red. Actualmente, las especificaciones de DHCP definen cerca de 80 opciones que pueden ir adjuntas a los diferentes mensajes. Para una descripción más detallada del funcionamiento y las opciones de DHCP se recomienda referirse a los RFC[10] 2131 y 2132.

1.3.2 Tipos de mensajes DHCP.

Los tipos de mensajes de las transacciones también se definen en el campo de opción *Tipo de mensaje* (DHCP Message Type). La tabla 2 lista los diferentes tipos de mensajes DHCP y sus funciones, así como la forma en que éstos son direccionados por sus emisores.

Tabla 2. Tipos de mensajes DHCP.

Tipo de Mensaje	Entidad que lo envía	Acción	Modo de Direccionamiento
DHCP Discover	Cliente	Intenta encontrar servidores DHCP.	Broadcast
DHCP Offer	Servidor	Ofrece propuestas de configuración a los clientes.	Unicast

[10] RFC, Request for comments.

DHCP Request	Cliente	Acepta la oferta de un servidor y rechaza las otras. Confirma la validez de la información asignada antes del reinicio del sistema. Extiende el contrato de una dirección IP determinada.	Broadcast
DHCP ACK	Servidor	Graba la configuración asignada excluyendo la dirección IP que ya fue aceptada. Confirma parámetros.	Unicast
DHCP NACK	Servidor	No confirma pues la dirección aceptada es incorrecta (por ejemplo, cuando el cliente cambia de subred) o que el contrato ha expirado.	Unicast
DHCP Decline	Cliente	Informa que la dirección confirmada está siendo usada.	Unicast
DHCP Release	Cliente	Renuncia a la dirección otorgada y cancela lo que queda del contrato.	Unicast
DHCP Inform	Cliente	Solicita ciertos parámetros de su configuración, excluyendo la dirección IP que ya tiene asignada.	Unicast / Brodacast

Fuente: RFC 2131

1.4 TRABAJOS RELACIONADOS

Actualmente son muchas las empresas y entidades educativas que han optado por implementar el servicio de DHCP en sus redes de datos, logrando así un buen funcionamiento de la red, gracias al alto desempeño del servidor y del servicio en general.

En Bucaramanga, son varias las universidades que cuentan con el servicio de DHCP para ofrecer configuración dinámica a sus hosts TCP/IP. La Universidad Autónoma de Bucaramanga (UNAB) es una de ellas; en esta universidad las 3 sedes locales están interconectadas, agrupando las cerca de 1300 estaciones con las que cuenta actualmente, en 4 VLANs[11]. El servidor DHCP que se tiene en uso es Windows Server 2000 y no cuentan

[11] VLAN, Virtual LAN.

con servidores redundantes. En su configuración se definió un ámbito[12] para cada VLAN, donde cada uno posee características particulares que se acomodan a las necesidades de los usuarios. El dispositivo configurado como agente relay, es un switch **3Com 4900**.

Un alto porcentaje de universidades tienen implementado el servicio de DHCP en las redes de datos institucionales; en todos los casos consultados, las observaciones que se hicieron estuvieron a favor del servicio, ya que en estos campus nunca se han presentado conflictos ocasionados por el servicio.

1.5 TRABAJOS REPRESENTATIVOS

A continuación se presentan algunos de los trabajos más representativos desarrollados en torno al estudio e implementación del servicio DHCP.

Sistema seguro de DHCP con autenticación de usuario. KOMORI y SAITO presentan un esquema de autenticación de usuario y control de acceso donde se asignan los parámetros de configuración sólo a usuarios legítimos sin limitarse a un host específico; éstos se registran con un identificador y un password, mejorando aspectos de la autenticación por MAC como la flexibilidad y la detección de direcciones IP y MAC falsas. Aunque no requiere dispositivos especiales, su implementación hace necesario instalar aplicaciones desarrolladas en Java y en C tanto en el cliente como en el servidor, lo cual representa un retardo en el proceso de configuración del cliente. -KOMORI, Tadashi; SAITO, Takamichi. " The Secure DHCP System with User Authentication", Tokio University of Science, 2002

DHCP para redes móviles con TCP/IP. PERKINS y JAGANNADH estudiaron la interacción entre DHCP e IP-móvil para proporcionar

[12]Un ámbito es el intervalo consecutivo completo de las direcciones IP posibles de una red. Normalmente los ámbitos definen una subred física de la red a la que se ofrecen los servicios DHCP.

portabilidad y movilidad a usuarios de nuevos sistemas inalámbricos. PERKINS, Charles E; JAGANNADH, Tangirala. "DHCP for Mobile Networking with TCP/IP", IBM, T.J. Watson Research Center, 1995.

DHCP para IPv6. PERKINS y BOUND presentan a DHCPv6 como la configuración ofrecida para IPv6, al compararlo con DHCPv4, se destaca que se pueden asignar múltiples direcciones por interfaz de usuario, además hay una reducción significativa del tráfico debido a que los mensajes generados por el cliente no son broadcast sino multicast y el cliente puede solicitar reconfiguración. Sin embargo, igual que DHCPv4 es necesario el agente relay para intercambiar transacciones entre clientes y servidor ubicados en diferentes subredes. -PERKINS, Charles E.; BOUND, Jim. "DHCP for IPv6", Sun Microsystems, Inc.

Desarrollos actuales del DHC WG. Se está trabajando en el rediseño del formato de opciones de DHCP que permita realizar nuevas funciones como mecanismos de autenticación para mejorar la integridad del intercambio de mensajes. Así mismo, se está diseñando un protocolo que permita que múltiples servidores DHCP ubicados en una misma LAN, puedan intercambiar información sobre direcciones asignadas a clientes y la formalización de la interacción que permita la negociación de registros entre clientes y servidores con DNS. Además se continúa con DHCPv6, la versión para IPv6, pues aunque éste incluye mecanismos con los que los dispositivos pueden autoconfigurarse, es necesario centralizar la configuración automatizada de los clientes. -DHC Working Group of the IETF. Resources for DHCP. Disponible en Internet: http://www.dhcp.org/.

2. DESCRIPCIÓN DEL ESTADO ACTUAL DE LA RED DE DATOS DE LA UIS

Actualmente la Universidad Industrial de Santander cuenta con una red de datos de área local con topología en estrella y tecnología Giga y Fast Ethernet; el cableado que comunica el switch central y los switches departamentales es en fibra óptica multimodo.

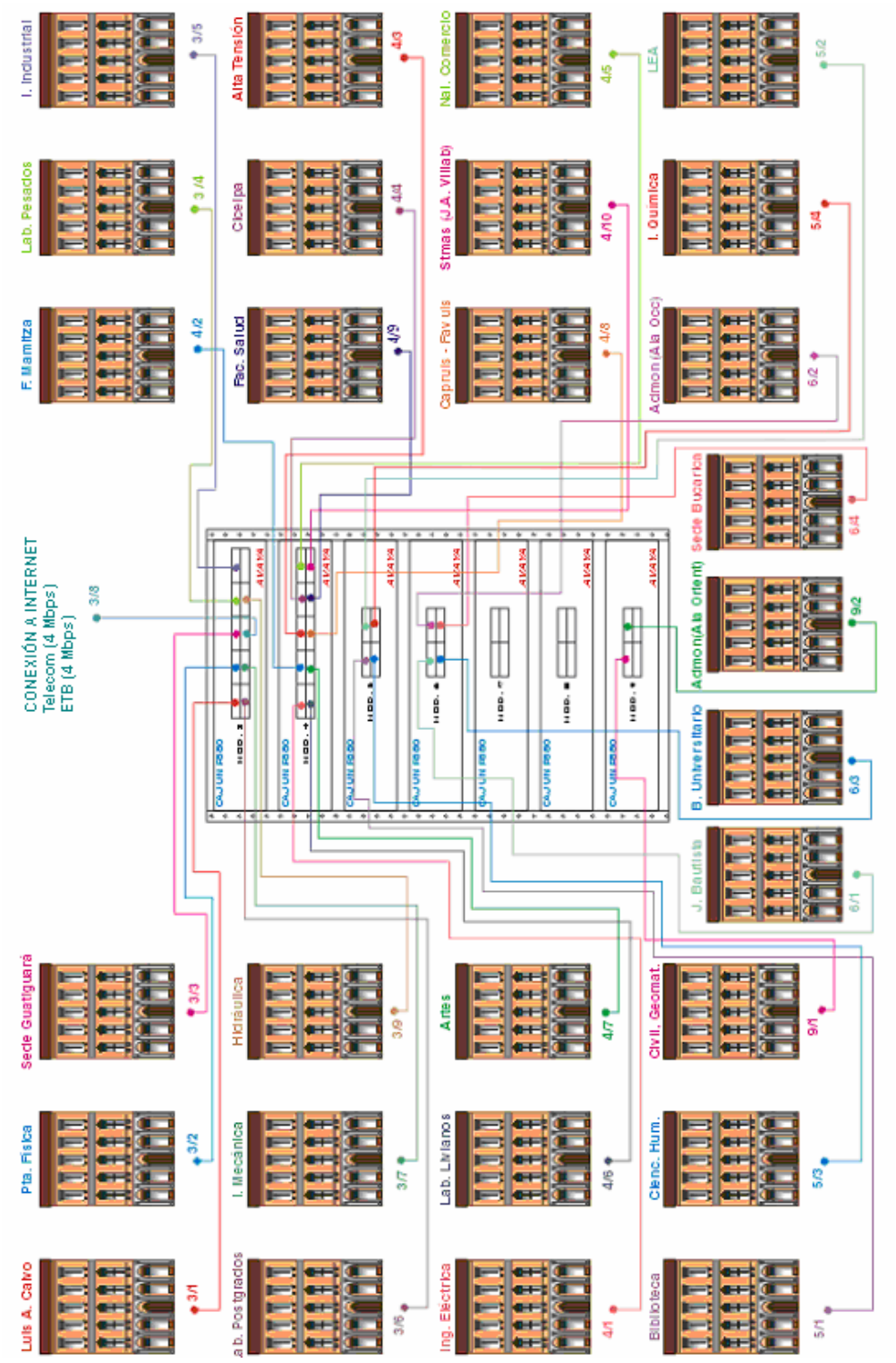
Sin embargo, por ser ésta una red que está en constante crecimiento y cuya estructura es modificada casi a diario, resulta complicado dar una descripción detallada de la misma, ya que cualquier generalización que se haga, va a resultar obsoleta en poco tiempo. A pesar de esto, se presenta a continuación una breve reseña del estado de la red de datos para el mes de diciembre de 2004.

2.1 DESCRIPCIÓN GENERAL

2.1.1 Switch Central.

El equipo central de la Universidad Industrial de Santander es un switch Cajun P880 marca Avaya de 16 slots, de los cuales 5 están siendo usados. Existen 2 módulos con 10 puertos Fast Ethernet cada uno, que conectan algunos edificios de la universidad por medio de fibra óptica, así como la Facultad de Salud, la sede de Guatiguará y el enlace externo a Internet. Los otros 3 módulos cuentan con 4 puertos Gigabit Ethernet cada uno, de los cuales 10 están siendo utilizados y conectan otros edificios y/o subredes del campus con el switch central, principalmente aquellos de alta prioridad como lo son la Biblioteca Central, el Edificio de Administración y la subred donde se encuentran los principales servidores. El esquema completo de este switch se observa en la figura 4, así mismo se especifica gráficamente la forma en que están distribuidos sus puertos para dar cubrimiento a los diferentes edificios y subredes.

Figura 4. Distribución de puertos del switch Cajun P880 para las diferentes subredes en la Universidad Industrial de Santander.



Fuente: Los autores.

Como se puede observar en la anterior gráfica, el puerto 8 del módulo 3 corresponde al puerto en el que se hace conexión con los proveedores de Internet. En la actualidad, la universidad cuenta con dos enlaces WAN que interconectan la red con dos ISPs[13], estos proveedores de Internet son Telecom y ETB, cada uno con enlaces de 4Mbps, asegurando así un ancho de banda total de 8 Mbps.

Ya que el Cajun P880 es un switch-router, posee todas las capacidades para desempeñarse como agente relay si se llevara a cabo la implementación de DHCP en la red de datos institucional, permitiendo así el intercambio de mensajes entre el servidor y los clientes que se encuentren en diferentes subredes.

2.1.2 Switches departamentales.

Son en su totalidad switches Cajun P330T marca Avaya, los cuales operan actualmente con la versión de software 3.5.23 y están conectados por medio de fibra óptica a los diferentes puertos Fast o Gigabit Ethernet del switch central.

Cada Switch departamental se encuentra ubicado dentro del cuarto de cableado de cada edificio y cuentan con 24 puertos RJ45, los cuales brindan conexión a otros switches y/o hubs y éstos a su vez a las estaciones de trabajo y servidores en las diferentes oficinas y salones de los edificios.

Debido a sus características y a la versión de software que manejan, los switches departamentales son dispositivos que operan únicamente en capa 2, es decir, no pueden desempeñarse como router y por consiguiente no podrían ser configurados como agente relay, lo cual no es en realidad un inconveniente a la hora de implementar el servicio, pero lo sería si se quisiera tener mas de 1 agente relay dentro de la LAN, pues de ser así resultaría necesario adquirir otro switch que sí presente las características

[13] ISP: Internet Service Provider. Las ISPs son empresas encargadas de proporcionar servicios de conexión a Internet a diferentes organizaciones o entidades que así lo requieran.

requeridas para funcionar como relay. Otra opción sería realizar una actualización de software en los switches departamentales que les permitiera operar en capa 3 y por lo tanto, ser configurados como agente relay.

2.1.3 Interconexión de sedes.

La Universidad Industrial de Santander ha alcanzado tal crecimiento tanto en la ciudad de Bucaramanga, como en el departamento de Santander, que además de la sede principal, posee actualmente 3 sedes dentro del área metropolitana y 4 más ubicadas en diferentes municipios del departamento, donde se adelantan todo tipo de actividades académicas, investigativas y administrativas. Dentro del área metropolitana de la ciudad se encuentran las sedes Bucarica, Guatiguará y la Facultad de salud, mientras que las sedes regionales están ubicadas en Socorro, Barrancabermeja, Málaga y Barbosa.

Todas estas sedes también se encuentran interconectadas con la sede principal en la misma red de datos, aunque para éstas se manejan en algunos casos velocidades de conexión diferentes a las que se usan en los enlaces de los edificios dentro del campus. Dichas velocidades se especifican en la tabla 3.

Tabla 3. Velocidades de conexión para las diferentes sedes de la Universidad Industrial de Santander.

SEDE	VELOCIDAD DE CONEXIÓN
Socorro	256 Kbps
Barrancabermeja	256 Kbps
Málaga	128 Kbps
Barbosa	128 Kbps
Fac. de Salud	100 Mbps
Guatiguará	100 Mbps
Bucarica	1000 Mbps

Fuente: Los autores.

Como se puede observar, las velocidades de conexión de las sedes regionales no permiten asegurar que el servicio de DHCP funcione adecuadamente en cada una de ellas, ya que el protocolo presente timeout de 2 seg para intercambio de mensajes. Sin embargo, posteriormente se tratará de estudiar este caso en particular y dar una opinión al respecto.

2.2 MANEJO Y ASIGNACIÓN DE DIRECCIONES IP

Cuando una red de datos incluye un número considerable de subredes y gran cantidad de estaciones, resulta difícil ejercer un control efectivo en cada segmento de la misma, presentando problemas con el manejo de las direcciones IP asignadas ya que éstas aumentan de acuerdo con las necesidades de los usuarios, constituyéndose de esta forma en un recurso difícil de administrar.

Desde sus inicios, en la red de datos de la universidad, las diferentes estaciones han venido siendo configuradas con direcciones IP estáticas, las cuales son asignadas por el Administrador de la Red de acuerdo a la ubicación física y lógica de cada estación, permitiendo así que los usuarios aprovechen este valioso recurso que la Universidad Industrial de Santander ofrece a su comunidad.

Sin embargo, no en pocas ocasiones se ha planteado la posibilidad de implantar ciertas políticas de gestión y administración de las direcciones, que permitan ejercer un mayor control sobre la forma en que éstas se asignan y cómo los usuarios las aprovechan correctamente. Actualmente no se cuenta con una normatividad adecuada para la solicitud de las direcciones IP; además, en múltiples ocasiones se han presentado situaciones que demuestran que se está incurriendo en faltas graves que afectan el correcto funcionamiento de la red.

Por ejemplo, en la red de datos de la universidad es común ver casos en los que clientes modifican su configuración de red y adquieren acceso a la

misma suplantando las direcciones IP de otros usuarios, cuyos parámetros sí les habían sido otorgados por el Departamento de Servicios de Información[14] de la universidad, generando así graves conflictos por duplicación de direcciones y consecuentemente deshabilitando al otro cliente como usuario de la red. Esta situación ha llevado a que estos clientes "expulsados" se vean obligados a configurar direcciones IP que no les asigna el administrador de la red, sino que ellos suponen les permitirá tener acceso nuevamente a la red; quienes reportan el caso, reciben otra configuración por parte del administrador, generando un desperdicio de recursos por direcciones abandonadas, ya que el cliente que realizó la modificación solo utilizará una dirección IP para acceder a la red.

Por otro lado, para la DSI ha resultado difícil mantener el control no sólo sobre los hosts nuevos que empiezan a ser parte de la LAN de manera ilegítima, sino también sobre aquellos que dejan de serlo, ya sea porque son dados de baja o porque el usuario decide no seguir haciendo parte de la red, sin embargo, es común que estos actos no sean reportados y propicien el mal uso de las direcciones IP.

Como consecuencia de estas situaciones, la DSI no posee un registro o inventario actualizado del número de estaciones que en el momento hacen parte de la LAN de la universidad, aunque se sospecha que esta cantidad estaría oscilando cerca de las 2000 estaciones.

Ya que resultaba indispensable conocer el número aproximado de las estaciones que serían clientes DHCP, fue necesario realizar unos barridos de direcciones IP en la red de datos, para ésto se usó la herramienta IP Address Management del software SolarWinds, la cual realiza una inspección por las diferentes subredes que conforman la LAN y da como resultado el número de estaciones que se encuentran encendidas en cada

[14] En adelante se llamará DSI a la División de Servicios de Información de la Universidad Industrial de Santander.

una de ellas, así como sus respectivas direcciones IP y tiempos de respuesta.

Como principales resultados de estas pruebas se obtuvo un número total de 1782 estaciones existentes en toda la LAN, las cuales se encuentran agrupadas en 80 subredes que se encuentran interconectadas a través del switch central de la universidad. Los resultados obtenidos en estos barridos se presentan tabulados y graficados en el ANEXO A.

Durante la realización de los barridos de direcciones IP que se llevaron a cabo, fue posible observar que existen subredes que no se registraban en los resultados obtenidos, posiblemente debido a la presencia de servidores Proxy que operan de manera clandestina dentro de la red y que permiten que clientes no autorizados tengan acceso a Internet. Éste es otro problema que se presenta comúnmente y que también dificulta que la DSI tenga un control sobre la cantidad de estaciones y el manejo de las direcciones IP que éstas utilizan.

Dadas las anteriores condiciones, para la DSI no ha resultado fácil mantener un control eficaz y desarrollar la administración de la red se ha convertido en una labor complicada y muy seguramente no se ha dado de una manera ordenada, lo cual indica que es urgente implantar nuevas políticas que garanticen un mejor funcionamiento y aprovechamiento de la red de datos.

2.3 BENEFICIOS DEL SERVICIO DHCP EN LA RED DE LA UNIVERSIDAD

La principal ventaja que presenta DHCP es que posee tres diferentes tipos de asignación de direcciones, los cuales pueden ser utilizados indistintamente dentro de una misma LAN de acuerdo no sólo a las necesidades de los clientes, sino también a las restricciones o políticas que

se quieran implantar a los usuarios, lo cual se realiza de manera centralizada desde el servidor.

En la red de datos de la universidad se manejan principalmente tres perfiles de usuario:

- Usuarios Administrativos.
- Usuarios Docentes.
- Usuarios Estudiantes.

Aunque estos tres usuarios presentan ciertas particularidades que los hacen diferir entre ellos, el uso que se hace de las estaciones de trabajo es generalmente el mismo en los tres casos, es decir, la mayor parte de estaciones trabajan de manera fija en una ubicación física dentro de las instalaciones de la universidad. Sin embargo, sería posible gracias a la implementación de DHCP, definir las políticas necesarias para el control de acceso a la red de cada usuario según su perfil; así mismo se facilitaría mantener actualizado un inventario con los equipos que hacen parte de la red.

Otro aspecto importante es la flexibilidad, ya que si por alguna razón es necesario cambiar direcciones de segmentos o de subredes, con DHCP dicha labor se efectúa de forma centralizada, y no es necesario que el administrador de la red se desplace al sitio donde se encuentra cada host para realizar su configuración respectiva, lo cual equivale a la reducción significativa en el tiempo que actualmente se emplea atendiendo este tipo de situaciones.

Así mismo, se plantearán nuevas políticas de gestión que permitirán llevar a cabo el proceso de solicitud de direcciones IP de una manera ordenada y eficiente, lo que le facilitará a la DSI obtener una base de datos actualizada, que posea la información correspondiente de cada equipo que se encuentra conectado a la red, donde se podrán manejar datos tan importantes como

sus direcciones MAC, IP, sistema operativo, nombre de host, entre otros. De esta manera se podrá ejercer un control eficaz sobre cada estación y se facilitará detectar las estaciones que incurran en faltas que alteren el buen funcionamiento de la red.

2.3.1 Estaciones móviles.

Las estaciones que requieren movilidad dentro de la LAN, son sólo un pequeño porcentaje del total de hosts que hacen uso de la red, aunque es importante tener en cuenta que actualmente este tipo de estaciones se está haciendo cada vez más común debido a los requerimientos de sus usuarios y a los múltiples avances tecnológicos que ofrecen los fabricantes.

En la actualidad, dentro de las políticas de gestión y asignación de direcciones IP no se hace diferenciación entre las estaciones fijas y las móviles, de esta manera los usuarios que poseen equipos portátiles se ven limitados a permanecer dentro del mismo espacio físico o donde se encuentre definida la subred en la cual es válida la configuración de red que les ha sido asignada. Si el usuario móvil requiere desplazarse a otro edificio o a otra subred y desea seguir manteniendo su conectividad, es necesario realizar una nueva configuración de los parámetros de red que sean válidos en el nuevo segmento al que se va a conectar.

Con DHCP se puede evitar la situación mencionada anteriormente, pues se podrían definir políticas que garanticen la movilidad de dichas estaciones sin necesidad de estar cambiando constantemente su configuración de red, manteniendo siempre la seguridad y el buen desempeño de la red.

2.3.2 WLANs.

La red de datos de la universidad cuenta actualmente con una red inalámbrica (WLAN[15]) implementada, la cual se encuentra ubicada en la

[15] Wireless Local Area Network.

sede de Guatiguará y está conformada por un Punto de Acceso (AP, Access Point[16]) marca D-Link[17] que le permite conectividad a 15 clientes.

La configuración de la interfaz de red se hace de manera idéntica a la de las estaciones fijas y móviles que se mencionaron anteriormente, una dirección IP es asignada por el administrador de la red y ésta es introducida por cada usuario, permitiéndole así tener acceso a la red.

Actualmente en el mercado se ofrecen gran número de Puntos de Acceso (Access Point) que poseen diferentes características de desempeño y configuración y algunos traen un servidor DHCP incorporado. Sin embargo, si se desea que los clientes de la WLAN obtengan su configuración de red desde un servidor DHCP centralizado, es necesario que los Puntos de Acceso implementados permitan el intercambio de mensajes para otorgar dicha configuración a los clientes, de lo contrario será necesario que éstos sean configurados estáticamente.

En conclusión, son numerosos los beneficios que se obtendrían por la implementación de DHCP en la red de la universidad, ya que ésta se convertiría en un recurso más seguro y confiable para toda la comunidad, el cual hará posible la prestación eficaz del servicio.

2.4 REQUERIMIENTOS PARA LA IMPLEMENTACIÓN DEL SERVICIO

Para implementar el servicio de DHCP es conveniente conocer las características propias de la red, además de otros factores, para poder establecer si se requiere segmentar la red y así el posible número de servidores a utilizar.

---

[16] Dispositivo que conecta una red cableada y un dispositivo remoto (cliente) a través de un enlace inalámbrico.

[17] DWL - 2000AP+ D-Link AriPlus G+ 2.4 GHz Wireless Access Point de 54 Mbps (802.11g).

Sin embargo, es claro que existen 3 entidades fundamentales que hacen posible que el servicio DHCP se preste en una red con características similares a las de la universidad, dichas entidades son:

- El servidor DHCP,
- Los clientes DHCP y
- El agente relay.

Las cuales se describen a continuación.

2.4.1 Servidor DHCP.

Es una aplicación administrable que se ejecuta en un host de la red, el cual atiende las solicitudes de los clientes y que en su configuración almacena tablas con posibles direcciones IP a otorgar, además del resto de la información necesaria para que los clientes accedan a la red.

Si se requiere segmentar la red y se van a configurar varios servidores hay que tener en cuenta que un servidor DHCP no comparte información con otros servidores DHCP; esto implica la necesidad de crear un rango de direcciones IP diferente para cada servidor y que pueda por tanto dar de su rango a determinados clientes DHCP

Así mismo, es necesario tener en cuenta que el servidor DHCP debe estar en capacidad de soportar una cantidad considerable de clientes, ya que, como es el caso de la red de la UIS, existen redes que constantemente están en crecimiento y/o expansión, haciendo que cada día el número de usuarios sea mayor.

Dado que DHCP utiliza UDP como protocolo de transporte, el cual es en su forma elemental bastante inseguro, es posible que servidores no autorizados se establezcan fácilmente y envíen información falsa y potencialmente destructiva a clientes, generando así direcciones incorrectas

o duplicadas.

Actualmente, existe una gran cantidad de servidores DHCP disponibles en el mercado, ya que los fabricantes han identificado este servicio como uno de los más implementados en las redes de datos. Es por esto que casi todos los sistemas operativos poseen una aplicación para ejecutar el servicio DHCP, algunos de estos son: Windows Server en sus versiones 2000 y 2003, Linux Red Hat, Windows NT, entre otros.

2.4.2 Clientes DHCP.

Son hosts que poseen en su configuración la pila de protocolos TCP/IP de la cual hace parte DHCP. La interfaz de red de un host, permite ser configurada para asignación estática o automática (por medio de DHCP), al habilitar la opción que indica que la dirección IP se obtendrá automáticamente, el cliente enviará un mensaje (DHCP Discover) para descubrir los posibles servidores DHCP al iniciar su actividad en la red. Esta característica es soportada por todos los sistemas operativos más comúnmente usados.

2.4.3 Agente DHCP Relay.

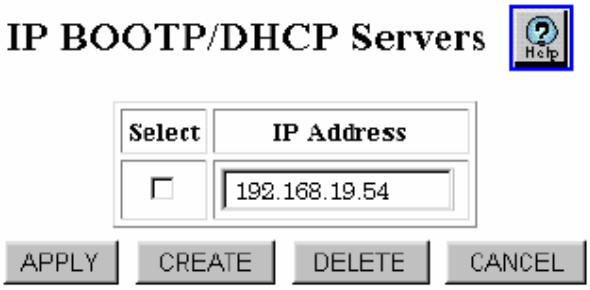
Como se mencionó, estos agentes permiten el intercambio de mensajes entre los clientes y servidores que se encuentren en diferentes subredes; interceptan las solicitudes broadcast de los clientes DHCP y reenvían los paquetes en forma unicast al servidor que está ubicado en otra subred, eliminando así la necesidad de tener un servidor DHCP en cada subred.

- **Configuración del Agente Relay.** Puede ser configurado en un router que interconecte las subredes a las cuales les vaya a prestar el servicio o también puede ser en un host que preste este servicio dentro de una subred determinada. En el caso de la universidad, el switch-router central (Cajun P880 de Avaya) permite ser configurado como agente relay por medio de un

sencillo procedimiento que puede ser ejecutado de dos maneras: por medio de la Interfaz de Línea de Comandos (CLI) o usando el Agente Web; por razones prácticas, como la interfaz gráfica y sencillez para efectuar cambios, se recomienda hacerlo a través de este último.

El primer paso para la configuración del Agente Relay en el switch P880 consiste en introducir la dirección del servidor DHCP en la caja de diálogo (del agente web) **IP BOOTP/DHCP Servers**, a la cual se accede siguiendo la ruta **Routing>IP>Configuration,** (figura 5). Como se puede observar, existen 4 opciones, de las cuales se tiene que elegir la opción **CREATE,** ya que éste es el primer servidor que se introduce.

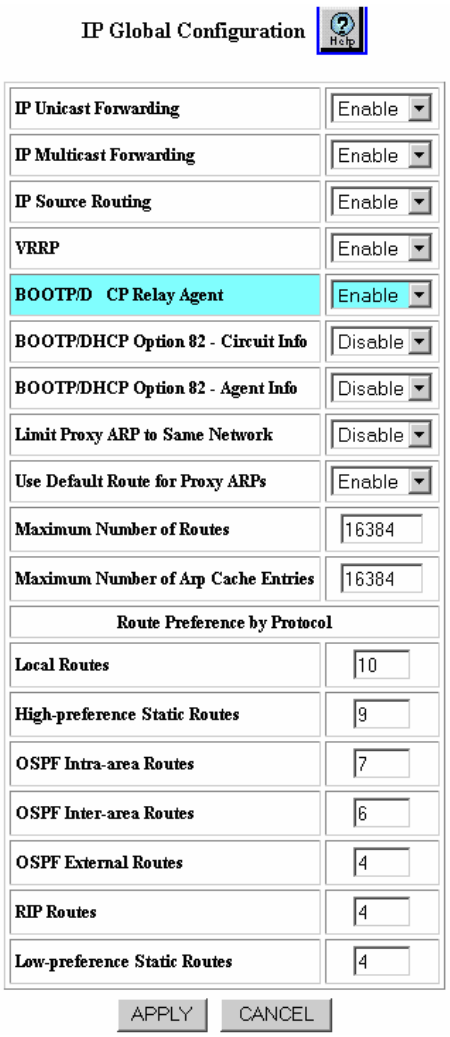
Figura 5. Caja de diálogo *IP BOOTP/DHCP Server*



Fuente: Avaya P550R, P580, P880, and P882 Multiservice Switch User Guide

Después de crear la nueva entrada, otra caja de diálogo se abre dando la posibilidad de adicionar otros servidores DHCP existentes en la red. Por último, es necesario habilitar el servicio del Agente Relay, que se ejecuta desde la caja de diálogo **IP Global Configuration**, la cual se aprecia en la figura 6.

Figura 6. Caja de diálogo *IP Global Configuration*



Fuente: Avaya P550R, P580, P880, and P882 Multiservice Switch User Guide

En el ANEXO B se presenta la información completa acerca de la configuración del switch Cajun P880 como Agente Relay.

Si después de realizar las pruebas de tráfico generado por el servicio DHCP se determinara que éste es muy elevado, es decir que el tráfico broadcast fuera necesario aislarlo antes de que llegara al switch central, y por lo tanto resultara aconsejable la utilización de varios agente relay, se podrían

plantear algunos escenarios que permitirían que el servicio se diera de una mejor manera.

El primero sería adquirir módulos de actualización del software de los switches departamentales que se deseen configurar como agentes relay, actualmente cada módulo posee un valor de US$932 y permitiría que los switches Cajun P330T operen como routers.

Otra posible solución sería adquirir switches-routers que permitieran ser configurados como agentes relay, algunos que cumplen con esta característica son los switches Cajun P333R y Cajun 363T de Avaya, los cuales cuentan con 24 puertos y tienen un valor de US$4480 y US$2244[18] respectivamente. Estos agentes relay deberán ser ubicados estratégicamente para permitir un balance en el tráfico que maneje cada uno.

Sin embargo, no es este el momento para adentrarse en estos temas; primero es necesario seleccionar el servidor adecuado para la realización de las pruebas de tráfico y así poder plantear una propuesta formal de diseño basada en la estimación de tráfico obtenida. En el siguiente capítulo se harán las consideraciones necesarias para obtener un servidor de buen desempeño y dar inicio a las pruebas para la implementación del protocolo.

[18] Precios proporcionados por la empresa Integrar S.A., proveedora de soluciones de conectividad para la Universidad Industrial de Santander.

3. REVISIÓN Y SELECCIÓN DE RECURSOS PARA LA REALIZACIÓN DE LAS PRUEBAS DE TRÁFICO GENERADO

Dentro del objetivo general de este proyecto está contemplado determinar la viabilidad del uso de DHCP en la red de datos institucional, lo que implica definir una metodología para desarrollar pruebas de tráfico cuyos resultados conlleven a tomar una decisión sobre la implementación del servicio; para realizarlas se deben propiciar escenarios adecuados y contar con los recursos y las herramientas necesarias que permitan hacer un análisis completo y detallado de los mensajes intercambiados por las entidades y los tiempos empleados en el proceso.

A continuación, en este capítulo se procederá a escoger adecuadamente los elementos fundamentales involucrados para ejecutar la metodología, y posteriormente se relacionarán mediante unas pruebas de flujo de tráfico.

3.1 COMPARACIÓN DE LAS ESPECIFICACIONES TEÓRICAS

De acuerdo a los requerimientos y el nivel de soporte ofrecido actualmente por la infraestructura de la red de datos institucional, es necesario seleccionar un servidor DHCP que ofrezca y almacene parámetros de configuración a los clientes, con quienes se comunicará a través de solicitudes que serán retransmitidas bidireccionalmente por un agente relay.

De igual forma, debe existir un analizador de red que permita hacerle seguimiento a la información intercambiada durante la ejecución del servicio, presente el registro de datos de una manera amigable y facilite el análisis de dichos paquetes.

3.1.1 Servidor DHCP.

Es fundamental que las prestaciones ofrecidas por el servidor, puedan satisfacer las necesidades de todos los clientes que la organización determine, más aún en una red de alta complejidad, considerable número de dispositivos activos y pasivos, de los cuales posiblemente un gran número requerirá parámetros de configuración TCP/IP.

En el mercado existen completas soluciones comerciales y de software libre que responden a lo mencionado anteriormente. Aunque diversas compañías ofrecen aplicaciones integrales del servicio DHCP, que permiten una administración sencilla y eficiente, acompañadas de un buen soporte de usuario, es conveniente señalar que los desarrollos de software abierto han ganado aceptación tanto a nivel empresarial como de la comunidad científica, ya que han presentado una evolución favorable en el desarrollo de sus productos, evidenciado por las mejoras incorporadas en los códigos y los esfuerzos por ofrecer un entorno más agradable al usuario.

De esta manera, se efectuó una revisión de las especificaciones de los posibles servidores y se escogieron algunos parámetros con el fin de determinar el más apropiado. A continuación, en la tabla 4 se presenta la relación de las correspondientes propuestas.

Tabla 4. Características de servidores DHCP.

SERVIDORES	WINDOWS 2003 SERVER	ISC SERVER DHCP V3.0PL1	VICOMSOFT DHCP SERVER
Requerimientos del Sistema	Procesador de 550 MHz. Memoria RAM:256MB Capacidad en Disco: 1,5 GB	Procesador Pentium II o Athlon Memoria RAM: 256 MB MB Capacidad en Disco: 33 MB.	Procesador Pentium 100 Mhz Memoria RAM:32MB. Capacidad en Disco 5 MB.
Número de clientes	No restricción, según pruebas soporta más de 10000	No restricción	1024
Sistema Operativo	Windows 2000, Windows NT 4 o superiores	Linux Red Hat 9.0	Windows 95/98 o Microsoft™ Windows NT 4 o superiores.

Clientes que soporta	Windows 95/98/NT4/2000/Me/XP	Windows 95/98/NT4/2000/Me/XP y Linux	Windows 95/98/NT4/2000/Me/XP y MacOS
Desempeño	Alto, según pruebas hubo tiempos de concesión de 80 ms para 10000 equipos	No se tiene registro.	Determinado solamente por el grado de satisfacción de sus clientes.
Vía de administración	Consola Interfaz gráfica	Interfaz gráfica Archivo de configuración	Consola Interfaz gráfica
Ventaja	Herramientas de supervisión del rendimiento y detección de servidores intrusos	Disponibilidad para modificar la configuración y las opciones del protocolo; código abierto	Solución a la medida, respaldada por un buen soporte.
Adquisición / Licencia/ Proveedor	Licencia Microsoft	Internet Software Consortium, gratuito	Licencia de Vicomsoft US$ 599

Fuente: Los autores.

Después de analizar cuidadosamente las diferentes alternativas, teniendo siempre presente la optimización de recursos y considerando la relación calidad/precio como argumento principal de comparación, se optó por seleccionar el Servidor DHCP v 3.0pl1 que ofrece Linux Red Hat 9.0; y aunque no se conocían registros en cuanto a su rendimiento, si existían buenas referencias de desempeño por parte de la DSI en cuanto a la implementación de servicios con características similares en distribuciones GNU/Linux. De esta manera se concluyó que era un servidor de alto rendimiento, fiabilidad y prestaciones a un costo muy bajo**.**

3.1.2 Herramienta software para análisis de tráfico.

Los analizadores de red conocidos también como sniffers, son programas que pueden obtener una copia de todos los paquetes de datos intercambiados en una red local, procesarlos, almacenarlos y presentarlos en una interfaz gráfica; estos programas muestran todo tipo de detalles sobre los paquetes, como tipo de protocolo utilizado, direcciones origen, destino, número de transacciones, permitiendo localizar fallas en la red,

recolectar estadísticas y determinar la cantidad de tráfico que se genera en cada nodo del segmento de red.

Existe un número considerable de analizadores de red que ofrecen potentes prestaciones en cuanto a filtrado de paquetes, monitoreo en tiempo real y generación de estadísticas, los cuales presentan características similares en cuanto a su operación; se deben instalar en una estación soportados por una librería de la interfaz de red sobre el sistema operativo, ofrecen posibilidad de trabajar en modo promiscuo[19] y es necesario especificar el hardware sobre el cual se va operar (NIC[20], módem, etc).

Sin embargo, hay que destacar que en las pruebas a realizar no se utilizarán los sniffers para la obtención de un patrón de tráfico o para efectuar un análisis profundo de diversos protocolos, sino que se orientarán hacia la estimación del incremento de tráfico en la red de datos generado por el servicio DHCP. A continuación, en la tabla 5 se describe la relación de las diferentes alternativas.

Tabla 5. Comparación de analizadores de red.

CARACTERÍSTICA	ANALYZER	ETHEREAL	NTOP	SNORT
Sistemas operativos	Windows	Windows y Linux	Windows y Unix	Linux, Solaris, Windows 2000
Análisis detallado protocolo DHCP	Si	Si	Si	No
Modo de Operación	Promiscuo	Promiscuo	Promiscuo	Lista reglas
Visualización gráfica	Si	Si	Si	Si
Estadísticas por tipo de mensaje DHCP	No	Si	No	No
Análisis de archivos generados previamente	Si	Si	Si	Si

[19] En modo promiscuo se obtiene una captura de todo el tráfico visible que atraviesa la tarjeta de red.

[20] Network Interface Card.

Construir Filtros de captura	Si	Si	Si	Si
Captura en Tiempo Real	Si	Si	Si	No
Modo de adquisición	De dominio público pero no de código fuente abierto .	Código fuente abierto	Código fuente abierto	Código fuente abierto

Fuente: Los autores.

Teniendo en cuenta que es necesario realizar capturas en el servidor y en los clientes, los cuales operarán en Linux y Windows respectivamente, para contrastar resultados, y aprovechando la sencillez de configuración de los filtros y el grado de detalle de información acerca del protocolo (cantidad de mensajes o tipo), se decidió utilizar ***Ethereal*** como analizador de red.

3.2 FUNCIONAMIENTO DE LOS ELEMENTOS SELECCIONADOS

3.2.1 Servidor DHCP v3.0pl1 de Linux Red Hat 9.0.

Para asegurar la correcta prestación del servicio, es prioritario tener en cuenta que la estación sobre la que se instale el servidor no será un cliente DHCP, por lo tanto sus parámetros de red deben ser proporcionados de manera estática.La configuración de DHCP se basa en un archivo de texto, ubicado en el directorio /etc/, nombrado dhcpd.conf, el cual contiene las especificaciones que describen los parámetros que se ofrecerán a los clientes de acuerdo a las subredes definidas por cada interfaz.

Entre los parámetros más importantes se encuentra la identificación del segmento de red, la máscara de subred, las puertas de enlace, el nombre de dominio, la dirección IP, el tiempo de lease, entre otros. Red Hat 9.0 contiene un archivo ubicado en el directorio /usr/share/doc/dhcp-3.0pl1, que presenta un ejemplo de la configuración del servidor DHCP, el cual se presenta a continuación:

```
ddns-update-style interim;
authoritative;
```

```
subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000;         # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
        # --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.255;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
```

Las directrices definidas en el archivo de configuración se pueden clasificar en dos tipos: la información que el servidor ofrece a los clientes, identificada con la palabra reservada “option” y la descripción de sus características las cuales no están precedidas de esta directiva; para el último caso es importante destacar que con las palabras reservadas “host” y “range dynamic-bootp” se implementan los mecanismos de asignación manual y dinámica, asociando la interfaz física a una única IP y especificando el tiempo de lease respectivamente. Las líneas que contienen ddns-update-style interim” y “authoritative” son parte de las características propias del servidor[21].

De igual manera, se presenta la agrupación de declaraciones para clientes dentro de un mismo segmento de red a través de la directiva “subnet”, labor que se puede extender a grupos mediante definiciones “pool” o “group”, o de otro modo ofrecer los parámetros globalmente. Cualquier parámetro especificado en una subred tiene preferencia sobre los

[21] Para mayor información remítase a la página man de dhcpd.conf.

establecidos de forma global y se le da prioridad a los de alcance más específico.

Cuando se ejecuta el servicio DHCP, ya sea por interfaz de línea de comandos digitando */sbin/service dhcpd restart* o activándolo desde el administrador de servicios de Linux, el demonio lee el archivo en mención y almacena en memoria una lista de las direcciones disponibles en cada subred; hay que tener en cuenta que para que cualquier modificación se actualice, se debe reinicializar el servicio, lo que implica recordar los contratos establecidos.

La información otorgada a los clientes se almacena en forma de base de datos en un archivo denominado *dhcpd.leases* y se guarda en el directorio /var/lib/dhcp, generado de forma automática por dhcpd, lo que le permite conocer al administrador el estado de las direcciones en cada momento. Este archivo es el almacén permanente de los parámetros relacionados con los clientes que se conectan al servidor; en él quedan grabadas las direcciones IP asignadas, el vencimiento del alquiler, la identificación única, siempre que un contrato se establezca, se renueve o expire, y se asumirá como una nueva entrada la que está ubicada al final del dhcpd.leases. Si aparece más de una entrada para un mismo contrato se asume como válida la que se encuentre más cercana al final del archivo.

El archivo dhcpd.leases es imprescindible cuando el servicio se ejecuta por primera vez, ya que el servidor primero lee el archivo de configuración *dhcpd.conf*, continúa con dhcpd.leases y marca los clientes con asignaciones activas; es decir, si éste no existe, se puede generar un conflicto, por lo tanto se debe crear el archivo desde la consola a través de:

```
# touch /var/lib/dhcp/dhcpd.leases
```

Para prevenir que el archivo de contratos crezca indefinidamente, cada cierto tiempo todos los contratos conocidos son trasladados hacia otro con el nombre dhcpd.leases~, permitiendo que los nuevos contratos se almacenen en el archivo principal; si durante este proceso el sistema y/o el

servicio abortan, puede que no se llegue a generar el nuevo archivo principal, en cuyo caso se requerirá crearlo manualmente para que el servicio pueda reiniciar correctamente.

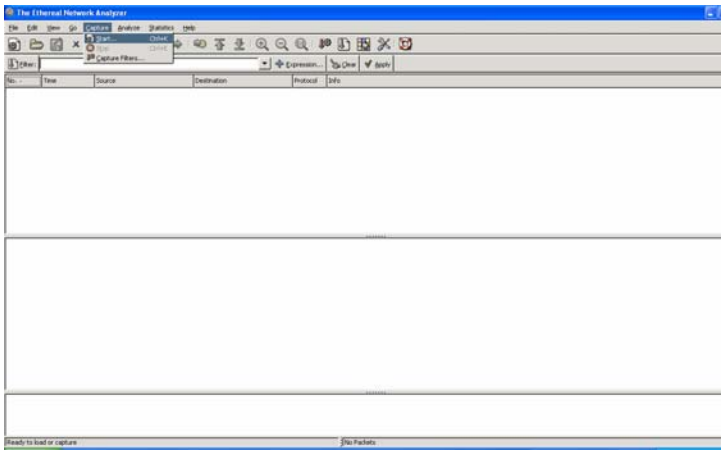
Como se observa, la configuración y modificación del archivo es un proceso bastante sencillo, el cual permite de una manera organizada y controlada prestar el servicio; además incorpora diversos comandos y directrices que permitirán establecer fácilmente políticas de acuerdo a las determinaciones del administrador de red o a las distribuciones de hosts requeridas. Si es necesario crear un archivo de gran tamaño, este se basará en el modelo presentando y se efectuarán las adiciones correspondientes.

3.2.2 Analizador de red Ethereal.

Conociendo el entorno de la aplicación y con suficiente conocimiento sobre la definición de los filtros, el procedimiento de configuración del sniffer, se puede describir en los siguientes pasos:

En el menú principal se despliega Capture y la opción start es seleccionada para iniciar el analizador, el cual conduce al cuadro de diálogo donde se definen los parámetros a tener en cuenta. La primera interacción con el analizador se muestra en la figura 7.

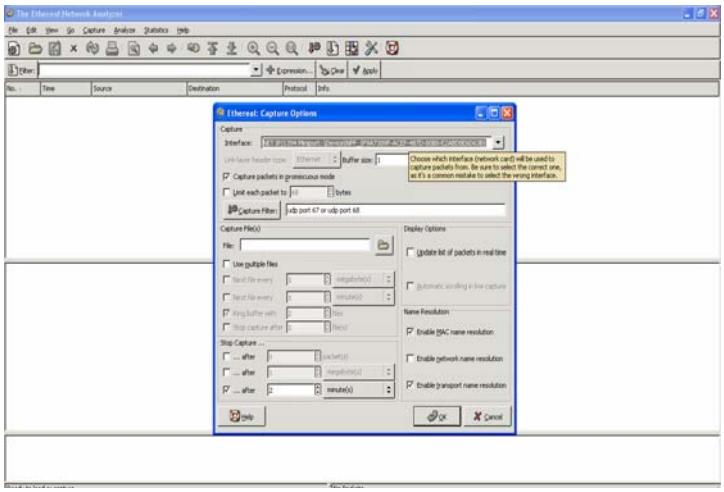
Figura 7. Vista general de Ethereal.



Fuente: interfaz de Ethereal

Posteriormente se determina la interfaz hardware a utilizar, que para este caso es una Intel® PRO/1000MT Network Connection y se define el filtro de captura; recordando que DHCP utiliza UDP como protocolo de transporte y de acuerdo a los puertos asignados, se crea la expresión “udp port 67 or udp port 68” con el objetivo de registrar solamente transacciones entre servidor y clientes DHCP, como se presenta en la figura 8.

Figura 8. Definición de la interfaz hardware, filtros y opciones de captura.

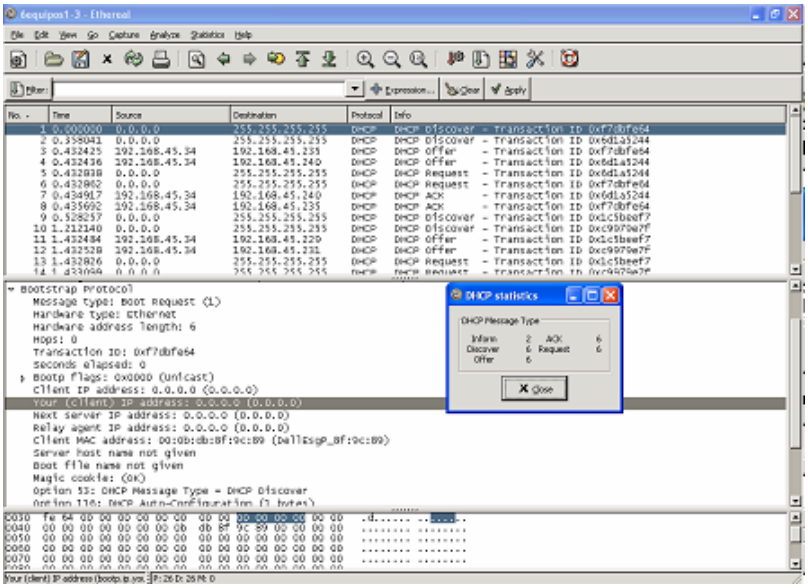


Fuente: Interfaz gráfica de ethereal

Adicionalmente, se puede establecer la duración de la captura de acuerdo al tiempo o la cantidad de bytes y actualizar la lista de paquetes en tiempo real. En esta instancia, el proceso está listo para activarse en cualquier momento.

Se realizó una captura de prueba, donde el analizador desplegó la información de cada paquete detallada al máximo, permitiendo hacer un completo seguimiento a cada transacción, presentando los diferentes campos y opciones del formato DHCP descrito en el capítulo 1; además emitió un reporte de gran valor, que consistió en una estadística por cada tipo de mensaje intercambiado. En la figura 9 se presenta una toma con lo que se confirma la selección adoptada.

Figura 9. Secciones del análisis de datos y estadísticas por tipo de mensaje.



Fuente: captura con Ethereal

La presentación de resultados está organizada en tres secciones: en la primera se muestran todos los mensajes capturados, identificando las direcciones fuente y destino, el protocolo, el tipo de mensaje y el identificador de transacción. En la segunda se realiza el análisis de cada paquete por protocolo, se despliegan los campos y opciones del mismo, permitiendo hacer un seguimiento completo a los mensajes intercambiados; en la tercera se expresan dichos valores en notación hexadecimal.

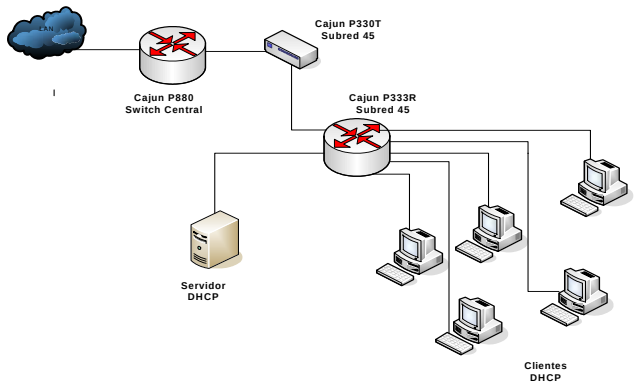
Además, la caja de diálogo *DHCP statistics* presenta el conteo de paquetes intercambiados en el proceso por tipo de paquete, importante si se quiere hacer una revisión rápida del correcto funcionamiento en cuanto a número de mensajes.

3.3 PRUEBAS DE VERIFICACIÓN DEL FUNCIONAMIENTO DEL SERVIDOR DHCP UTILIZANDO LA HERRAMIENTA SOFTWARE ETHEREAL

Para asegurar que el servidor DHCP v 3.0pl1 de la distribución Linux Red Hat 9.0 funcionará correctamente en la ejecución de la metodología, es necesario desarrollar minuciosas pruebas preliminares soportadas por ***Ethereal,*** con el objetivo de verificar la obtención de la configuración de red ofrecida a cada cliente.

El escenario generado para la realización de estas pruebas se muestra en la figura 10, en el cual el servidor DHCP se configuró para realizar asignaciones a clientes que se encontraban en el mismo segmento de red formando parte de la subred 192.168.45.0, los cuales estaban conectados a un switch Cajun P333R[22] marca Avaya que establecía conectividad con el switch departamental del Laboratorio de Alta Tensión. El servidor Linux se ejecutó en una máquina Optiplex marca Dell con procesador Pentium 4, 512 MB en RAM, el cual se identificaba con la dirección IP estática 192.168.45.33 y los equipos cliente trabajaron sobre el Sistema Operativo Windows XP, solicitando direcciones dinámicamente en un rango de 10 direcciones IP (de 192.168.45.2 a 192.168.45.11).

Figura 10. Esquema de red implementado para las pruebas de verificación.



Fuente: Los autores.

Estas pruebas se realizaron activando y desactivando la conexión de red simultáneamente en los clientes que realizaban las solicitudes, de la misma forma se iniciaban las capturas de tráfico en el correspondiente analizador.

[22] Es un dispositivo que funciona como switch-router, para estas pruebas estaba configurado como switch.

Los parámetros a los cuales se les evidenció la validez de sus valores fueron: el tiempo de lease, el rango de asignación y el tiempo de renovación, así como el tiempo de configuración de cada cliente y el número de mensajes que emplean en sus transacciones.

3.3.1 Tiempo de Lease y renovación.

El archivo dhcpd.conf trae configurados por defecto ciertos valores para el tiempo de lease, los cuales se presentan a continuación, expresados en segundos

Default lease time 21600
Max lease time 43200

Estos tiempos definen los períodos por defecto y máximo que un cliente puede mantener su dirección IP sin necesidad de renovarla. Para estas pruebas fue necesario modificarlos por tiempos menores, los cuales fueron iguales para cada uno de ellos, con el fin de verificar las consecuencias en la configuración de un cliente. Los principales resultados de estas pruebas se presentan en la tabla 6.

Tabla 6. Resultados de las pruebas de verificación del tiempo de lease.

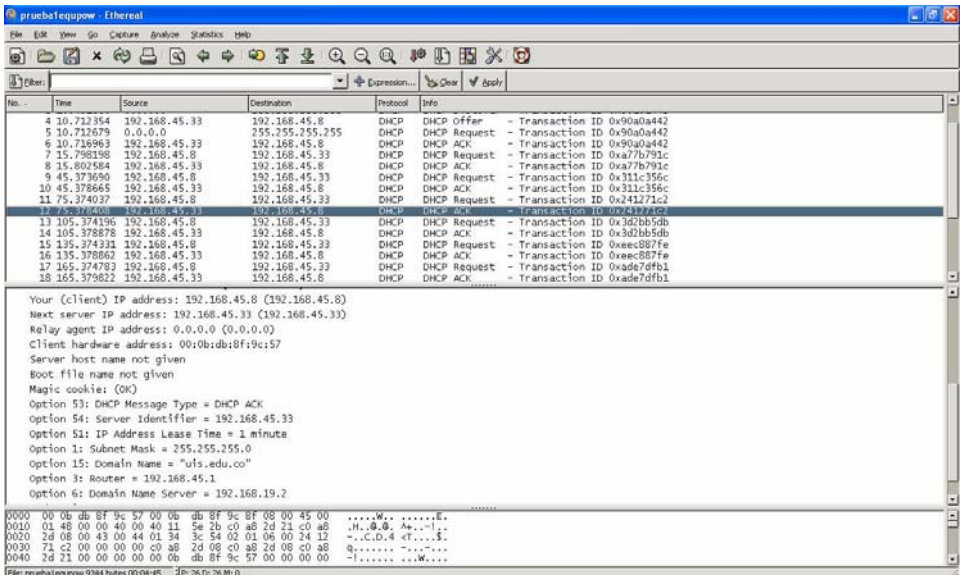
Prueba Nº	Parámetros (segs.)		Renovación (segs)
	Default lease time	Max lease time	
1	30	30	15
2	60	60	30
3	120	120	60
4	180	180	90
5	240	240	120

Fuente: Los autores.

Como se puede ver en la columna de renovación, el tiempo en el que cada cliente hace este proceso corresponde a la mitad del tiempo configurado para los parámetros de Default o Max lease time y el tiempo de lease es

consecuente con lo especificado en la columna del “Default Lease time”. Estos datos se obtuvieron gracias a la revisión detallada de las capturas que se hicieron con el software analizador de red Ethereal, tanto en el servidor como en cada cliente. En la figura 11 se presenta una captura registrada en un cliente.

Figura 11. Captura de asignación de parámetros a un cliente.



Fuente: Los autores.

Centrándose en la segunda sección, se pueden detallar todos los parámetros de configuración adquiridos por el cliente y se identifican las entidades involucradas en el proceso: el servidor tiene asociada la dirección IP 192.168.45.33 (Next Server IP address) y el cliente recibió la 192.168.45.8 (Your (Client) IP address), tal y como se había planteado en el esquema inicial. En cuanto al tiempo de lease, se observó la Opción 51 (IP Address Lease Time) donde el valor asignado al cliente es efectivamente el tiempo definido en el fichero de configuración, que corresponde a un (1) minuto.

Un detalle importante, es que las transacciones que se muestran en la parte superior de la captura, tienen un identificador único que distingue cada

pareja de REQUEST y ACK, con lo que se evidenció que las solicitudes de renovación se hicieron cada 30 segundos. Con esto se observó que en promedio el tiempo en el que cada cliente realizó la renovación de su configuración fue aproximadamente la mitad del tiempo de lease configurado en el servidor, correspondiente al tiempo T1 cuando el cliente hace la transición al estado RENEWING[23], garantizando de esta manera suficiente tiempo al proceso por si llegara a existir alguna eventualidad durante la renovación.

Posteriormente se definieron menores tiempos para el Default Lease Time respecto al Max Lease Time, con el fin de revalidar lo encontrado anteriormente o identificar alguna anomalía. Según esto, se obtuvieron los resultados que se aprecian en la tabla 7.

Tabla 7. Resultados a las pruebas de verificación del tiempo de renovación.

Prueba Nº	Parámetros (segs.)		Resultado (segs)
	Default lease time	Max lease time	
1	30	60	15
2	60	120	30
3	120	240	60
4	480	960	240

Fuente: Los autores.

Continuando con el mismo análisis de las capturas, se verificó que efectivamente el parámetro del cual depende el tiempo en que se hacen las renovaciones es el Default lease time. Además se hizo una prueba adicional para medir la confiabilidad del servidor, definiendo el Default lease time mayor que el Max lease time, del cual se obtuvo una respuesta acertada, es decir, el servidor tomó como tiempo de renovación la mitad del Max lease time y es quien determina el tiempo máximo para asignar un arrendamiento.

[23] Para mayor información remítase al RFC 2131, sección Estados del protocolo

3.3.2 Rango de direcciones.

Con estas pruebas se buscó verificar que el servidor asignara siempre la misma dirección IP a los equipos cliente, tal y como está definido en la teoría referente a la asignación dinámica de direcciones. Para su ejecución se mantuvo el esquema de la figura 1, pero a diferencia de las pruebas anteriores, éstas se realizaron para 2 y 4 clientes simultáneamente; además se quiso comprobar si el tiempo de renovación era similar para los diferentes clientes.

En la tabla 8, se muestran los resultados obtenidos en las pruebas para 2 clientes, así mismo se presentaron los valores de Default y Max lease time con los que se configuró el servidor para dicha prueba.

Tabla 8. Resultados a las pruebas de verificación del rango de direcciones en 2 equipos cliente.

No. De Prueba	Default & Max Lease Time (seg.)	Cliente 1		Cliente 2	
		Dirección Asignada	Tiempo (seg.)	Dirección Asignada	Tiempo (seg.)
1	30	192.168.45.11	14.999473	192.168.45.10	15.0021
2	60	192.168.45.11	30.000893	192.168.45.10	30.0011
3	120	192.168.45.11	60.003484	192.168.45.10	60.0041
4	180	192.168.45.11	90.021192	192.168.45.10	90.0067
5	240	192.168.45.11	120.021815	192.168.45.10	120.003

Fuente: Los autores.

En el mismo orden de ideas se realizaron las pruebas con 4 clientes, presentando los resultados en la tabla 9.

Tabla 9. Resultados de las pruebas de verificación de los tiempos de renovación en 4 equipos cliente.

No. De Prueba	Default & Max Lease Time (seg.)	Cliente 1		Cliente 2		Cliente 3		Cliente 4	
		Dir. Asignada	T (seg.)	Dir. Asignada	T (seg.)	Dir. Asignada	T (seg.)	Dir. Asignada	T (seg.)
1	30	192.168.45.11	15.001	192.168.45.10	15.001	192.168.45.4	14.999	192.168.45.9	15
2	60	192.168.45.11	30.001	192.168.45.10	30.020	192.168.45.4	30	192.168.45.9	30.007

3	120	192.168.45.11	60.017	192.168.45.10	60	192.168.45.4	60.042	192.168.45.9	60.017
4	180	192.168.45.11	90	192.168.45.10	90	192.168.45.4	90.008	192.168.45.9	90.019
5	240	192.168.45.11	120	192.168.45.10	120	192.168.45.4	120.006	192.168.45.9	120.019

Fuente: Los autores.

De esta misma manera se pudo verificar que el servidor asigna la misma dirección IP a cada cliente cada vez que solicita renovación o cuando reinicia el proceso de solicitud, a pesar que el servidor aún tenía otras direcciones libres en su rango (Asignación Dinámica).

Así mismo, se verificó que el servidor después de haber asignado todas las direcciones definidas en su rango no asigna configuración de red a otros clientes que hagan solicitudes posteriores; aunque si el cliente es apagado y su interfaz de red desactivada, antes que haga renovación, sus parámetros pueden ser asignados a los nuevos clientes.

3.3.3 Número de mensajes y tiempo de configuración de clientes.

Según la documentación teórica que se realizó en el primer capítulo de este libro, la configuración de un cliente DHCP se realiza por medio de la interacción cliente-servidor, la cual consiste en el intercambio de 4 mensajes entre estas 2 entidades; estos mensajes son: DHCP Discover, DHCP Offer, DHCP Request y DHCP ACK, y cada uno tiene su función dentro del proceso de configuración. El comportamiento de estos paquetes es también de vital importancia para el análisis del protocolo, generándose la necesidad de hacer un estudio de cada una de las transacciones, así como del tiempo que le toma a cada cliente obtener sus parámetros de red.

De esta manera, se planeó realizar otras pruebas para diferentes grupos de equipos, empezando con un cliente y aumentando en igual cantidad hasta obtener un máximo de 14 estaciones solicitando parámetros. Se continuó usando el escenario de la figura 9, con la diferencia que el rango de direcciones del servidor fue ampliado para permitir realizar el número de asignaciones deseadas.

Los resultados de estas pruebas se muestran en la tabla 10, y como se puede apreciar, sólo se presentan los resultados hasta con 4 clientes, ya que en este punto se observó que las transacciones no se estaban llevando a cabo correctamente, es decir, la configuración de los clientes se estaba realizando con más de los 4 mensajes necesarios para este proceso, en ocasiones casi el doble; además el tiempo en el que cada cliente adquiría su configuración de red completamente era de aproximadamente 28,397 segundos, considerado demasiado alto, teniendo en cuenta que en la red de la universidad existen 1782 estaciones.

Tabla 10. Resultados de las pruebas de verificación del número de mensajes y tiempos de configuración.

No. De Equipos	Equipo	Tiempo (seg)		Mensajes				No. De Bytes Conf.
		Config. cliente	Promedio	Config.	Perdidos	Adicional	Total	
1	Equipo 1 192.168.45.4	29,258259	29,258259	7	0	0	7	**2406**
2	Equipo 1 192.168.45.4	25,151894	24,421099	6	0	0	12	2064
	Equipo 2 192.168.45.9	23,690304		6	0	0		2064
							TOTAL BYTES	**4128**
3	Equipo 1 192.168.45.4	30,225520	30,464066	7	0	0	21	2406
	Equipo 2 192.168.45.9	30,710348		7	0	0		2406
	Equipo 3 192.168.45.13	30,456332		7	0	0		2406
							TOTAL BYTES	**7218**
4	Equipo 1 192.168.45.4	27,115522	29,447637	7	0	0	28	2406
	Equipo 2 192.168.45.9	30,989984		7	0	0		1380
	Equipo 3 192.168.45.13	28,341222		7	0	0		1380
	Equipo 4 192.168.45.11	31,344122		7	0	0		1380
							TOTAL BYTES DE CONFIGURACION	**9624**

Fuente: Los autores.

Las columnas marcadas como “total mensajes” y “total bytes” se refieren al número total de mensajes y bytes con los que cada cliente obtuvo su

configuración, además, a continuación de los resultados de cada prueba se presenta el número total de mensajes y bytes que se aprecian en las capturas, así como un promedio de los tiempos de configuración de todos los clientes para cada prueba.

En este punto se había estimado el tráfico generado como la sumatoria de los mensajes en los clientes, pues según las capturas que se tomaron tanto en el servidor como en cada uno de los clientes, el número de mensajes de configuración (y por consiguiente el tráfico) en los clientes siempre resultaba superior al número de mensajes que el servidor registraba; según las capturas se creía que esta anormalidad se debía a que muchos de los mensajes DHCP Discover que el cliente enviaba en búsqueda de los servidores, no llegaban realmente a su destino: el servidor DHCP. Además también hubo otros mensajes que se repetían múltiples veces en cada cliente, generando retardos, ya que el cliente espera un tiempo considerable entre cada reenvío y esto ocasionaba los altos tiempos de configuración.

Después de un detallado estudio de los resultados, se llegó a una conclusión bastante desalentadora, que indicaba que se estaban presentando 3 graves problemas, los cuales debían ser corregidos antes de continuar con lo programado para el desarrollo de este proyecto, de lo contrario resultaría inútil cualquier estudio que se hiciera para la implementación del protocolo. A continuación se mencionan dichos problemas para tener así una mayor claridad acerca de éstos.

El primero de estos problemas, como ya se mencionó, eran los mensajes que los clientes enviaban pero que el servidor nunca recibía (en su gran mayoría eran DHCP Discover), por lo tanto el cliente se veía obligado a reenviar varias veces los mensajes al servidor, lo cual ocasionaba el segundo problema a mencionar en este listado.
El segundo, era el tiempo tan elevado en el que los equipos estaban realizando su configuración, aproximadamente 28,397 segundos por cliente,

un tiempo que estaba muy distante del que se había supuesto duraría este proceso de asignación, que debería ser menor a 1 segundo.

El tercero y no menos preocupante, era la aparición de todos los mensajes de configuración como mensajes de broadcast, si bien es cierto que los mensajes DHCP Discover y DHCP Request deben ir en broadcast, el DHCP offer y el DHCP ACK deben ir direccionados en unicast desde el servidor hacia el cliente.

Para poder dar solución a estos inconvenientes fue necesario plantear una metodología[24] que permitiera descartar paulatinamente cuales serían las posibles causas que los estarían originando; con el desarrollo de la misma se concluyó con plena seguridad que el switch Cajun P333R era el dispositivo que generaba los problemas descritos y se determinó suprimirlo de cualquier configuración con que se fueran a realizar futuras pruebas.

Los resultados obtenidos en los diferentes escenarios desarrollados con la estrategia implementada, especialmente donde el servidor y los clientes hacían parte de la red de datos institucional al conectarse directamente al switch P330T del Laboratorio de Alta Tensión, permitieron comprobar el correcto funcionamiento del servicio en cuanto a número de mensajes y tiempos de configuración, confirmando la buena elección del servidor para efectuar las pruebas de estimación y proyección de tráfico en la red de datos institucional.

[24] Para una descripción completa de la metodología desarrollada remitirse al Anexo C.

4. PRUEBAS PARA EL ANÁLISIS Y ESTIMACIÓN DEL TRÁFICO GENERADO POR EL SERVICIO

Después de realizar las pruebas necesarias para determinar que el servidor DHCP que ofrece Linux Red Hat 9.0 cumple con todas las características requeridas para la implementación del servicio en la red de datos institucional y que presenta un buen desempeño de sus prestaciones, se dio inicio a la obtención de la estimación del tráfico generado por las transacciones entre los clientes y el servidor, para lo cual fue necesario la ejecución de múltiples pruebas en diferentes escenarios.

Con las pruebas realizadas se pretendió analizar no sólo el tráfico que se generaba en diferentes segmentos de red dentro de la sede principal de la universidad, sino que también se quiso estudiar la manera en que se hacía la configuración de clientes en otros espacios físicos, para lo cual se llevó a cabo un conjunto de pruebas en las sedes del área metropolitana y las de los otros municipios del departamento.

4.1 PLANEACIÓN DE ESCENARIOS PARA LAS DIFERENTES PRUEBAS

Antes de dar inicio a la toma de muestras, fue necesario plantear los escenarios adecuados que permitieran obtener resultados acordes a lo que se espera sucederá al implementar el servicio en la red de datos de la universidad.

4.1.1 Definición de escenarios.

Basándose en el estudio previo realizado sobre el estado actual de la red de la universidad se plantearon 3 diferentes escenarios adecuados para realizar

las pruebas necesarias que permitirán determinar el tráfico generado por el servicio:

- El primero en implementarse es el más sencillo y con menos probabilidades de que exista en un entorno de red complejo como lo es el de la universidad, el cual consiste en la ubicación del servidor en el mismo segmento de red en el que se encuentran los clientes, haciendo innecesaria la intervención del agente DHCP relay.

- El segundo corresponde a llevar el servidor DHCP a un segmento de red diferente al que contiene los clientes que le harán solicitudes, para lo cual resulta indispensable tener el switch central configurado como agente relay[25] y que haga posible el intercambio de mensajes en cada transacción. Contrario al primer escenario, éste va a ser el más comúnmente implementado en la red de datos, por lo cual se les dará mayor énfasis a los resultados obtenidos en las pruebas que se realicen en él. Así mismo, serán éstos los que brinden mayor información para hallar la estimación de tráfico.

- El tercero y último consiste en efectuar la configuración del servidor de manera que permita otorgar los parámetros de red a clientes que se encuentren en otras sedes regionales y/o del área metropolitana y de esta manera deducir si la viabilidad de implementar el protocolo se extiende o no hasta la totalidad de sedes con que cuenta la universidad actualmente.

Al finalizar la toma de datos en estos 3 escenarios se tendrá información suficiente para realizar una estimación del tráfico generado por DHCP.

4.1.2 Definición de los clientes DHCP.

Para obtener una estimación del tráfico generado que estuviera de acuerdo con las características actuales de la red de datos de la universidad, se

[25] El procedimiento para llevar a cabo la configuración del switch Cajun P880 como agente relay ya fue expuesto en el capítulo 2, sección 2.4.3.

planteó la posibilidad de observar la forma en que clientes con diferentes sistemas operativos realizaban las transacciones con el servidor y si la longitud de los paquetes intercambiados durante este proceso es siempre igual sin importar el sistema operativo con que cuente el cliente DHCP; debido a esto se quiso llevar a cabo una serie de pruebas con clientes que trabajaran bajo los diferentes SO[26] que se encuentran en mayor proporción distribuidos en la red.

En la actualidad se estima que el 45% de los equipos conectados a la red de datos de la UIS, usan Windows XP; otro 45% opera con Windows 95 y Windows 98 (manteniendo Windows 98 la mayor parte de este porcentaje) y un 10% lo hace con diferentes SO, como Linux, Unix y otras versiones de Windows[27].

Al revisar los resultados obtenidos durante las pruebas de verificación, las cuales se realizaron con clientes que operaban bajo Windows XP, se observa que las longitudes de los mensajes DHCP son generalmente iguales. Estas longitudes se muestran en la tabla 11.

Tabla 11. Longitud de los mensajes de configuración.

MENSAJE	LONGITUD
DHCP Discover	342 Bytes
DHCP Offer	342 Bytes
DHCP Request	354 Bytes
DHCP ACK	342 Bytes

Fuente: Los autores.

Antes de proseguir, es importante recordar que para que un cliente pueda obtener su configuración de red automáticamente, es indispensable que en sus propiedades de conexión de área local mantenga seleccionadas las opciones que se lo permitirán. En el ANEXO D se presenta una completa

[26] SO: Sistema operativo.

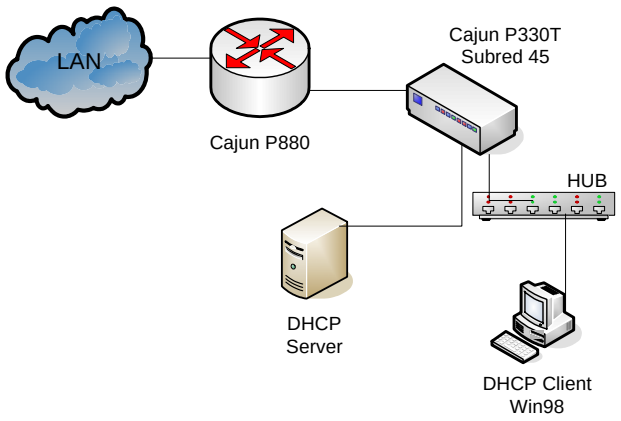
[27] Información proporcionada por la División de Servicios de Información (DSI) de la Universidad Industrial de Santander.

guía donde se indica el procedimiento a seguir para que una estación sea habilitada para obtener su configuración de red desde un servidor DHCP.

Una vez habilitado el cliente para que utilice el servicio DHCP y teniendo en cuenta las longitudes de los mensajes DHCP presentadas en la tabla 11, se ejecutó una prueba en la cual el cliente operaba bajo Windows 98, ya que después de Windows XP, éste es el SO más usado en las estaciones pertenecientes a la red de la universidad. Los otros SO fueron omitidos de las pruebas para estimación de tráfico, ya que las estaciones que operan bajo Linux o Unix son en su mayoría servidores o estaciones para fines específicos, a las cuales se recomienda seguir usando su configuración de red que les ha sido asignada estáticamente; mientras que las estaciones que trabajan con Windows 95 u otras versiones son sólo una pequeña cantidad del total de equipos que hacen parte de la red, consecuentemente el tráfico que generen por sus solicitudes va a ser mínimo comparado con el total.

En este orden de ideas se prosiguió con la ejecución de la prueba con el cliente Windows 98, para lo cual se implementó el esquema de red mostrado en la figura 12.

Figura 12. Esquema de red implementado para la toma de datos con clientes Windows 98.



Fuente: Los autores

Al examinar los resultados de esta prueba, se comprobó que la transacción y todas sus características eran similares a las que se observaron en los clientes con Windows XP, ya que se vieron los 4 mensajes de configuración y sus longitudes eran idénticas a las observadas para clientes Windows XP. Los resultados para esta prueba se muestran en la tabla 12.

Tabla 12. Resultados obtenidos en la configuración de un cliente Windows 98.

N° EQUIPOS	TIEMPO		MENSAJES		BYTES	
	Total	Config.	Total	Config.	Total	Config.
1	0,698	0,698	4	4	1380	1380

Fuente: Los autores.

Debido a que con 1 cliente Windows 98 se genera el mismo tráfico que con 1 cliente Windows XP, se decidió realizar la totalidad de pruebas subsiguientes con clientes Windows XP, además, este SO presenta mayores facilidades en su procedimiento de configuración.

4.1.3 Definición del servidor y otros aspectos.

En el capítulo 3 ya se dedicó gran esfuerzo a la selección y estudio del servidor a utilizar en estas pruebas, por lo tanto no se hará más énfasis al respecto.

Sin embargo, es necesario aclarar el manejo que se hizo al archivo de configuración (dhcpd.conf) durante la ejecución de estas pruebas en cada escenario definido:

Para las pruebas que se realizaron en un mismo segmento de red, el servidor se configuró en un equipo Optiplex GX 260 marca Dell, con procesador Pentium 4 de 2.4 Ghz y 512 MB de memoria RAM. En el archivo de configuración se definió únicamente la subred[28] en la que se iban a hacer las asignaciones dinámicas, para la cual se destinó un rango de 10

[28] Las pruebas en un solo segmento se realizaron en la subred 192.168.45.0, la cual corresponde a la subred del laboratorio de Redes de Computadores, aula 201 del Laboratorio de Alta Tensión

direcciones IP, teniendo siempre la precaución de que éstas no coincidieran con otras ya configuradas estáticamente en cualquier equipo de la subred.

Las pruebas en las cuales era necesario mantener el servidor en una subred diferente a la que contenía los clientes DHCP, se llevaron a cabo ubicando el servidor en la subred 19, mientras que los clientes fueron ubicados en diferentes subredes de la LAN (principalmente la subred 192.168.45.0). El equipo que se utilizó para montar el servidor es un PowerEdge 400 SC marca Dell, con procesador Pentium 4 de 2,8 Ghz y memoria RAM de 1024 MB, con sistema operativo Linux Red Hat 9.0, el cual también presta el servicio FTP[29] a usuarios registrados. Cada vez que se iba a realizar una prueba en una nueva subred, la información correspondiente era introducida al archivo de configuración del servidor DHCP y seguidamente el servicio era reiniciado.

Algunas de estas pruebas se realizaron utilizando asignación dinámica de direcciones y para otras se usó la asignación manual, sin embargo, en adelante, para los resultados que se presenten se asumirá que éstos fueron obtenidos haciendo asignación dinámica. Cuando los resultados sean obtenidos por asignación manual, entonces se dará a conocer.

Así mismo, es importante resaltar que las pruebas generalmente fueron realizadas desactivando y activando la interfaz de red de cada equipo, lo cual hace que éste ejecute un proceso que le permite borrar y luego actualizar su memoria caché, por lo tanto el equipo vuelve a realizar el procedimiento completo de solicitud cada vez que se active su conexión de esta manera. Cuando las pruebas se lleven a cabo de otra manera, será especificado en esa instancia.

En varias ocasiones el servidor DHCP fue administrado remotamente, por medio de una herramienta SSH[30], otorgando movilidad por toda la LAN al

[29] FTP, File Transfer Protocol.
[30] Esta herramienta es un cliente SSH (Secure Shell) llamado PuTTY, que al ser instalado y ejecutado en cualquier estación dentro de la LAN, permite establecer una conexión remota

administrador del servidor durante la realización de las pruebas y brindando alta seguridad en la conexión.

Las pruebas ejecutadas en uno y varios segmentos de red, se llevaron a cabo de manera que se pudiera obtener un patrón de comportamiento de los diferentes parámetros como los son los tiempos y bytes de configuración de los clientes, para esto fue necesario que las pruebas se realizaran varias veces y en cada una el número de clientes era incrementado en 1, teniendo como límite inferior 1 cliente, hasta un máximo de 6. En algunos casos y por diferentes circunstancias, no se llevó a cabo esta metodología, sin embargo cuando sea el caso se hará conocer el número de clientes con que se obtuvieron los resultados

Teniendo claridad sobre los escenarios que se van a implementar durante las diferentes pruebas y las características de cada entidad involucrada, se proseguirá con la exposición de los resultados obtenidos.

4.2 PRUEBAS DE TRÁFICO EN UN SEGMENTO DE RED

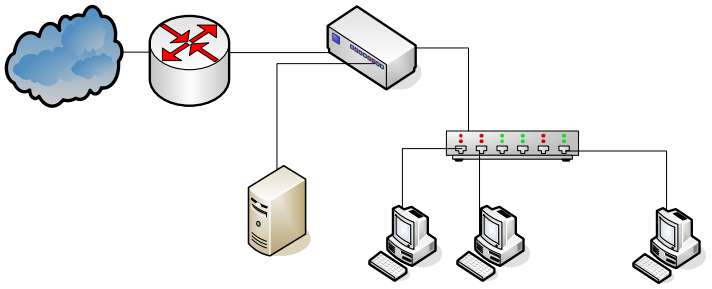
4.2.1 Primera Prueba.

El primer esquema de red implementado para estas pruebas se muestra en la figura 13, sin embargo, antes de continuar es conveniente mencionar que no se hará -un estudio detallado de los resultados obtenidos en estas pruebas, ya que no se hallará la estimación del tráfico generado por las solicitudes, esto debido a que el escenario de ejecución no representa la situación real en que se va a realizar la implementación del servicio en la red de la universidad.

---

utilizando RSA como algoritmo de llave asimétrica, brindando así mayor seguridad en la conexión.

Figura 13. Esquema de red utilizado en la primera prueba.



Fuente: Los autores

Los resultados obtenidos se muestran en la tabla 13, los cuales estuvieron de acuerdo con lo especificado en la teoría del protocolo, porque como se puede observar, en todos los casos las transacciones se llevaron a cabo con el número de mensajes necesario para la configuración y en tiempos adecuados, esto debido a que en ningún caso se vieron pérdidas ni repeticiones de mensajes.

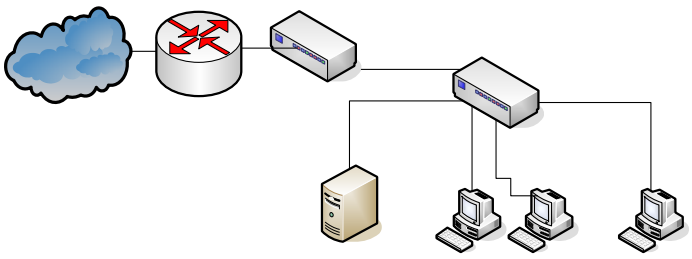
Tabla 13. Resultados obtenidos en la primera prueba.

N° EQUIPOS	TIEMPO		MENSAJES				BYTES	
	Promedio	Config.	Total	Config.	Perdidos	Repetidos	Total	Config.
1	0,687	0,687	4	4	0	0	1380	1380
2	0,332172	0,546963	8	4	0	0	2760	1380
		0,11738		4	0	0		1380
3	0,534038	0,549053	12	4	0	0	4140	1380
		0,604522		4	0	0		1380
		0,44854		4	0	0		1380
4	0,606669	0,894417	16	4	0	0	5520	1380
		0,60104		4	0	0		1380
		0,529931		4	0	0		1380
		0,401287		4	0	0		1380
5	0,515542	0,74123	20	4	0	0	6900	1380
		0,412563		4	0	0		1380
		0,542581		4	0	0		1380
		0,22546		4	0	0		1380
		0,655877		4	0	0		1380
6	0,520727	0,424092	24	4	0	0	8280	1380
		0,593862		4	0	0		1380
		0,542357		4	0	0		1380
		0,136543		4	0	0		1380
		0,837155		4	0	0		1380
		0,590354		4	0	0		1380

4.2.2 Segunda Prueba.

Se realizó otra prueba similar a la anterior, pero esta vez no se utilizó un hub, sino que el servidor y los clientes fueron conectados a un switch no administrable marca Planet[31] y éste a su vez iba conectado al switch departamental del edificio Eléctrica Antigua. La figura 14 muestra este escenario, el cual es también un esquema de red muy comúnmente utilizado en la red de datos de la UIS.

Figura 14. Esquema de red implementado en la segunda prueba.



Fuente: Los autores

El objetivo principal de esta prueba era verificar si debido a la intermediación de un dispositivo activo de capa 2 en el proceso de configuración se introducía algún aumento en los tiempos que se obtuvieron en la primera prueba, en la que se implementó un hub, el cual debido a su propio funcionamiento no le introduce ningún retardo al reenvío de paquetes; sin embargo, los resultados obtenidos demuestran que la implementación de otros switches no representa aumento alguno en el tiempo que demoran los clientes en obtener su configuración. Estos resultados se presentan en la tabla 14.

LAN

Cajun P880

[31] Switch Planet Modelo FSD-8080, posee 8 Puertos RJ-45 de 100Mbps (100Base-TX), propiedad de la Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones de la UIS.

Tabla 14. Resultados obtenidos en la segunda prueba.

N° EQUIPOS	TIEMPO		MENSAJES				BYTES	
	Promedio	Config.	Total	Config.	Perdidos	Repetidos	Total	Config.
1	0,5351	0,5351	4	4	0	0	1380	1380
2	0,485772	0,323539	8	4	0	0	2760	1380
		0,648004		4	0	0		1380
3	0,637182	0,693291	12	4	0	0	4140	1380
		0,762031		4	0	0		1380
		0,456225		4	0	0		1380
4	0,466052	0,593476	16	4	0	0	5520	1380
		0,67911		4	0	0		1380
		0,588934		4	0	0		1380
		0,002689		4	0	0		1380
5	0,613892	0,475695	20	4	0	0	6900	1380
		0,668917		4	0	0		1380
		0,747415		4	0	0		1380
		0,427648		4	0	0		1380
		0,749785		4	0	0		1380
6	0,466506	0,676309	24	4	0	0	8280	1380
		0,282149		4	0	0		1380
		0,637476		4	0	0		1380
		0,207376		4	0	0		1380
		0,277141		4	0	0		1380
		0,718585		4	0	0		1380

Fuente: Los autores.

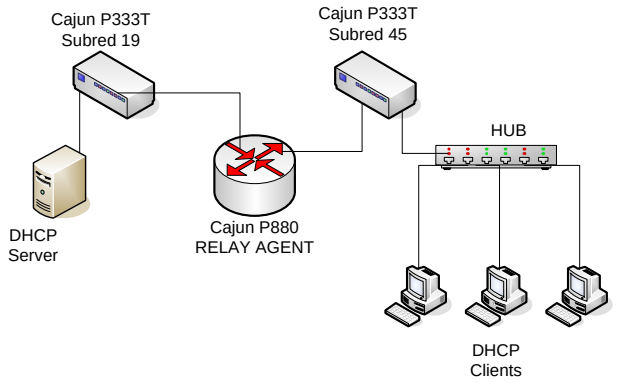
Al comparar los resultados de las dos pruebas anteriores, se pudo comprobar que para ambos esquemas la longitud de los mensajes es la misma, teniendo en cuenta que los mensajes DHCP Discover, DHCP Offer y DHCP ACK tienen una longitud de 342 Bytes cada uno, mientras que el DHCP Request presenta una longitud de 354 Bytes.

4.3 PRUEBAS DE TRÁFICO EN DIFERENTES SEGMENTOS DE RED

4.3.1 Tercera prueba.

Para iniciar el estudio del tráfico que se genera por el servicio cuando el servidor y los clientes se encuentran en diferentes subredes, se realizó una prueba utilizando el esquema de red mostrado en la figura 15, el cual presenta una estructura bastante sencilla pero al mismo tiempo muy común dentro de las implementaciones que se encuentran actualmente en la red de la universidad.

Figura 15. Esquema de red utilizado durante la tercera prueba.



Fuente: Los autores

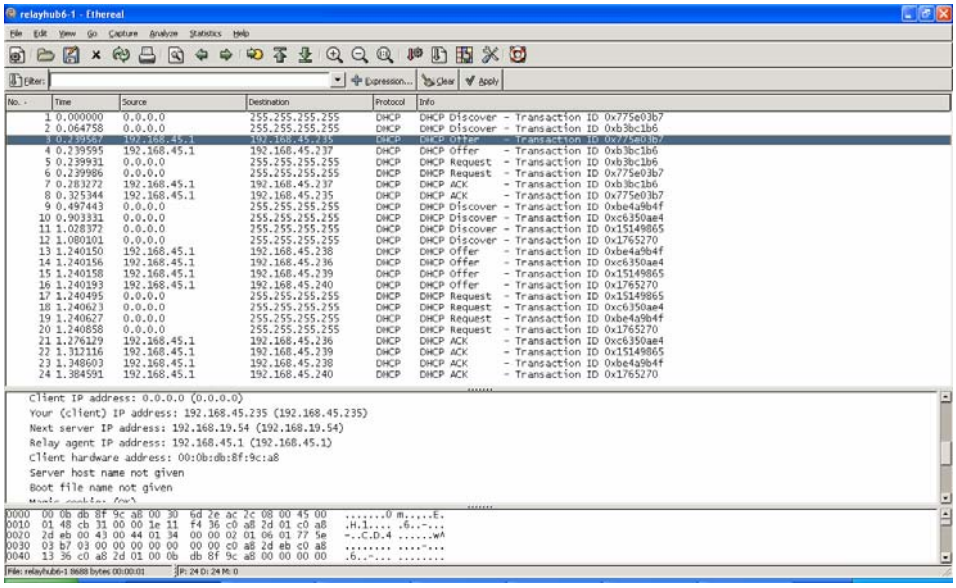
Los resultados a estas pruebas se muestran en la tabla 15, en la cual se puede constatar que no se presentó pérdida ni repetición de mensajes, por lo cual estos resultados se consideraron aptos para continuar con este estudio que permitió hallar la estimación del tráfico que se genera por DHCP.

Tabla 15. Resultados obtenidos en la tercera prueba.

No. De equipos	Tiempo		Mensajes				Bytes	
	Promedio	Config.	Total	Config.	Perdidos	Repetidos	Total	Config.
1	0,413476	0,413476	4	4	0	0	1380	1380
2	0,619201	0,299865	8	4	0	0	2760	1380
		0,938536		4	0	0		1380
3	0,58345	0,103641	12	4	0	0	4140	1380
		0,629739		4	0	0		1380
		1,016971		4	0	0		1380
4	0,597686	0,659631	16	4	0	0	5520	1380
		0,517995		4	0	0		1380
		0,665647		4	0	0		1380
		0,547471		4	0	0		1380
5	0,4994	0,408836	20	4	0	0	6900	1380
		0,45727		4	0	0		1380
		0,402985		4	0	0		1380
		0,477892		4	0	0		1380
		0,750019		4	0	0		1380
6	0,392675	0,325344	24	4	0	0	8280	1380
		0,218514		4	0	0		1380
		0,85116		4	0	0		1380
		0,372798		4	0	0		1380
		0,283744		4	0	0		1380
		0,30449		4	0	0		1380

En las capturas de Ethereal fue posible chequear las opciones DHCP que se envían en los mensajes, tales como la dirección IP, la máscara de subred, el tiempo de lease, entre otras. Además, se observó la influencia del agente relay en las transacciones, ya que en las diferentes capturas se registró que cuando los clientes reciben los mensajes de su configuración, la dirección que aparece como fuente o emisora de dichos mensajes no es la dirección del servidor, sino la dirección de la interfaz asociada en el agente relay para esa subred. Sin embargo al revisar el contenido de las cabeceras se comprobó que sí se envía la dirección IP del servidor, la cual es utilizada por el cliente como un medio para identificar el servidor DHCP que le asignó su configuración. La figura 16 muestra una captura en la que se puede apreciar la situación mencionada anteriormente.

Figura 16. Captura tomada con Ethereal durante la ejecución de la tercera prueba.



Fuente: Los autores.

4.3.2 Revalidación de los resultados.

Los resultados obtenidos hasta este punto son altamente satisfactorios y confirman la alta capacidad de soporte para DHCP de los clientes Windows XP; sin embargo, fue necesario ejecutar una prueba de revalidación que

permitiera demostrar que dichos resultados representaban argumentos suficientemente sólidos para efectuar la estimación del tráfico.

Basándose en el escenario definido en la figura 15, se ejecutó 15 veces la prueba para 6 clientes, con el fin de establecer si existe alguna tendencia en los datos obtenidos. Los resultados a esta prueba se muestran en la tabla 16.

Tabla 16. Resultados obtenidos en las pruebas de revalidación con el esquema de red de la figura 15.

Muestra No.	Tiempo		Mensajes				Bytes	
	Promedio	Config.	Total	Config.	Perdidos	Repetidos	Total	Config.
1	0,384795	0,356694	24	4	0	0	8280	1380
		0,457124		4	0	0		1380
		0,422125		4	0	0		1380
		0,256246		4	0	0		1380
		0,403622		4	0	0		1380
		0,412959		4	0	0		1380
2	0,440872	0,446124	24	4	0	0	8280	1380
		0,426898		4	0	0		1380
		0,213561		4	0	0		1380
		0,47471		4	0	0		1380
		0,663942		4	0	0		1380
		0,419997		4	0	0		1380
3	1,070795	0,64104	27	4	0	0	9306	1380
		0,587424		4	0	0		1380
		0,664482		4	0	0		1380
		0,515582		4	0	0		1380
		3,328713		7	2	1		2406
		0,687529		4	0	0		1380
4	0,548423	0,498361	24	4	0	0	8280	1380
		0,65607		4	0	0		1380
		0,515171		4	0	0		1380
		0,617731		4	0	0		1380
		0,6136		4	0	0		1380
		0,389604		4	0	0		1380
5	0,407581	0,49927	24	4	0	0	8280	1380
		0,589072		4	0	0		1380
		0,388333		4	0	0		1380
		0,183963		4	0	0		1380
		0,302571		4	0	0		1380
		0,482279		4	0	0		1380

6	0,646151	0,530252	24	4	0	0	8280	1380
		0,571105		4	0	0		1380
		0,823589		4	0	0		1380
		0,597791		4	0	0		1380
		0,474993		4	0	0		1380
		0,879176		4	0	0		1380
7	0,564342	0,529792	24	4	0	0	8280	1380
		0,610027		4	0	0		1380
		0,522225		4	0	0		1380
		0,401527		4	0	0		1380
		0,692607		4	0	0		1380
		0,629874		4	0	0		1380
8	0,593553	0,546323	24	4	0	0	8280	1380
		0,578662		4	0	0		1380
		1,040609		4	0	0		1380
		0,434827		4	0	0		1380
		0,249263		4	0	0		1380
		0,711633		4	0	0		1380
9	0,455213	0,899152	24	4	0	0	8280	1380
		0,571015		4	0	0		1380
		0,64197		4	0	0		1380
		0,235147		4	0	0		1380
		0,163673		4	0	0		1380
		0,220318		4	0	0		1380
10	0,115548	0,462698	24	4	0	0	8280	1380
		0,08583		4	0	0		1380
		0,031946		4	0	0		1380
		0,041563		4	0	0		1380
		0,036466		4	0	0		1380
		0,034783		4	0	0		1380
11	0,480515	0,70379	24	4	0	0	8280	1380
		0,72102		4	0	0		1380
		0,043823		4	0	0		1380
		0,217649		4	0	0		1380
		1,052089		4	0	0		1380
		0,144718		4	0	0		1380
12	0,208208	0,345345	24	4	0	0	8280	1380
		0,194819		4	0	0		1380
		0,154579		4	0	0		1380
		0,24223		4	0	0		1380
		0,218153		4	0	0		1380
		0,094121		4	0	0		1380
13	0,546534	0,825023	24	4	0	0	8280	1380
		0,752808		4	0	0		1380
		0,470381		4	0	0		1380
		0,133929		4	0	0		1380
		0,107716		4	0	0		1380

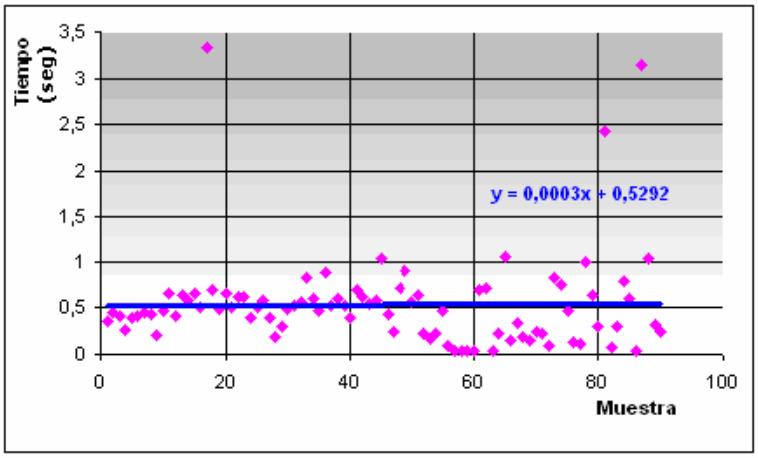
		0,989348		4	0	0		1380
14	0,754337	0,638933	27	4	0	0	9306	1380
		0,30629		4	0	0		1380
		2,420796		7	2	1		2406
		0,075591		4	0	0		1380
		0,298403		4	0	0		1380
		0,786011		4	0	0		1380
15	0,899221	0,604497	27	4	0	0	9306	1380
		0,042394		4	0	0		1380
		3,147782		7	2	1		2406
		1,041058		4	0	0		1380
		0,313718		4	0	0		1380
		0,245878		4	0	0		1380

Fuente: Los autores.

Como se puede observar, en las muestras 3, 14 y 15 se presentaron 2 mensajes perdidos y 1 repetido durante el proceso de configuración de un cliente, aún así, se determinó que este hecho no representa un incremento considerable en el tráfico total que se genera. Además, los tiempos de configuración que mostró cada cliente están de acuerdo con lo esperado.

Con la información contenida en la tabla 16 se construyó una serie de gráficas que permitieron analizar el comportamiento de los diferentes parámetros. La primera de ellas corresponde a la variación del tiempo de configuración para cada cliente (figura 17).

Figura 17. Variación de los tiempos de configuración en la prueba de revalidación.

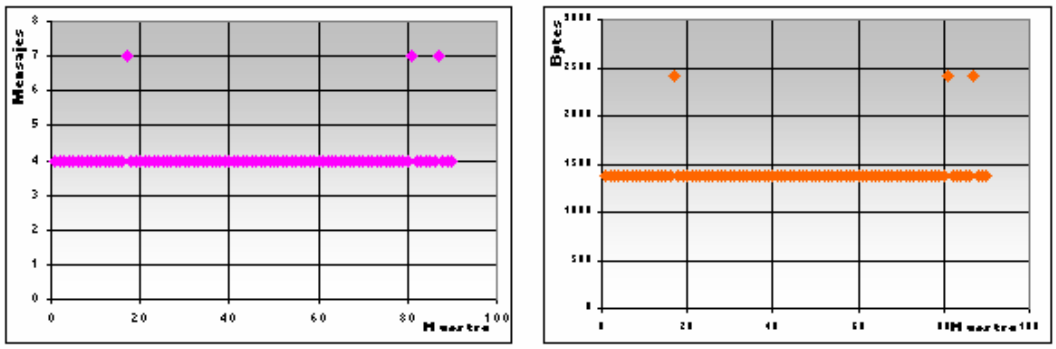


Fuente: Los autores.

Los tiempos de configuración en las diferentes muestras se mantuvieron dentro del rango definido por los 0.031946 y 3.328713 segundos. La gráfica en azul corresponde a la tendencia lineal de los valores de tiempo obtenidos y de acuerdo a su ecuación es posible afirmar que cada cliente toma en promedio **0.5292 segundos** en obtener su configuración, ya que la pendiente de la recta puede ser despreciada, haciendo así que este tiempo presente un valor constante.

Por otro lado, se analizaron las variaciones en la cantidad de mensajes y la longitud de éstos para observar el comportamiento de dichos parámetros, estas gráficas se muestran en la figura 18.

Figura 18. Variación de mensajes y su longitud en las pruebas de revalidación.



Fuente: Los autores

Como ya se había notado, sólo en 3 oportunidades el número de mensajes (y por consiguiente de bytes) superó el valor normal que deberían registrar las capturas, esto como consecuencia de los mensajes de configuración que se repitieron y los que se perdieron, los cuales comparados con el total de muestras, representan sólo el 3.3%.

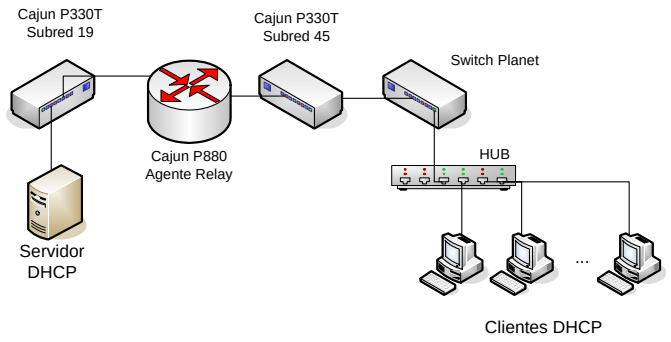
Los anteriores resultados proporcionaron información que permitió evidenciar que los datos presentados en la tabla 16 son apropiados para realizar la estimación del tráfico que se generará con el servicio DHCP en la

red de datos institucional. De esta manera se puede extender este comportamiento a las diferentes pruebas, teniendo certeza sobre la generalidad de los resultados.

4.3.3 Cuarta Prueba.

Al igual que en las pruebas que se realizaron en un segmento de red, para esta parte también se ejecutó una prueba en la cual se incluyó un switch no administrable marca Planet para observar si se daba algún incremento en los tiempos de configuración. La figura 19 muestra el esquema de red implementado.

Figura 19. Esquema de red implementado para la ejecución de la cuarta prueba.



Fuente: Los autores

Esta prueba sólo se realizó para un máximo de 4 clientes, ya que con esta cantidad fue suficiente para demostrar que los tiempos de configuración obtenidos son bastante próximos a los mostrados en las tablas 15 y 16. Los resultados se presentan en la tabla 17.

Tabla 17. Resultados obtenidos en la ejecución de la cuarta prueba.

No. De equipos	Tiempo		Mensajes				Bytes	
	Promedio	Config.	Total	Config.	Perdidos	Repetidos	Total	Config.
1	0,586113	0,586113	4	4	0	0	1380	1380
2	0,13448	0,199648	8	4	0	0	2760	1380
		0,069311		4	0	0		1380
3	0,407438	0,609458	12	4	0	0	4140	1380
		0,497337		4	0	0		1380
		0,11552		4	0	0		1380

4	0,77009	0,616739	16	4	0	0	5520	1380
		0,729357		4	0	0		1380
		0,955783		4	0	0		1380
		0,778482		4	0	0		1380

Fuente: Los autores.

Los resultados obtenidos hasta esta instancia han sido favorables para suponer la viabilidad de la implementación del servicio, teniendo en cuenta que con la desactivación y activación de la interfaz de red se hace todo el proceso de obtención de parámetros.

La concesión otorgada a los clientes se presenta cuando éstos solicitan el servicio por primera vez, pues aunque liberan los parámetros al apagarse, realizan renovación de los mismos al ser encendidos. A continuación se estudiará el tráfico generado por las renovaciones de configuración que efectúan los clientes al ser encendidos.

4.4 TRÁFICO GENERADO AL ENCENDER LAS ESTACIONES CLIENTE

En un escenario como el que se muestra en la figura 15, cuando se reinician las estaciones cuyos clientes DHCP han obtenido previamente su configuración de red, se realiza la renovación de sus parámetros de red al tiempo en que el cliente carga su configuración del sistema, consiguiendo así un nuevo lease que le permitirá iniciar su operación en la red. Para esto, el cliente envía al servidor un mensaje DHCP Request que contiene la configuración de red asignada previamente y si ésta aún es válida para el cliente, el servidor le reconfirma con un mensaje DHCP ACK.

Para verificar que este proceso de renovación se llevara a cabo adecuadamente, se realizó un conjunto de pruebas, las cuales consistieron en encender simultáneamente los mismos clientes a los cuales les había sido asignada una configuración de red desde el servidor DHCP ubicado en la subred 192.168.19.0. La tabla 18 expone los resultados obtenidos.

Tabla 18. Resultados obtenidos al encender los equipos cliente.

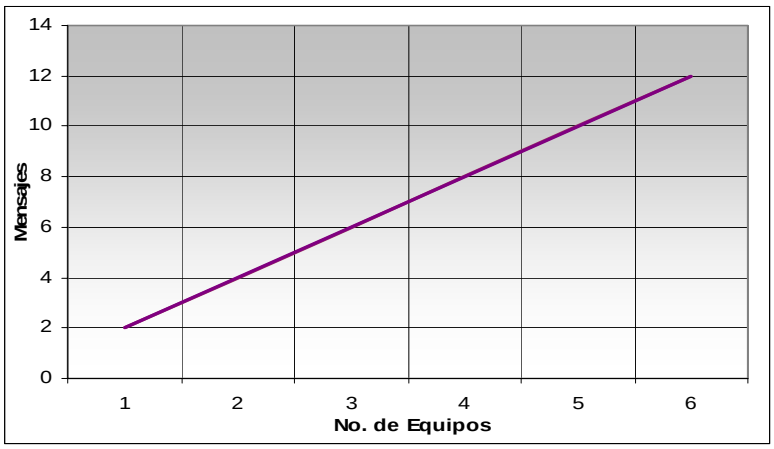
N° de equipos		TIEMPO		MENSAJES		BYTES	
		Promedio	Renovación	Total	Renovación	Total	Renovación
1		**0,02163**	0,02163	2	2	690	690
2	1	**0,04582**	0,05983	4	2	1380	690
	2		0,03181		2		690
3	1	**0,03355**	0,02941	6	2	2070	690
	2		0,01726		2		690
	3		0,0173		2		690
4	1	**0,02516**	0,02308	8	2	2760	690
	2		0,03623		2		690
	3		0,01946		2		690
	4		0,02188		2		690
5	1	**0,02232**	0,02797	10	2	3450	690
	2		0,02066		2		690
	3		0,02043		2		690
	4		0,02065		2		690
	5		0,02187		2		690
6	1	**0,02211**	0,01923	12	2	4140	690
	2		0,02564		2		690
	3		0,02262		2		690
	4		0,021158		2		690
	5		0,019685		2		690
	6		0,024344		2		690

Fuente: Los autores.

Los valores registrados para los tiempos de renovación se presentan de 2 maneras diferentes. La columna “renovación” hace referencia al tiempo que le tomó a cada cliente llevar a cabo el proceso de renovación, mientras que la columna “promedio” se refiere al promedio de tiempo en el que los clientes realizaron la renovación de su configuración en cada prueba, es importante aclarar que este tiempo no equivale al tiempo total que se observó en las capturas, ya que no se consideró apto para ningún tipo de análisis debido a que depende del tiempo que se toma cada estación en iniciar.

De esta manera se obtuvo la gráfica que demuestra la relación existente entre los mensajes generados y el número de clientes. En la figura 20 se muestra dicha gráfica.

Figura 20. Relación entre los mensajes y el número de clientes al ser encendidos.



Fuente: Los autores.

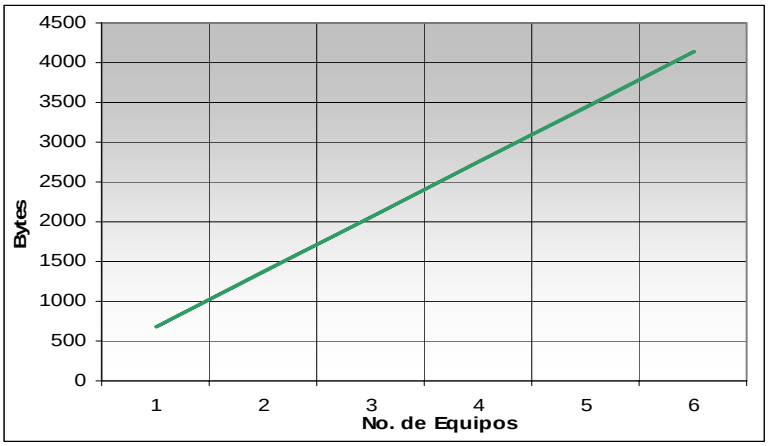
La ecuación que define la anterior recta es

$$y = 2 * x$$

Y demuestra el crecimiento lineal que presenta el tráfico ocasionado por las renovaciones de los clientes DHCP.

El aspecto de mayor importancia para este análisis es la longitud de los mensajes de renovación. De esta manera, se observó que el DHCP Request presenta una longitud equivalente a 348 Bytes y el DHCP ACK una de 342, así que la carga total que un solo cliente le añade al tráfico en la red es de 690 Bytes por renovación, una cantidad aceptable para poder afirmar desde ya, que el tráfico total que se agrega a la red por el servicio DHCP no será tan significativo. Teniendo en cuenta lo anterior, se halló la relación entre los bytes de las transacciones y el número de clientes, la figura 21 muestra dicha relación.

Figura 21. Relación entre bytes y número de clientes al ser encendidos.



Fuente: Los autores.

Como era de esperarse después de analizar la figura 20, la relación entre bytes y número de clientes también resultó completamente lineal y está definida por la siguiente ecuación

$$y = 690 * x$$

Una vez obtenidas las ecuaciones de las relaciones que definen el tráfico que se introduce a la red por el servicio y habiendo dejado en claro las circunstancias bajo las cuales se hicieron las pruebas anteriores y la validez de las mismas, se tuvo la suficiente información para poder hacer la estimación del tráfico. Sin embargo, antes de hallar esta estimación se realizaron unas últimas pruebas en las cuales se utilizó la asignación manual de direcciones.

4.5 PRUEBA USANDO ASIGNACIÓN MANUAL DE DIRECCIONES

El principal objetivo planteado para la ejecución de esta prueba, fue verificar si la longitud de los mensajes intercambiados entre un cliente y el

servidor, seguía manteniéndose en el mismo valor al utilizar la asignación manual.

Esta prueba se llevó a cabo en un esquema de red como el que se muestra en la figura 15, pero esta vez en el archivo de configuración se hizo una declaración de host para el cliente al cual se le iba a asignar la dirección IP de acuerdo a su dirección física. La tabla 19 presenta los resultados que se obtuvieron en esta prueba.

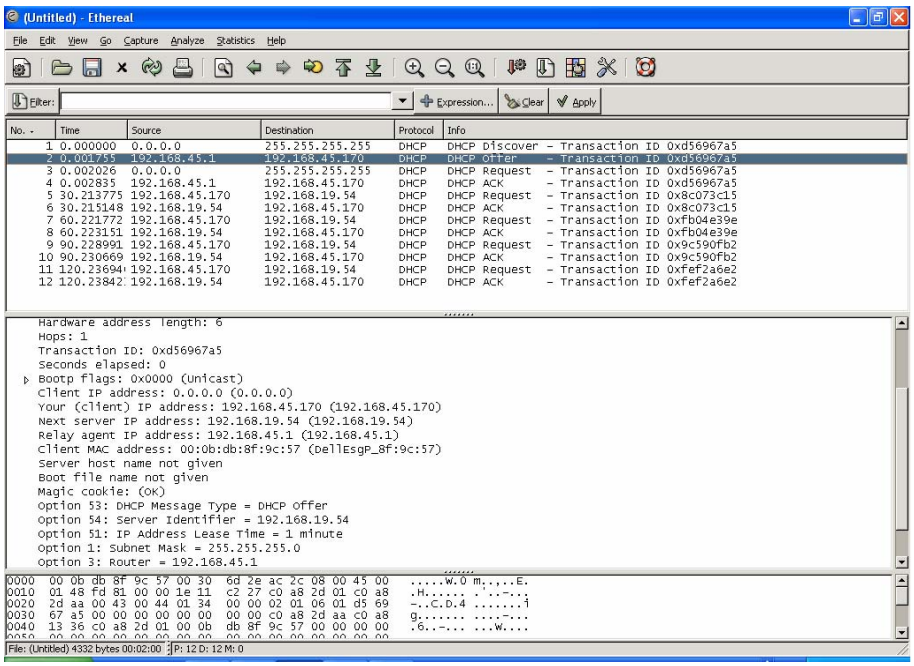
Tabla 19. Resultados al hacer asignación manual a un cliente DHCP.

N° EQUIPOS	TIEMPO		MENSAJES		BYTES	
	Total	Config.	Total	Config.	Total	Config.
1	0.002835	0.002835	4	4	1380	1380

Fuente: Los autores.

La captura realizada con Ethereal para esta prueba es mostrada en la figura 22.

Figura 22. Captura de la prueba con asignación manual.



Fuente: Los autores.

Como se puede observar, las longitudes de los mensajes se mantuvieron en los mismos valores que se dieron para la asignación dinámica, confirmando así que la estimación de tráfico que se halle es totalmente independiente del tipo de asignación que se utilice.

4.6 ESTIMACIÓN DEL TRÁFICO GENERADO POR EL SERVICIO DHCP

Para hallar el incremento de tráfico, se decidió trabajar únicamente con los resultados obtenidos en las pruebas que se hicieron con el servidor y los clientes en diferentes segmentos de red, ya que éstos representan de manera más aproximada la forma en que se llevarían a cabo las solicitudes y renovaciones al implementar el servicio DHCP en la red institucional.

4.6.1 Tráfico generado por las concesiones.

Con base en los resultados presentados en las tablas 15 y 16, fue posible estimar el tráfico generado por las concesiones a los clientes DHCP. Los valores obtenidos para un solo cliente y que permitirán hallar la proyección general del servicio son:

Mensajes de configuración: **4** [1]
Bytes de configuración: **1380** [2]

Considerando que a la red se encuentran conectadas cerca de 1782[32] estaciones, se puede afirmar que si todas hicieran la solicitud de sus configuraciones al servidor DHCP, se generarían los siguientes totales:

Mensajes de configuración: **7128** [3]
Bytes de configuración: **2459160 (2.46 MB aprox.)** [4]

[32] Ver ANEXO A.

Para poder hallar el ancho de banda consumido por la prestación del servicio, es necesario definir diferentes intervalos de tiempo que describan cómo se repartirá la cantidad de tráfico que genera el servicio cuando se efectúan las concesiones.

La tabla 20 muestra los valores de ancho de banda consumido por las transacciones del servicio para diferentes intervalos de tiempo.

Tabla 20. Anchos de banda consumidos por las concesiones en diferentes intervalos de tiempo.

Intervalo de Tiempo (seg)	Ancho de Banda (Kbps)
60	327,488
300	65,4976
600	32,7888
900	21,8592
1800	10,9296
3600	5,4648

Fuente: Los autores.

Como se observa, en la medida que el intervalo de encendido de los clientes aumenta, la capacidad del canal empleado para el servicio DHCP disminuye. Teniendo en cuenta que la red de datos institucional posee un ancho de banda de 100 Mbps o 1000 Mbps, es válido afirmar que la cantidad de tráfico adicionada no es significativa. Las situaciones descritas en la tabla 20, tienen alta probabilidad de presentarse, ya que generalmente las estaciones cliente no son encendidas con alto grado de sincronización.

A continuación se hallará la estimación del tráfico generado por las renovaciones de los clientes cuando son encendidos o cuando su tiempo de lease vence; éste es el tráfico al que se le debe prestar mayor atención en su estudio, ya que será el que más se presente cuando el servicio se encuentre implementado.

4.6.2 Tráfico generado por las renovaciones.

Teniendo en cuenta los resultados mostrados en la tabla 18, se puede hallar una estimación del tráfico generado por las renovaciones que hacen los clientes al ser encendidos. Para la renovación de configuración efectuada por un cliente DHCP se obtuvo la siguiente información:

Mensajes de renovación: **2** [5]
Bytes de renovación: **690** [6]

Si el total de clientes de la red de datos institucional hiciera renovación de su configuración al servidor DHCP se generarían los siguientes totales:

Mensajes de renovación: **3564** [7]
Bytes de renovación: **1229580 (1.23 MB aprox.)** [8]

Si se comparan estos valores con los obtenidos en la estimación de tráfico de las concesiones, es decir, los valores [3] y [4], es evidente que los de las renovaciones son exactamente la mitad, lo que asegura que el tráfico normal de la red no va a ser incrementado en grandes cantidades debido a las renovaciones de parámetros de los clientes DHCP.

Además, teniendo en cuenta que los clientes generalmente realizarán renovación, es necesario destacar el tiempo que emplea un cliente en ejecutar dicho proceso; de acuerdo con los valores presentados en la tabla 18, un cliente necesita en promedio 0,02843 segundos para renovar su configuración de red; entonces, asumiendo que el total de clientes se encendiera simultáneamente y considerando que por colisiones o por efectos de carga de la red de datos, cada estación debería esperar que la otra terminase la tarea para poder renovar, el tiempo total empleado sería:

Tiempo de renovación del total de clientes DHCP:
50,66226 segundos [9]

Suponiendo que en este tiempo se realizaran todas las transacciones de los clientes, al relacionarse los valores [8] y [9], la estimación de tráfico sería:

196732,8 bps o 196,732 Kbps [10]

El anterior es un valor moderado que representa el tráfico que se obtendría bajo condiciones normales de funcionamiento, si se diera la implementación del servicio. Sin embargo, si se desearan conocer los valores de ancho de banda consumido por las renovaciones bajo los mismos escenarios planteados en la sección 4.6.1, sería necesario obviar el tiempo definido en [9] y hallarlos para los diferentes intervalos de tiempo establecidos. La tabla 21 muestra estas ponderaciones.

Tabla 21. Anchos de Banda ocupados por las renovaciones en diferentes intervalos de tiempo.

Intervalo de Tiempo	Ancho de Banda (Kbps)
60	163,944
300	32,7888
600	16,3944
900	10,9296
1800	5,4648
3600	2,7324

De acuerdo al valor [10] y a los mostrados en la tabla anterior, se puede afirmar con gran certeza que la viabilidad de la implementación de DHCP en la red de datos de la UIS es plena, si se considera el tráfico generado y los tiempos de configuración que se presentan por el servicio.

4.7 CONSIDERACIONES PARA LA IMPLEMENTACION EN OTRAS SEDES DE LA UNIVERSIDAD

Según la estimación de tráfico que se obtuvo, es fácil comprender que desde el punto de vista de tráfico y tiempo de configuración, la

implementación del protocolo es viable. Resulta ahora indispensable hacer ciertas consideraciones para conocer si esta viabilidad se extiende a otras sedes de la universidad.

4.7.1 Sedes del área metropolitana.

Como se mencionó en el capítulo 2, la Universidad Industrial de Santander cuenta actualmente con 3 sedes ubicadas en diferentes puntos de la ciudad de Bucaramanga, las cuales se encuentran interconectadas con la sede principal por medio de fibra óptica.

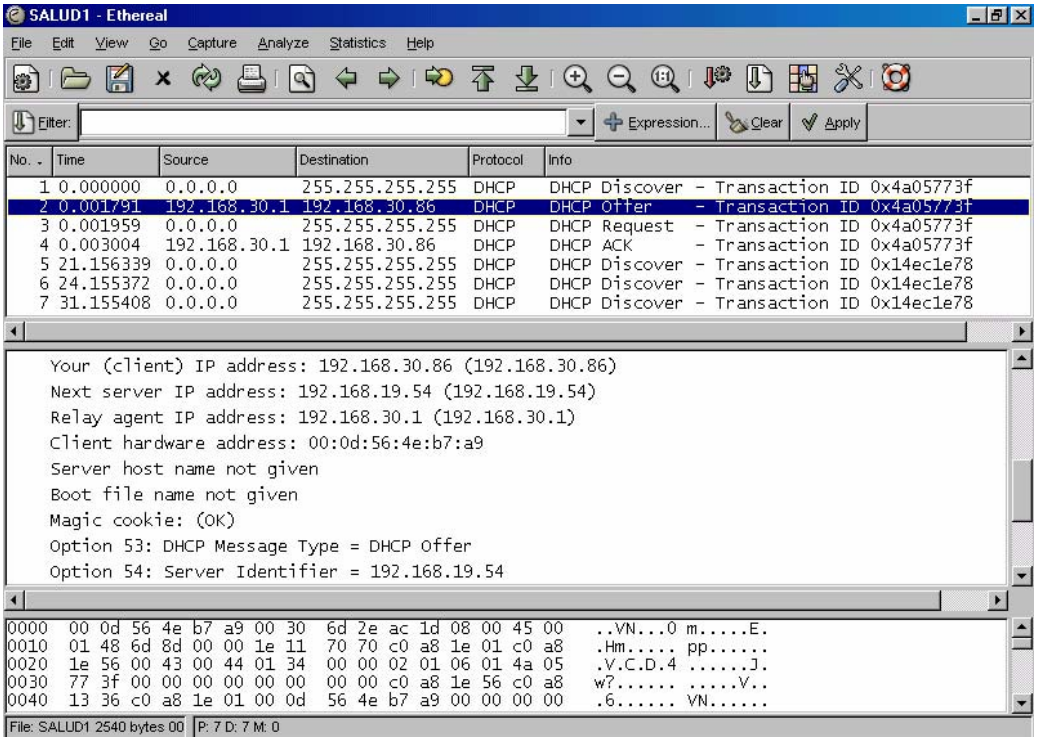
Para determinar si es factible llevar a cabo la implementación del protocolo a estas sedes, se ejecutó una prueba que consistió en ubicar 1 cliente en la facultad de salud, el cual solicitó su configuración de red al servidor DHCP (ubicado en la sede principal), y éste le asignó todos los parámetros necesarios utilizando asignación manual, ya que en el archivo de configuración del servicio, se hizo una declaración de host para la estación cliente.

Los resultados que se obtuvieron fueron buenos, ya que el tiempo de configuración que se observó fue muy bajo (0.003 segundos) y las longitudes de los mensajes de las transacciones estuvieron de acuerdo con los obtenidos en pruebas anteriores. Era de esperar pues los tiempos de respuesta que presentan las estaciones ubicadas en estas sedes son iguales a los que se registraron para las estaciones de la sede principal, debido a la forma en que se encuentran interconectadas. Por estas razones se considera que sí es viable prestar el servicio DHCP a las sedes ubicadas en el área metropolitana de Bucaramanga.

La figura 23 muestra la captura que se obtuvo en la estación cliente utilizando Ethereal y donde se puede apreciar el intercambio de mensajes para la solicitud de configuración. También se observan otros 3 mensajes

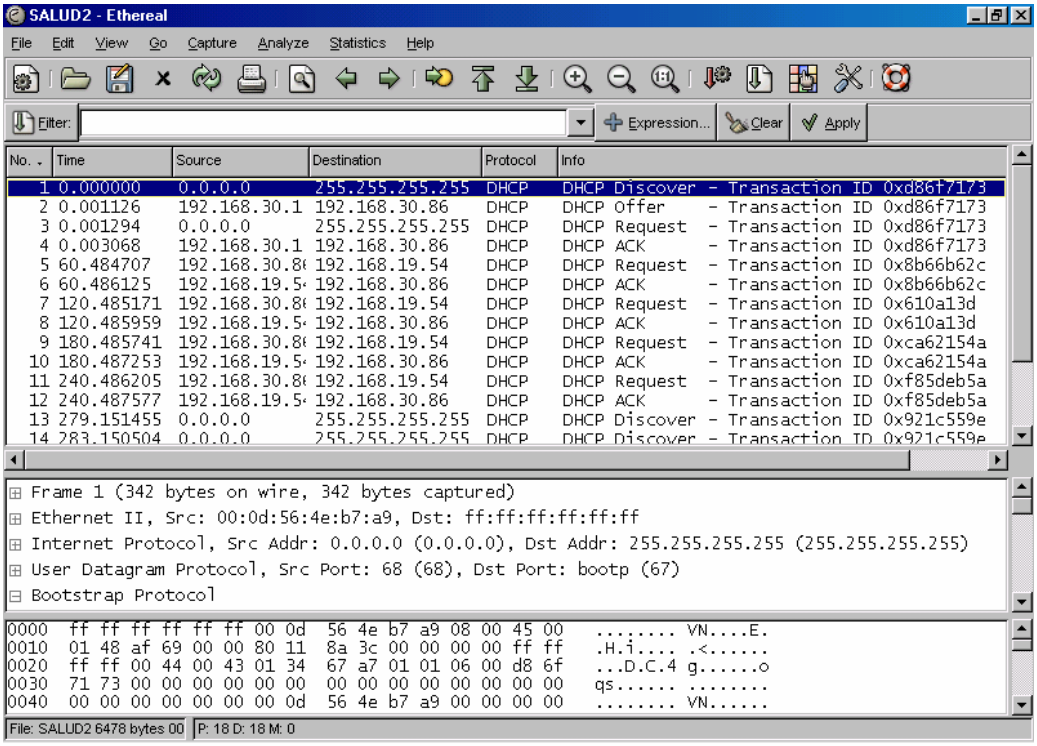
DHCP Discover que se efectuaron desde otro host dentro de esa misma subred.

Figura 23. Captura de la concesión entre un cliente ubicado en la facultad de salud y el servidor DHCP.



Una segunda captura fue realizada, para observar si las renovaciones que hacía el cliente se estaban llevando a cabo en los tiempos adecuados; para ello, el tiempo de lease fue fijado en 2 minutos, asegurando de esta manera que las renovaciones se realizaran cada 60 segundos. La figura 24 muestra dicha captura y como se puede observar, las renovaciones que efectuó el cliente se dieron una vez transcurridos los segundos que se esperaba.

Figura 24. Renovaciones de configuración que efectuó el cliente DHCP ubicado en la facultad de salud.



4.7.2 Sedes regionales.

Para determinar la viabilidad en la implementación del protocolo en las sedes ubicadas en diferentes municipios del departamento, fue necesario realizar mediciones de los tiempos de respuesta que presentaban las estaciones que conforman las subredes pertenecientes a estas sedes.

Estas mediciones fueron realizadas durante varios días consecutivos en horarios de alto tráfico y se utilizaron como herramientas de medición 2 programas diferentes: SolarWinds y Ping[33]. Como principales observaciones de estas pruebas se destacan:

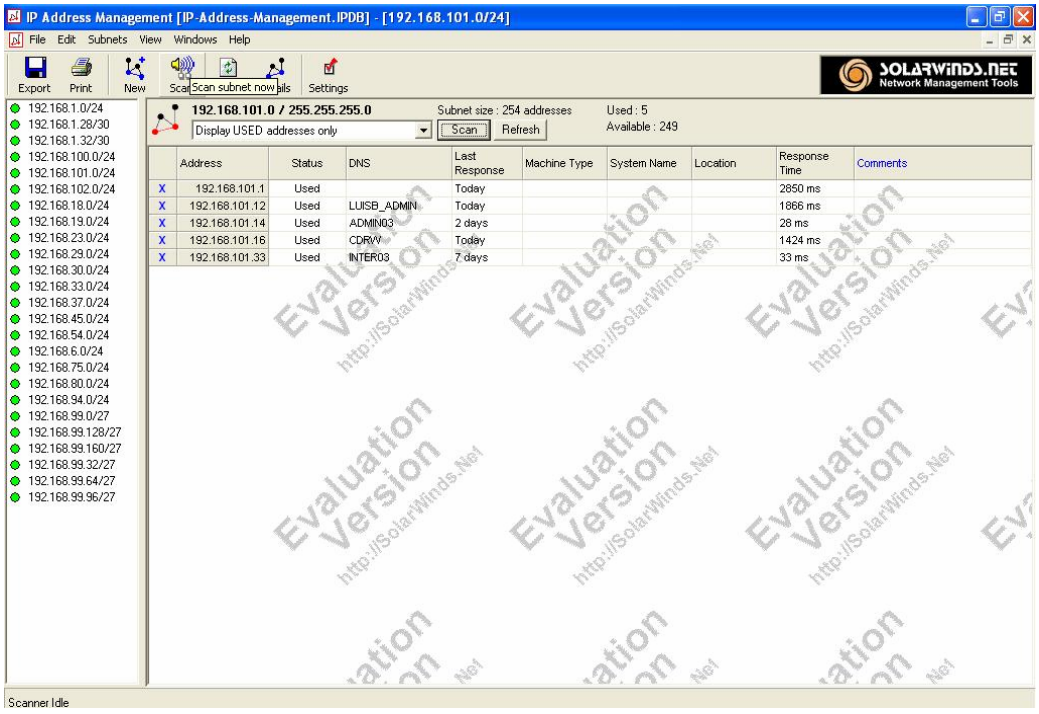
Los tiempos de respuesta que presentan las estaciones en estas subredes son muy elevados comparados con los de las estaciones ubicadas dentro de

[33] Programa que permite a un usuario realizar el envío de paquetes desde y hacia un host específico y espera que éste último envíe una respuesta, sin embargo, la exactitud de su respuesta es muy baja.

las sedes en Bucaramanga, ya que mientras en la sede principal los tiempos de respuesta son menores a 1 ms, en las sedes regionales alcanzan a superar los 50 ms.

Al realizar barridos de direcciones con SolarWinds por las 4 subredes correspondientes a las sedes regionales, se observó en múltiples ocasiones que dentro de una misma subred los tiempos de respuesta de algunas estaciones es demasiado elevado comparado con los de las demás estaciones, ya que en ciertas ocasiones se alcanzan a superar los 2000 y hasta 3000 ms. En la figura 25 se presenta una imagen que así lo demuestra.

Figura 25. Tiempos de respuesta de las estaciones pertenecientes a la subred de la sede de Málaga.



La sede con tiempos de respuesta más elevados es Málaga, donde se logran alcanzar valores de hasta casi 4000 ms. Por el contrario, la sede de Barbosa presenta los tiempos de respuesta más aceptables. En la tabla 22 se

presentan algunos de los resultados obtenidos al ejecutar Ping a las direcciones de las puertas de enlace de dichas subredes, los cuales demuestran la situación mencionada.

Tabla 22. Tiempos de respuesta de las puertas de enlace de las subredes de Málaga y Barbosa.

TIEMPOS DE RESPUESTA
Málaga (Subred 192.168.101.0)
Respuesta desde 192.168.101.1: bytes=32 tiempo=1462ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3283ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3365ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2246ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=1921ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2108ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2739ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3426ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3292ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2636ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=1995ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=1819ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=1633ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2259ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2263ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3902ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2330ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2247ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2337ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2494ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3205ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3114ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3191ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3024ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2816ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2948ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2997ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3175ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3376ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3273ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=3538ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2454ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=2566ms TTL=253
Respuesta desde 192.168.101.1: bytes=32 tiempo=1935ms TTL=253

Barbosa (Subred 192.168.102.0)
Respuesta desde 192.168.102.1: bytes=32 tiempo=138ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=166ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=200ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=25ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=28ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=34ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=102ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=51ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=111ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=148ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=338ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=279ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=122ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=171ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=25ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=25ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=139ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=256ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=27ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=26ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=104ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=87ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=276ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=35ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=40ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=143ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=163ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=25ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=25ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=45ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=120ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=76ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=90ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=26ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=132ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=81ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=25ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=234ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=244ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=71ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=25ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=25ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=312ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=25ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=307ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=78ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=25ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=83ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=98ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=25ms TTL=253
Respuesta desde 192.168.102.1: bytes=32 tiempo=110ms TTL=253

Las sedes regionales restantes también presentaron tiempos de respuesta poco favorables, en la tabla 23 se presentan los valores obtenidos al ejecutar Ping en las puertas de enlace de cada una de estas subredes.

Tabla 23. Tiempos de respuesta de las puertas de enlace de las subredes de Socorro y Barranca.

TIEMPOS DE RESPUESTA
Socorro (Subred 192.168.99.0)
Respuesta desde 192.168.99.1: bytes=32 tiempo=1365ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1139ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=982ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=839ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1001ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1114ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1288ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1140ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=964ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1104ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1174ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=946ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=643ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=628ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=902ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=87ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=230ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=662ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=699ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=860ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1039ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1046ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=966ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=881ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=983ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1172ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1248ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=658ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=950ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1204ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1463ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1106ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=760ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1063ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=880ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1065ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1052ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1202ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1180ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1230ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1133ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1270ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1243ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1172ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1127ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=981ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1253ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1342ms TTL=253
Respuesta desde 192.168.99.1: bytes=32 tiempo=1435ms TTL=253

Barranca (Subred 192.168.100.0)
Respuesta desde 192.168.100.1: bytes=32 tiempo=508ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=471ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=669ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=783ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=987ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=714ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=474ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=755ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=715ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=766ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=585ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=492ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=753ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=483ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=365ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=672ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=787ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=519ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=779ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=662ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=520ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=518ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=757ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=1000ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=742ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=417ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=813ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=700ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=410ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=375ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=413ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=353ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=391ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=163ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=511ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=404ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=275ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=779ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=626ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=161ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=356ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=278ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=346ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=710ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=687ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=404ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=268ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=334ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=190ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=303ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=314ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=163ms TTL=253
Respuesta desde 192.168.100.1: bytes=32 tiempo=126ms TTL=253

Para comprobar si los anteriores tiempos de respuesta son suficientemente válidos para afirmar que no se puede asegurar el servicio DHCP en las

sedes regionales, se halló la media aritmética. Estos valores se presentan a continuación.

Sede de Málaga: Media aritmética = 708.732143 ms
Número de muestras = 392

Sede de Barbosa: Media aritmética = 156.863415 ms
Número de muestras = 205

Sede de Socorro: Media aritmética = 698.89071 ms
Número de muestras = 183

Sede de Barranca: Media aritmética = 331.759076 ms
Número de muestras = 303

Si se observan los valores correspondientes a la sede de Málaga, es posible determinar que la media es bastante alta y teniendo en cuenta que el timeout entre el Offer y el ACK que el servidor envía al cliente es de 2 segundos y que el Request debe llegar al servidor en menos de un segundo, es posible que el servicio no se ejecute correctamente, implicando retransmisión de mensajes que aumentarían el tráfico en la red y elevarían considerablemente los tiempos de configuración.

Debido a todas las observaciones hechas anteriormente, no se puede afirmar que el servicio DHCP pueda ser prestado eficientemente a clientes que se encuentren ubicados en las subredes de las sedes regionales de la universidad, además, no resultaría provechoso hacer grandes esfuerzos para lograr prestar el servicio en dichas sedes, ya que de las estaciones ubicadas allí, son sólo unas cuantas las que poseen acceso a la red. Además, en cada sede regional, la DSI cuenta con personal capacitado para dar soporte a la red, por lo tanto se recomendaría hacer asignación estática de direcciones IP en las sedes, de la misma manera en que se han venido otorgando hasta el momento.

Sin embargo, si se deseara extender el servicio a estas sedes, se recomendaría ubicar un servidor DHCP en cada subred, que les permitiera a las estaciones obtener su configuración dinámicamente, además, si no se desea perder el beneficio de poder realizar la configuración de los hosts de una manera centralizada, se podría implementar una herramienta que permita la administración remota de estos servidores.

5. POLÍTICAS DEL SERVICIO

5.1 CONSIDERACIONES PRELIMINARES

Teniendo certeza sobre la viabilidad de implementación del Protocolo de Configuración Dinámica de Host (DHCP) en la red de datos de la Universidad Industrial de Santander y conscientes del nivel de complejidad que actualmente representa la administración y gestión de direcciones IP, es pertinente plantear algunas consideraciones para establecer las políticas más adecuadas que contribuyan a solucionar las necesidades actuales.

5.1.1 Alcances de las Políticas.

La formulación y planificación de las políticas a adoptar se deben desarrollar con base en metas específicas que conlleven a un uso óptimo de los recursos disponibles. Los objetivos a cumplir con el desarrollo de las políticas de servicio son:

- Centralizar la configuración y administración de los parámetros de red de todos los equipos de cómputo que hacen parte de la red de datos.

- Simplificar la administración de direcciones IP para reducir conflictos como duplicación o suplantación y llevar un registro de las mismas de acuerdo al número real de estaciones existentes en la red.

- Garantizar la coexistencia de DHCP con configuraciones estáticas en hosts no participantes de la implementación del servicio.

- Habilitar técnicas para utilizar DHCP en los estaciones móviles (laptops), de tal modo que no sea necesario identificar en qué ubicación física se encuentran ni realizar cambios en la configuración, permitiéndoles una

conexión "plug and play"; además proporcionar roaming[34] para el consumo de una sola dirección IP.

- Asegurar que los recursos que ofrece la red a la comunidad universitaria sean aprovechados óptimamente por usuarios con derecho a los mismos, restringiendo en lo posible el acceso a clientes no autorizados.

- Realizar el diseño de DHCP como un mecanismo a través del cual los administradores puedan implementar políticas de administración en la red.

- Plantear un proceso adecuado para la gestión de las direcciones IP, que esté de acuerdo con las necesidades de los clientes y las restricciones que la administración necesite implementar.

- Sugerir la forma más eficiente en que se puede llevar a cabo el procedimiento de recolección de información para migrar hacia el uso de DHCP en la red de datos institucional.

5.1.2 Recursos de Configuración.

Para poder desarrollar las diferentes políticas, es prioritario seleccionar cuáles recursos del servidor se van a utilizar y cómo, especialmente lo concerniente a la asignación y renovación de direcciones IP que se debe suministrar al gran número de estaciones que conforman la red; es importante señalar que aunque los tres mecanismos de asignación: manual, dinámica y automática, pueden ajustarse a los diferentes perfiles de usuario existentes, es valioso que con la implementación del protocolo DHCP se permita identificar y hacerle un seguimiento a cada una de las estaciones que conforman la red de datos.

El mecanismo de asignación manual asocia una dirección IP a cada host de acuerdo a su dirección MAC, permitiendo identificar cada uno de los equipos

[34] Habilidad de un usuario móvil inalámbrico para utilizar servicios de red fuera de su área de cobertura.

que obtienen parámetros de configuración de red utilizando DHCP; para sustentar que la asignación manual es la más adecuada para esta red de datos, se presentan los siguientes argumentos:

La organización de la red dispone de un buen número de subredes con rangos de direcciones suficientemente amplios, con lo que cada equipo tendrá una dirección IP que lo identifique de las demás estaciones, siendo así innecesaria la reutilización de direcciones, ofrecida por la asignación dinámica; la mayoría de subredes soporta hasta 254 hosts. Actualmente el segmento de red más grande está compuesto de 130 estaciones, correspondiendo a la subred 192.168.30.0 Facultad de Salud, por lo tanto es poco probable que se presente un crecimiento tan acelerado que agote rápidamente el rango de direcciones disponibles.

Un alto porcentaje de hosts siempre se mantiene en el mismo lugar físico, consecuentemente en el mismo segmento de red; si en dado caso se desplaza sobre la misma subred, el mecanismo garantiza que mantendrá la misma dirección IP y el servicio funcionará correctamente.

Si se traslada un equipo hacia otra subred, la nueva ubicación debe reportarse al administrador para que le asigne una dirección válida dentro del segmento actual; si no existe una IP asociada a la MAC, el cliente no recibirá los parámetros de red adecuados. Por lo tanto, los usuarios se verán obligados a informar la sustitución de tarjetas de red o la incorporación de nuevos equipos, lo que permitiría establecer la ubicación de cada PC dentro de la red en cualquier momento.

Con la revisión de las razones expuestas se establece que la asignación manual permite desarrollar un control centralizado y efectivo en cada segmento de la red, pues el identificador de cada cliente DHCP es único dentro de la subred a la cual él está conectado; con esto es posible mantener actualizado el inventario general de PCs de la Universidad lo que representa información muy importante para la DSI.

5.2 POLÍTICAS DE ADMINISTRACIÓN

Con el mecanismo de asignación seleccionado se procede a incorporar las políticas de administración que complementarán el funcionamiento del servicio para ofrecer una solución integral. Para ello se propone enmarcar la prestación del servicio desde tres clases de clientes: estaciones fijas, estaciones móviles cableadas y estaciones móviles inalámbricas, especificando en cada caso la configuración y las directrices adoptadas.

5.2.1 Estaciones Fijas.

Un alto porcentaje de equipos de cómputo de la red de datos, sede principal y área metropolitana, se configurarán como clientes DHCP y obtendrán sus parámetros mediante el mecanismo de asignación manual desde un servidor DHCP centralizado; los hosts restantes, que corresponden a servidores y dispositivos activos que ejecutan funciones de alta prioridad, continuarán con la configuración estática.

La coexistencia del servicio DHCP y la configuración estática se garantizará al agrupar los servidores en subredes específicas, diferentes a aquellas en que se encuentran los equipos distribuidos actualmente. De acuerdo con esto, si alguna entidad requiere incorporar un servidor debe reportarlo para que sea incluido en la subred adecuada; si no se informa podría generar conflictos de duplicación y será considerado como un cliente ilegítimo, sobre el que se puede imponer sanciones al ser detectado.

El servicio sólo se prestará a clientes conocidos, es decir, equipos que estén registrados con su respectiva MAC, información que se ingresará al archivo de configuración[35]; si un equipo se configura para utilizar el servicio DHCP pero no se reporta al administrador, obtendrá parámetros no válidos ya que

[35] El archivo final se entregó oficialmente a la DSI; allí se especifica la configuración para todos los clientes y se incluyen todas las subredes, junto con las maneras para implementar políticas y debido a su importancia y nivel de profundidad no se incluyó como anexo en este documento.

no se definirán rangos para la asignación dinámica y los clientes desconocidos se restringirán con directivas como "deny unknown clients" en el archivo de configuración.

Los administradores de salas de cómputo de escuelas o dependencias que utilicen servidores Proxy para el servicio de red, deben eliminarlos y su uso quedará prohibido, delegando esta labor de control a la respectiva entidad; esta medida permitirá mantener el inventario real de estaciones, pues en estas subredes pueden efectuarse configuraciones con direcciones IP que en muchos casos nunca llegan a ser de conocimiento de la DSI. Además existen suficientes direcciones disponibles por subred, eliminando la necesidad de un Proxy.

Para el ingreso de nuevas estaciones a la Red de Datos, las solicitudes se canalizarán a través de personal del Laboratorio Luis Eduardo Arias[36] , que reportará la información a la DSI, desde donde se actualizará centralizadamente el archivo del servidor DHCP con los datos entrantes; en situaciones críticas, las peticiones de ingreso se podrán realizar directamente con la DSI. En esta instancia, el administrador debe solamente revisar las direcciones ya asignadas y adicionar la definición del nuevo cliente, lo que implica en cuanto a escalabilidad, efectuar un crecimiento controlado.

Cuando se requiera cambiar parámetros o adicionar políticas a un determinado grupo de clientes o subredes, se adoptarán mediante la creación de grupos, pilas y/o declaraciones[37]; es importante destacar la flexibilidad ofrecida por el servicio al poder ejecutar modificaciones desde un servidor centralizado, evitando el desplazamiento por cada una de las estaciones implicadas, representando ahorro de tiempo y esfuerzo.

[36] En adelante se nombrará como LEA al laboratorio de informática Luis Eduardo Arias.

[37] Las opciones y directrices para implementar políticas se especifican claramente en el manual de configuración en el anexo F.

5.2.2 Estaciones móviles cableadas.

Para aprovechar las múltiples prestaciones que traen consigo los equipos portátiles, es fundamental ofrecerles acceso a la red en cualquier lugar del campus al que se desplacen sin requerir realizar modificaciones a la configuración para obtener parámetros de red.

Para resolver esta situación, se consideró una alternativa que ofrece el servidor entre sus opciones de configuración, la cual consiste en asignar varias direcciones IP a una misma MAC dentro de una declaración host; las direcciones que se asignen corresponden a los segmentos de red sobre los que el cliente posiblemente se desplace.

Esta solución no es la mejor ya que restringe la conectividad a las subredes informadas; si surge la necesidad de conectarse en otro lugar, necesita reportarse oportunamente, lo que puede convertirse en un procedimiento tedioso e ineficiente para situaciones imprevistas; además representa mayor control en el archivo de configuración y más cuidado en la actualización del mismo.

Para garantizar movilidad al portátil y además asignarle una IP única, se debe crear una VLAN similar a la que actualmente se encuentra definida para los servidores, lo que implicaría tener que realizar una reconfiguración de las interfaces asociadas a los puertos del switch central, con el fin de adicionar la nueva subred de portátiles y disponer uno o varios puertos para los clientes móviles; de esta manera el equipo podrá mantener su conectividad en cualquier edificio o dependencia que tenga acceso a la red, y sólo requiere conocer la ubicación de los puntos de red designados para tal fin, los cuales se localizarán posiblemente en salones de eventos, direcciones de escuela, auditorios, salas de juntas, entre otros.

Es conveniente mencionar que para verificar el buen funcionamiento de esta estrategia se realizaron pruebas con un equipo portátil sobre la VLAN 192.168.46.0 que tiene equipos distribuidos en los edificios de Eléctrica y de

Civil. Al host se le configuró una dirección IP asociada a su MAC en el servidor, y al iniciar su actividad recibió la misma configuración de red en ambas locaciones, las cuales están separadas una distancia considerable.

En cuanto a los equipos portátiles de profesores, directivos y personal interno, la DSI determinará cuáles se registrarán en la subred de portátiles con su correspondencia entre direcciones MAC e IP, los cuales se considerarán clientes conocidos; para la DSI es muy importante conocer y controlar en lo posible todos los hosts que hacen uso de la red, por lo tanto, equipos de visitantes que estarán temporalmente conectados a la red, deberán registrar su dirección física para que se les asigne una dirección de red y puedan moverse en la subred; el administrador puede crear las restricciones que considere necesarias a los visitantes, definiéndoles opciones dentro de un grupo creado en la subred de laptops, por ejemplo configurarle el tiempo de lease para que estos clientes mantengan conectividad sólo por un periodo de tiempo limitado; también puede restringirle el acceso a internet, no incluyendo la dirección del servidor DNS en la configuración del grupo. Sin embargo no se descarta que más adelante se habilite un rango de asignación dinámica para portátiles.

5.2.3 Clientes móviles inalámbricos.

La tendencia de implementar WLANs sigue creciendo, por lo tanto es necesario proyectar el funcionamiento del servicio DHCP en este entorno. Teniendo en cuenta que una red de área local inalámbrica se considera como una extensión de la red cableada a través de un Access Point, es necesario que este dispositivo soporte el protocolo DHCP y así garantice el intercambio de solicitudes entre el servidor y los clientes móviles.

Para asegurar que el servicio se prestará sólo a clientes conocidos, se creará un pool dentro de la subred en la que se encuentre el Access Point, donde se efectuará el registro de las direcciones MAC de la interfaz de red inalámbrica para asignarle una dirección IP válida a dichas estaciones,

impidiendo de esta manera que cualquier cliente no registrado obtenga parámetros válidos. Además dependiendo del lugar es posible instalar HotSpot (puntos de acceso público).

La DSI determinará cuáles portátiles con interfaz inalámbrica de miembros de la comunidad universitaria ingresarán como clientes conocidos al grupo de la WLAN, garantizándoles conectividad de datos y movilidad de usuario. Los equipos de visitantes que estarán temporalmente conectados a la red, deberán registrar su MAC para que se les asigne manualmente una dirección IP válida y puedan aprovechar el servicio; dicha asignación se mantendrá el tiempo que el host permanezca utilizando los recursos, posteriormente se deshabilitará.

Si un equipo portátil no posee tarjeta de red inalámbrica, el cliente debe remitirse a la respectiva dependencia y solicitarla en calidad de préstamo para poder ingresar a la WLAN; dichas tarjetas están ya registradas en el pool, indistintamente si el cliente es interno o externo, permitiendo que obtenga conectividad inmediata. El préstamo de la tarjeta inalámbrica se efectuará por el tiempo que el cliente vaya a permanecer en la WLAN.

5.3 POLÍTICAS DE GESTIÓN

Como resultado de la implementación del servicio DHCP en la mayoría de hosts que hacen parte de la red de datos, se tendrán parámetros de configuración persistentes para los clientes y la gestión se limita a un intercambio de información entre las dos entidades; las políticas van enfocadas básicamente hacia la incorporación de nuevos equipos y el servicio para visitantes.

5.3.1 Estaciones fijas.

Cuando una dependencia adquiere nuevos equipos de cómputo, generalmente recurre al personal del LEA para que los configuren y los adecúen para ofrecer servicios a sus usuarios; con este manejo, la solicitud de direcciones IP puede delegarse a funcionarios del LEA, que enviarán la información necesaria a la DSI desde donde se hará el registro y habilitarán las nuevas estaciones.

Sin embargo, se definirá una cuenta de correo por escuela o dependencia, por medio de la cual se podrán solicitar parámetros de configuración para uno o varios hosts, en caso que no se comunique al LEA. En la solicitud se debe especificar la dirección MAC, el hostname, el sistema operativo, la subred y el edificio donde se ubicarán los PCs. Para disminuir problemas de autenticación, la cuenta y su respectivo password se otorgarán a un alto funcionario del correspondiente ente, sea director de escuela o jefe de dependencia.

De la misma forma se gestionará la dirección IP cuando se realiza el cambio de tarjeta de red de una máquina, pues el host permanecerá con el registro de la MAC antigua si no se reporta al administrador; también se espera que por este medio se informe los equipos que se dan de baja, para mejorar el inventario y evitar desperdicio de recursos por direcciones abandonadas.

5.3.2 Estaciones móviles cableadas.

Cuando un cliente externo, sea visitante o miembro de la comunidad universitaria desee ingresar a la subred de portátiles, debe suministrar la información mencionada anteriormente. La escuela o dependencia que servirá de anfitriona para un invitado externo, por ejemplo un conferencista, debe hacer el respectivo trámite y garantizar parámetros válidos al equipo portátil; la asignación se otorgará por el tiempo que considere estará el usuario dentro del campus. En dado caso que no se

alcance a realizar por este medio y sea muy necesario el servicio, se contactará telefónicamente al administrador de la red.

5.3.3 Clientes móviles inalámbricos.

Para clientes externos que requieran ingresar a las WLANs se manejarán dos situaciones: cuando el cliente posee interfaz inalámbrica y cuando requiere alquilar una. En el primer caso debe remitirse a la dependencia para hacer el registro de la dirección MAC y así se le asignará una IP válida dentro del área de cobertura, la cual se gestionará telefónicamente con la DSI. Si el cliente hace uso frecuente del servicio, se registrará permanentemente a través del LEA para agilizar el acceso a la red, pero mantendrá la calidad de visitante, sujeto a las restricciones que el administrador considere para este grupo.

Si el usuario requiere solicitar en préstamo una tarjeta de red, debe suministrar su documento de identidad (visitante) acompañado de la información completa del equipo[38]; desde el momento de entrega del dispositivo hasta la devolución, el cliente se hace responsable por la integridad de la interfaz de red inalámbrica. Si eventualmente un cliente interno necesita una tarjeta de red para acceder a la WLAN y no está registrado como cliente conocido, ejecuta el anterior procedimiento pero en lugar del documento de identidad presentará la identificación que lo acredite como parte de la comunidad universitaria.

5.4 POLÍTICAS DE SOPORTE

Actualmente la solución de conflictos o dificultades de acceso a la red por parte de los usuarios no sigue un procedimiento adecuado; sencillamente la situación se reporta al administrador de la red, quien debe tomar las medidas necesarias para solucionar el problema. Sin embargo, muchas de

[38] Esta información incluye hostname, dirección MAC, SO.

las situaciones informadas pueden solventarse desde el usuario o delegarse a personal capacitado de la DSI, de tal modo que libere en gran parte al administrador de esta tarea, en ocasiones tediosa y repetitiva, y su intervención se presentará cuando sea estrictamente necesario.

Para ofrecer un servicio integral, se ubicará una etiqueta en cada estación de la red, la cual contendrá información de soporte, de manera que el usuario reciba orientación para la resolución de sus necesidades o pueda reportar la información oportunamente al personal encargado. El contenido que presentará el sticker[39] será el siguiente:

- Procedimiento para que cada usuario obtenga los parámetros de red que posee la estación para permitirle compartir archivos. Para esto, el usuario deberá ejecutar una aplicación que ha sido desarrollada como parte de este trabajo.

- Un URL[40] donde encontrará un instructivo para la solución de problemas de la red y preguntas frecuentes, las cuales van a estar especificadas para los diferentes sistemas operativos.

- Medio para entrar en contacto con el personal encargado de prestar soporte técnico de la red.

5.5 PROPUESTA DE DISEÑO

Inicialmente se había contemplado la posibilidad de utilizar uno o varios agentes relay y/o servidores dependiendo de las pruebas de tráfico

[39] El diseño del sticker y la información a la que hace referencia se presenta en el anexo E.

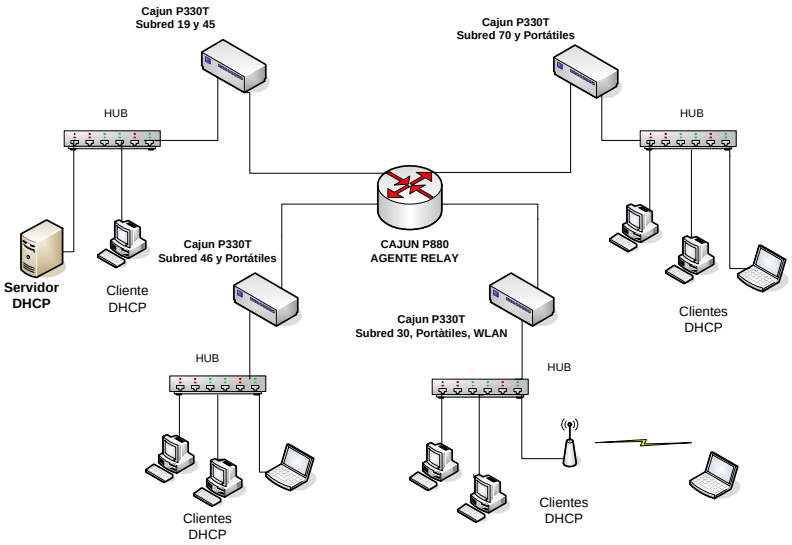
[40] Localizador Uniforme de Recursos, identificador de un elemento que se puede obtener mediante un navegador de la World Wide Web, indicando una localización concreta. Su contenido se especifica también en el anexo E.

efectuadas en el capítulo 4. Los resultados obtenidos en cuanto a estimación de tráfico y funcionamiento del servicio, demuestran que no es necesario más de un servidor y un agente relay, revalidando el diseño utilizado como la solución más adecuada para implementar el Protocolo de Configuración Dinámica de Host (DHCP) en la red de datos institucional.

Como se observó, el tráfico total que se generaría por la implementación del servicio no es significativo (196,732 Kbps) y de la misma manera, el servidor estaría en capacidad de ofrecer el servicio a un gran número de hosts, incluso superior al existente en la red de la UIS; además, el switch central configurado como agente relay, interconecta todas las subredes, pudiendo interceptar cualquier solicitud broadcast proveniente de clientes de cualquier subred y reenviarlas al servidor DHCP ubicado en la subred de servidores. El funcionamiento del agente relay se probó con clientes en varias subredes: eléctrica (192.168.46.0), Alta Tensión (192.168.45.0) y geomática (192.168.85.0), obteniendo resultados satisfactorios.

Soportados en los argumentos técnicos y de desempeño como parámetros primordiales en la selección del diseño, es igualmente importante mencionar que se aprovecharán al máximo los recursos existentes, el software puede instalarse en una máquina que ejecuta otros servicios y no es necesario realizar inversiones adicionales, que como se presentó en el segundo capítulo, pueden ascender a varios millones de pesos para una implementación con varios agente relay. El diseño recomendado se presenta en la figura 26.

Figura 26. Diseño de implementación del servicio DHCP en la Red de Datos de la Universidad Industrial de Santander.



Fuente: Los autores

El software que prestará el servicio será el programa Servidor de Linux Red Hat 9.0. que contará con un servidor de respaldo (par failover); se configurarán haciendo uso del protocolo failover que ofrece el servidor seleccionado, el cual permite mantener comunicación constante entre fuente y respaldo, garantizando que si en dado caso el servidor primario falla, el servidor secundario efectuará el relevo en la prestación del servicio DHCP oportunamente. Para esto, es importante recordar que ambos pares deben operar bajo la misma versión del SO que garantice una correcta interacción entre los dos.

Una ventaja adicional del diseño propuesto, se origina en la topología en estrella que presenta la Red de Datos de la Universidad, ya que si se instalara un servidor DHCP intruso (servidor no autorizado que esté ejecutando el servicio), los parámetros que ofrecerá, solo podrán ser adquiridos por clientes en la subred donde éste se encuentre, ya que el tráfico broadcast es aislado debido a la topología de la red y al agente relay, el cual impide que dichos parámetros lleguen a clientes de otras subredes al no tener configurada la dirección de red del intruso.

5.6 MIGRACIÓN HACIA DHCP

Para dar inicio al funcionamiento real del servicio y aprovechar las ventajas que ofrece, es necesario establecer una estrategia que permita hacer la transición de la configuración estática a la configuración dinámica de los hosts, que no afecte el desempeño de la red de datos. Por lo tanto, la migración se debe realizar gradualmente, configurando subred por subred, permitiendo al mismo tiempo la verificación del correcto funcionamiento del protocolo; además el procedimiento deberá ser transparente a los usuarios.

Teniendo en cuenta el gran número de estaciones y la cantidad de subredes, sería una labor bastante dispendiosa para el personal de la DSI tener que desplazarse por cada edificio y realizar la recolección de la información necesaria para llevar a cabo este proceso. Para agilizar esta tarea, se contará con el apoyo de estudiantes de pregrado de la Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones que estén cursando la asignatura Redes de Computadores, quienes supervisados por funcionarios de la DSI configurarán los hosts y simultáneamente desarrollarán el inventario de equipos con un formato que se les suministrará, donde se especificará la dirección IP estática con que cuenta en ese momento, la dirección MAC, el sistema operativo, el nombre de host (hostname), la subred a la cual pertenece y su ubicación física dentro del campus, así como la persona o entidad responsable de cada estación. Cabe resaltar que este procedimiento se realizará solamente una sola vez. El formato a utilizar se muestra en el ANEXO E.

6. CONCLUSIONES

Con la realización de las pruebas propuestas para el desarrollo de este proyecto, se determinó que la viabilidad de la implementación de DHCP en la red de la UIS es indudable, ya que en este estudio no sólo se tuvo en cuenta el impacto del servicio en el tráfico de la red, sino que se consideraron otros factores que también resultan de gran interés y que al igual que la estimación de tráfico, señalaron que se cuenta con todas las capacidades y recursos para prestar el servicio de manera eficiente. Dichos factores son los tiempos de configuración y renovación de los clientes DHCP, así como el soporte de los diferentes dispositivos que actualmente hacen parte de la estructura de la red. Además es evidente el interés que tienen los entes encargados de la administración de la red, en adoptar nuevas políticas que les permitan tener un mayor control sobre el uso que se ha venido dando a la red.

Los resultados de las pruebas realizadas permitieron establecer que el tráfico generado por la implementación del servicio no es significativo (196,732 Kbps) y no afectará el funcionamiento normal de la red de datos. Además, los datos obtenidos demostraron que el tráfico no se ve afectado por el mecanismo de asignación que se implemente, es decir, la longitud de los mensajes DHCP es la misma en cualquier caso.

Al tener conocimiento acerca de la estructura y organización de la red de datos de la universidad, así como de las diferentes características que rodean la utilización de la red por parte de los usuarios, se determinó que el tipo de asignación más conveniente para la implementación era la asignación manual, ya que así los recursos de red se aprovecharán solamente por usuarios registrados. De la misma manera, el tipo de asignación propuesta permitirá realizar el proceso de configuración de los hosts de una forma controlada y centralizada, optimizando el uso de

direcciones en la red y permitiendo controlar la expansión de la misma, además será posible mantener un inventario actualizado de los equipos de cómputo.

Con el servicio DHCP se fortalecerá la labor de administración de la red y se incrementará levemente la seguridad de la misma, lo cual no implica que sea invulnerable; para mejorar este importante factor, se deben implementar políticas y métodos de control adicionales. En la red de la UIS donde se hará asignación manual de direcciones, se eliminará el riesgo que un cliente malintencionado reclame todos los recursos del servidor para si mismo, negando la posibilidad a otros clientes de obtener su configuración de red, caso que posiblemente se presentaría si se utilizara la asignación dinámica. Adicionalmente, la topología física en estrella de la red contribuye a proteger el servicio, ya que si se instalan servidores no autorizados, sólo podrán otorgar parámetros a clientes en la subred donde se encuentren ubicados, gracias a que el agente relay, al no tener configurada la dirección IP del servidor intruso, impedirá la transmisión de paquetes a otro segmento de red.

Al momento de implementar cualquier servicio, es necesario tener presente la relación costo/beneficio, lo cual implica sopesar criterios técnicos y administrativos. Para el caso de las sedes regionales, cuyas subredes no contienen un alto número de hosts y donde no se garantiza el buen desempeño de DHCP, se contempló prestar el servicio instalando un servidor por subred y hacer su administración de manera remota con SSH, pero por circunstancias de coordinación y manejo, planteadas por la DSI, se determinó que los equipos continuarán con la configuración estática que ya traían.

Las herramientas de monitorización y análisis de red utilizadas, SolarWinds y Ethereal, fueron fundamentales en la ejecución de este proyecto e incluso permitieron detectar anomalías en la red de datos; cuando se hizo la revisión de sus archivos de captura, se encontraron interesantes resultados,

como equipos configurados como clientes BOOTP y solicitudes DHCP desde subredes diferentes a las definidas para las pruebas, los cuales posiblemente presentaban problemas de configuración y los usuarios no se habían percatado de estos hechos. Dicha información fue reportada a la DSI en ese momento para que se adoptaran las medidas necesarias; además, se identificaron múltiples servicios instalados que no eran de conocimiento de la DSI y con algunas visitas se descubrieron subredes que utilizaban servidores Proxy, que les proporcionaban conexión a Internet a múltiples equipos.

Con la migración hacia DHCP, se registrará la información de configuración de red de todos los equipos; dicha labor se realizará por cada subred que conforma la LAN de la UIS, con esto la DSI podrá identificar las diversas anomalías que actualmente se presentan, como el uso de servidores Proxy y emprender las medidas necesarias. Sin embargo, para que la implementación de DHCP se realice de una manera eficiente, es fundamental la disposición y colaboración del personal de administración de red de las respectivas escuelas o dependencias.

Con la política de soporte propuesta, se agilizará la solución de gran parte de los conflictos que se presentan actualmente. Además permite una mayor interacción de los usuarios con los servicios de la red, con lo cual se fortalece la capacitación de la comunidad UIS en cuanto a tecnologías de la información, aspecto fundamental en la actual cultura de conocimiento.

El desarrollo de este proyecto contribuyó significativamente a mejorar los servicios ofrecidos y administrados por la DSI, constituyéndose en un gran aporte del grupo de investigación en conectividad y procesado de señal (CPS), demostrando que cuando existen canales de comunicación eficientes y se anudan esfuerzos, se producen resultados de beneficio general para la comunidad universitaria.

7. RECOMENDACIONES

Para garantizar que la configuración de los parámetros de red se realice completamente desde un servidor centralizado, es necesario deshabilitar las propiedades de red en todos los equipos de las subredes existentes; si se requiere implementar cambios, como configurar estaciones de manera estática, deben ser ejecutados solo por personal autorizado, evitando que alteraciones voluntarias o involuntarias afecten el buen funcionamiento del servicio.

Antes de poner en marcha el servidor por primera vez, es necesario cerciorarse que exista el archivo .leases y el servidor DHCP esté configurado de manera estática, para evitar conflictos en el funcionamiento del servicio.

Hay que tener en cuenta la prioridad de los parámetros definidos para cada estación, ya que cuando un cliente inicia, consulta su binding en las declaraciones de “host”, después declaraciones de clase, seguida por el pool, subnet y shared network. El servidor DHCP primero identifica y asigna el alcance más específico.

La calidad de prestación del servicio DHCP está representada por el impacto del tráfico generado en una red de datos y por el tiempo de configuración de los clientes; de igual manera, es muy importante verificar que los dispositivos a intervenir en la implementación del servicio, es decir, servidor DHCP, clientes y agentes relay funcionen correctamente.

Teniendo en cuenta que los binding otorgados con la asignación manual no entran a formar parte del archivo dhcpd.leases, y aunque en el archivo de configuración se tiene registro de todas las declaraciones hechas por estación, se sugiere crear una base de datos que permita efectuar un seguimiento detallado a cada estación.

Debido a la gran cantidad de estaciones (1782) que existen conectadas a la red de la UIS, el archivo de configuración será de gran tamaño y a pesar que se agruparán por subredes o grupos, identificar determinada estación desde allí no es una tarea sencilla. Para facilitar la administración se recomienda utilizar la interfaz gráfica conocida como Webmin, con la que el control y actualización es mucho más rápido.

Actualmente, la DSI cuenta con 2 sistemas de Windows 2000 Server, los cuales se encuentran prestando servicios de red de baja exigencia, por lo tanto, sería posible que estos equipos fueran implementados también como servidores DHCP ya que se conocen registros del alto desempeño que éstos presentan.

Windows 2000 y 2003 server presentan dentro de sus opciones de configuración del servicio DHCP, la opción para habilitar el servicio MADCAP (Multicast Address Dynamic Client Allocation Protocol) el cual permite la asignación dinámica de direcciones multicast a equipos clientes del servicio. Esto sería valioso al momento de implementar grupos multicast dentro de la red de datos institucional.

Para reconocer fácilmente los puntos de conexión que establecen conectividad a la subred de dispositivos portátiles, se deben implantar identificadores que permitan indicar los puntos de red destinados para tal fin, lo cual hace necesario que se deba llevar un control de los puntos asignados por cada edificio.

El Diseño propuesto se consideró conjuntamente con la DSI de acuerdo al soporte y a las necesidades actuales de la red; teniendo en cuenta que para la DSI es importante conocer los equipos que están conectados a la red, si se desea implementar mecanismos de asignación diferente al manual, se recomienda adoptar mecanismos de autenticación para garantizar la integridad del servicio. Al respecto existen múltiples trabajos que se están desarrollando, entre los que se destacan los realizados por el DHC Working.

Si existe un considerable número de equipos que permanecerán encendidos por gran tiempo, se les debe definir en la declaración “host” un tiempo de lease mayor al que tiene por defecto con el objetivo de disminuir el tráfico por renovación; normalmente las estaciones solicitan renovación de sus parámetros a las 6 horas de encenderse y el mecanismo garantiza que los parámetros de red siempre se asocien a determinada dirección.

Es conveniente rotar las direcciones IP de los equipos, aprovechando que por cada subred existe un considerable número de direcciones disponibles, con el objetivo de evitar suplantación o duplicación de IP por clientes externos que configuren sus propiedades, o clientes internos que de alguna forma modifiquen las propiedades de red.

Para disminuir el posible acceso de clientes no autorizados a la red de datos, es conveniente que en el archivo de configuración no se defina la puerta de enlace de las subredes como la primera dirección IP de las mismas, sino aleatoriamente para que la configuración de los parámetros de red no sea tan inmediata. Igualmente distribuir las direcciones IP uniformemente en el rango de direcciones y no de forma consecutiva.

Se recomienda profundizar en las prestaciones que ofrecen los dispositivos activos que hacen parte de la red en cuanto a manejo de direcciones IP, con el fin de mejorar el servicio DHCP. Particularmente el switch central de la red de datos posee un comando “Creating IP Static ARP entries”, y al implementarse se observó que asociaba la dirección MAC de una estación con una dirección IP determinada; con esto si un usuario malintencionado suplanta los parámetros de otro cliente, mantendrá conectividad solamente con estaciones de su segmento de red pero no podrá tener acceso a Internet, ni compartir recursos con clientes de otras subredes, limitándolo en gran medida para utilizar los servicios de la red.

Periódicamente se debe realizar un escaneo general de la red utilizando alguna herramienta de monitorización de red, con el fin de identificar posibles direcciones abandonadas y de esta forma tener actualizado inventario.

Si la infraestructura de red hace migración a Ipv6, se podrá continuar con la prestación del servicio gracias al desarrollo de DHCPv6, el cual es superior a la versión 4 (Ipv4), ya que éste presenta mejor desempeño en cuanto a tráfico y tiempos de configuración, debido a que las solicitudes que se realizarán de los clientes al servidor se transmitirán por multicast y no por broadcast como se describió anteriormente. Sin embargo DHCPv6 también requiere el uso de un agente relay que comunique al servidor y los clientes localizados en diferente subredes.

8. BIBLIOGRAFIA

Avaya P550R, P580, P880, and P882 Multiservice Switch User Guide.

BLUM, Richard. "Network Performance Open Source Toolkit Using Netperf, tcptrace, NIST Net, and SSFNet". Wiley Publishing, Inc., 2003.

Cajun P333R Stackable 3rd Layer Switch User's Guide, Software Version 3.0.

CEPEDA, Oscar; CHAMBERS, Bob; MOSCA, Julián; ROBBINS, Matt. "Beyond DHCP -Work Your TCP/IP Internetwork with Dynamic IP". IBM, International Technical Support Organization, Junio de 2000. Disponible en Internet: www.redbooks.ibm.com

Cisco CNS Network Registrar User's Guide, Chapter 11: Configuring DHCP Scopes and Policies, 2003.

Command Reference Guide for the Avaya P550R, P580, P880 and P882 Multiservice Switches version 5.3.1.

DHC Working Group of the IETF. Resources for DHCP. Disponible en Internet: http://www.dhcp.org/.

DROMS, Ralph. "Automated Configuration of TCP/IP with DHCP". Bucknell University, 1998.

FEIT, Sidnie. "TCP/IP Arquitectura, protocolos e implementación con Ipv6 y seguridad de IP", Mc. Graw Hill, 1998.

GOFF, Brian David. “Distributed Resource Monitoring Tool and its Use in Security and Quality of Service Evaluation”, febrero 27 de 2002.

KOMORI, Tadashi; SAITO, Takamichi. “ The Secure DHCP System with User Authentication”, Tokio University of Science, 2002.

LAPOINTE, Dave; WINSLOW Josh. “Analyzing and simulating Network Game Traffic”, WORCESTER POLYTECHNIC INSTITUTE, Diciembre 19 de 2001.

LU, Kaining; TU, Xiangyun; ZOU, Jun. “Design and Implementation of DHCP & LDAP Directory”. School Of Electronic Information Engineering, TianJin University, 2002.

PARK, Chul-Jin; AHN, Seong-Jin; CHUNG, Jin-Wook; LEE, Choon-Hi; PARK, Chang-Soon. “The Improvement for Integrity between DHCP and DNS”, 1997.

PERKINS, Charles E.; BOUND, Jim. “DHCP for IPv6”, Sun Microsystems, Inc.

_____; JAGANNADH, Tangirala. “DHCP for Mobile Networking with TCP/IP”, IBM, T.J. Watson Research Center, 1995.

Proyecto LuCAS, “Linux: Instalación y Primeros Pasos”. Septiembre 17 de 1998.

RFC 1541, RFC 2131, RFC 2132.

STALLINGS William, COMUNICACIONES Y REDES DE COMPUTADORES, Sexta Edición, Pearson Educación S.A:, 2000.

TANENBAUN Andrew S., REDES DE COMPUTADORAS, Cuarta Edición, Pearson Prentice Hall, 2003.

The Microsoft Company. Windows 2003 Server. Disponible en Internet: http://www.microsoft.com/windows2003/es/server/help/.

The SCAMPY Project, INFORMATION SOCIETY TECHNOLOGIES (IST) PROGRAMME, Septiembre 17 de 2002.

WANG, Jenq-Haur; LEE, Tzao-Lin. "Enhanced Intranet Management in a DHCP-enabled Environment", Department of Computer Science and Information Engineering, National Taiwan University, 2002.

ANEXOS

ANEXO A

Determinación de la cantidad de subredes y estaciones

Para llevar a cabo la ejecución de esta tesis de grado, resultó indispensable identificar y conocer cada una de las características de la organización lógica y física de la red de datos de la UIS. Con este fin, se empleó una versión de prueba del software para monitorización de redes SolarWinds Network Toolbar versión 5.5[41], el cual cuenta con un amplio conjunto de herramientas que permiten desarrollar diferentes estudios del desempeño y la organización de una red de datos.

Los requerimientos de SolarWinds son mínimos, ya que sólo es necesario mantenerlo instalado en un equipo que haga parte de la red de datos y desde ahí realizar la monitorización que se desee. Dicho equipo debe poseer un procesador Pentium II de 500 Mhz o superior, mínimo 128 MB de memoria RAM, al menos 100 MB de espacio en disco y tarjeta de red o módem, para poder dar el soporte necesario a este software.

Dentro de las múltiples herramientas que *SolarWinds* ofrece, se utilizaron únicamente 2 de ellas. La primera fue Subnet List, la cual descubre las subredes comunicadas a un determinado router que opere con SNMP[42] y muestra un listado con ellas, indicando también su máscara de subred. Gracias a la utilización de esta útil herramienta, se pudo determinar que actualmente se encuentran definidas **80** subredes dentro de la red institucional.

Teniendo conocimiento de las diferentes direcciones de red de las subredes que se descubrieron anteriormente, se procedió a realizar barridos de direcciones IP en cada una de ellas; para esto, se utilizó la herramienta *IP*

[41] Mayor información en http://solarwinds.net.

[42] SNMP, Simple Network Management Protocol.

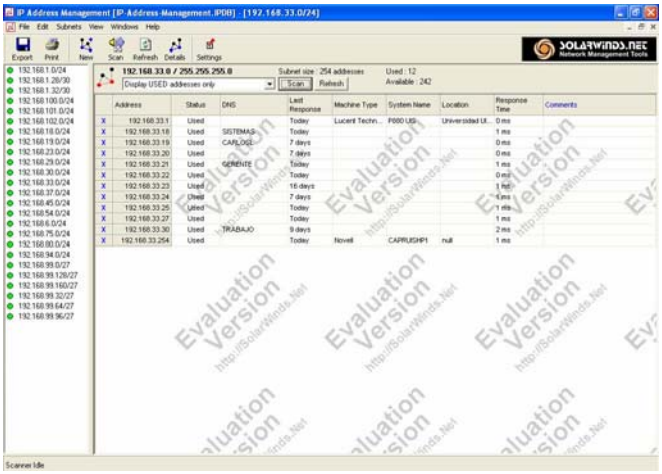
Address Management, permitiendo determinar de esta manera el número total de estaciones que hacen parte de la LAN.

SolarWinds IP Address Management puede ser usada para monitorear activamente cuáles direcciones IP están siendo usadas en una red de datos, así mismo da una estimación del tiempo de uso de dichas direcciones. La información que presenta para cada dirección IP es la siguiente:

- Estado de la Dirección IP (Disponible, en uso o reservada para futuros usos).
- Nombre DNS.
- Número de días desde que se obtuvo la última respuesta.
- Tipo de máquina (si el dispositivo soporta SNMP).
- Nombre del sistema (si el dispositivo soporta SNMP).
- Ubicación (si el dispositivo soporta SNMP).
- Tiempo de respuesta.
- Comentarios (el usuario puede agregar sus propios comentarios para cada dirección).

La figura 1 muestra la ventana de operación del IP address management durante uno de los barridos que se llevaron a cabo en la subred 192.168.33.0 de la red de datos institucional.

Figura 1. Ventana de operación del IP address management.



La metodología utilizada en esta inspección fue bastante acertada, ya que se escogieron horarios en los que el tráfico en la red es crítico, lo cual indica que se encuentra encendido un gran número de estaciones que están haciendo uso de la red. Estos horarios son: entre las 8 y 10 de la mañana y las 4 y 6 de la tarde; además, los barridos por las diferentes subredes se realizaron continuamente durante 7 días hábiles para obtener datos más aproximados. La tabla 1 muestra los resultados que se obtuvieron al realizar los barridos con IP address management.

Tabla 1. Resultados obtenidos en los barridos de direcciones IP para las diferentes subredes.

Subred	Máscara	Día 1		Día 2		Día 3		Día 4		Día 5		Día 6		Día 7	
		Total	Uso	Total	Uso	Total	Uso	Total	Uso	Total	Uso	Total	Uso	Total	Uso
10.2.2.0	255.255.255.224	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.1.0	255.255.255.252	10	10	10	10	10	10	10	10	10	10	10	10	10	10
192.168.1.4	255.255.255.252	2	2	2	2	2	2	2	2	2	1	2	2	2	2
192.168.1.8	255.255.255.252	2	2	2	2	2	2	2	2	2	2	2	2	2	2
192.168.1.12	255.255.255.252	2	2	2	2	2	2	2	2	2	2	2	1	2	2
192.168.1.24	255.255.255.0	2	2	2	2	2	2	2	2	2	2	2	2	2	2
192.168.5.0	255.255.255.0	35	35	35	34	35	33	35	33	35	33	35	33	35	33
192.168.6.0	255.255.255.0	53	53	54	40	55	43	55	39	56	45	56	38	57	31
192.168.8.0	255.255.255.248	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.9.0	255.255.255.0	2	2	2	2	2	2	2	2	2	2	2	2	2	2
192.168.18.0	255.255.255.0	42	42	42	34	42	34	43	35	43	34	43	33	47	36
192.168.19.0	255.255.255.0	22	22	22	22	22	21	22	19	22	21	22	22	22	21
192.168.20.0	255.255.255.0	53	53	53	39	55	43	56	46	58	43	58	42	58	35
192.168.21.0	255.255.255.0	9	9	9	4	9	8	10	9	10	7	10	6	10	5
192.168.22.0	255.255.255.0	22	22	22	15	22	17	22	14	23	19	23	20	23	21
192.168.23.0	255.255.255.0	25	25	25	24	26	25	33	32	36	35	36	35	36	35
192.168.24.0	255.255.255.0	38	38	38	23	38	33	38	28	38	32	38	28	39	27
192.168.27.0	255.255.255.0	49	49	51	44	54	41	55	32	58	51	59	51	64	42
192.168.28.0	255.255.255.0	8	8	8	7	9	8	9	8	10	8	10	8	11	7
192.168.29.0	255.255.255.0	3	3	3	3	3	2	3	3	3	3	4	4	4	3
192.168.30.0	255.255.255.0	112	112	114	41	121	85	130	95	133	94	135	94	136	67
192.168.31.0	255.255.255.0	20	20	20	17	22	21	25	19	25	21	25	20	25	16
192.168.32.0	255.255.255.0	4	4	4	1	4	3	4	3	4	3	4	2	5	4
192.168.33.0	255.255.255.0	9	9	9	8	9	9	11	10	11	9	11	9	12	9
192.168.34.0	255.255.255.0	20	20	22	13	24	23	26	24	28	18	29	25	29	21
192.168.35.0	255.255.255.0	23	23	23	17	24	21	25	22	25	22	25	23	25	21
192.168.36.0	255.255.255.0	5	5	5	4	5	4	6	4	6	5	6	4	6	5
192.168.37.0	255.255.255.0	32	32	32	29	32	31	33	29	35	30	35	31	36	30
192.168.38.0	255.255.255.0	55	55	55	48	57	53	58	54	58	51	58	51	58	54
192.168.39.0	255.255.255.0	35	35	36	26	37	31	37	29	37	27	38	30	41	29
192.168.40.0	255.255.255.0	30	30	30	21	32	29	33	23	33	24	33	28	33	24
192.168.41.0	255.255.255.0	64	64	67	53	69	56	72	54	75	61	76	60	76	58
192.168.42.0	255.255.255.0	22	22	23	17	24	19	24	19	24	18	24	15	24	17

192.168.43.0	255.255.255.0	46	46	46	28	46	28	50	38	52	44	52	42	52	39
192.168.44.0	255.255.255.0	68	68	68	44	76	70	80	67	80	71	80	63	82	67
192.168.45.0	255.255.255.0	42	42	42	24	43	30	43	25	43	32	43	29	43	35
192.168.46.0	255.255.255.0	27	27	28	15	33	19	34	24	34	27	34	26	35	28
192.168.47.0	255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.48.0	255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.49.0	255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.50.0	255.255.255.0	49	49	50	39	59	51	60	41	61	46	61	45	61	18
192.168.51.0	255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.54.0	255.255.255.0	21	21	21	12	22	14	23	13	23	14	24	15	25	16
192.168.58.0	255.255.255.0	23	23	24	24	24	24	24	22	24	23	24	21	24	24
192.168.59.0	255.255.255.0	14	14	14	14	15	15	15	14	15	14	15	13	15	13
192.168.61.0	255.255.255.0	59	59	59	21	59	44	59	41	59	41	59	38	59	47
192.168.62.0	255.255.255.0	39	39	39	1	39	17	39	14	39	34	39	39	39	19
192.168.65.0	255.255.255.0	28	28	30	21	33	27	33	23	33	27	33	27	34	25
192.168.71.0	255.255.255.0	3	3	4	3	11	11	11	3	13	4	13	1	16	2
192.168.72.0	255.255.255.0	2	2	2	1	3	2	3	2	3	3	3	3	3	3
192.168.73.0	255.255.255.0	9	9	9	6	11	11	11	8	11	10	11	9	11	11
192.168.74.0	255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.75.0	255.255.255.0	10	10	10	9	10	9	10	9	10	1	10	8	10	8
192.168.76.0	255.255.255.0	8	8	8	6	8	7	8	1	8	8	8	7	8	5
192.168.80.0	255.255.255.0	11	11	11	10	11	11	11	9	11	11	12	12	12	9
192.168.81.0	255.255.255.0	19	19	19	18	19	19	19	19	19	11	19	17	19	16
192.168.84.0	255.255.255.0	26	26	29	26	33	32	33	10	36	31	37	33	37	7
192.168.85.0	255.255.255.0	51	51	53	40	54	51	54	46	54	37	55	42	56	15
192.168.86.0	255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.87.0	255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.88.0	255.255.255.0	8	8	9	8	10	7	10	6	14	12	15	9	16	7
192.168.89.0	255.255.255.0	13	13	13	11	15	14	15	12	15	9	15	14	15	4
192.168.92.0	255.255.255.0	6	6	7	6	8	8	8	6	8	5	8	7	8	4
192.168.93.0	255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.94.0	255.255.255.0	13	13	15	11	15	12	15	8	15	8	15	9	17	9
192.168.96.0	255.255.255.0	3	3	4	3	4	3	4	4	4	2	4	3	4	2
192.168.97.0	255.255.255.0	14	14	14	14	15	15	15	15	15	4	15	15	15	4
192.168.99.0	255.255.255.224	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.99.32	255.255.255.224	12	12	14	13	14	10	14	13	14	14	14	12	15	0
192.168.99.64	255.255.255.224	1	1	1	1	3	3	3	0	3	0	3	0	3	0
192.168.99.96	255.255.255.224	16	16	17	17	17	17	17	0	17	17	17	17	17	0
192.168.99.128	255.255.255.224	16	16	16	1	16	2	16	2	16	2	16	2	16	0
192.168.99.160	255.255.255.224	25	25	25	0	28	21	30	0	30	0	30	0	30	0
192.168.100.0	255.255.255.0	19	19	19	14	21	16	21	14	22	17	23	22	23	19
192.168.101.0	255.255.255.0	1	1	1	1	2	2	2	1	4	2	4	2	4	3
192.168.102.0	255.255.255.0	2	2	2	2	2	2	2	2	3	3	3	3	3	3
192.168.105.0	255.255.255.0	2	2	2	2	2	1	2	1	2	2	2	2	2	2
192.168.106.0	255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.107.0	255.255.255.0	7	7	8	8	9	8	9	8	9	8	9	8	9	4

Al realizar la sumatoria de los valores contenidos en la columna “Total” de la medición para el día 7, se determinó que el número de estaciones que se

encuentran conectadas a la red es de **1782**.

Los resultado que se obtuvieron gracias a la implementación de SolarWinds son de gran importancia para el desarrollo de este estudio, demostrando así la gran ayuda que significó el aprovechamiento de este software.

ANEXO B

Procedimientos para la configuración del agente relay

La importancia de un agente DHCP relay en una red de datos que cuente con el servicio DHCP implementado es indiscutible. Ya en capítulos anteriores se han dedicado múltiples explicaciones para dejar claro este tema.

Al realizar un detallado estudio sobre los diferentes dispositivos como switches y routers que conforman la estructura de la red de la UIS se comprobó que el switch central (Cajun P880 de Avaya) permite ser configurado como agente DHCP relay, evidenciando así la capacidad de soporte para DHCP de la red institucional.

En el capitulo 2 se presentó un corto procedimiento que permite configurar el switch central como agente relay, sin embargo, a continuación se muestra la información extraída del manual de usuario de dicho dispositivo, **Avaya P550R, P580, P880, and P882 Multiservice Switch User Guide, Version 5.3.1** ***Document Revision 2.0***, exponiendo así el procedimiento de configuración de dicho agente a través de la CLI (Command Line Interface).

3. Refer to Table 9-6 to configure the **Add IP Static ARP Entry** dialog box parameters:

Table 9-6. IP Static ARP Parameters

Parameter	Allows you to...
IP Address	Enter an IP address to associate with the Static ARP entry.
MAC Address	Enter the MAC address of a node to which you want to create a static ARP entry.

4. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings.

Creating IP Static ARP Entries Using the CLI

To create IP static ARP entries using the CLI, enter the following command in Configure mode:

```
<configure># arp <ip-address> <hardware-address>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

Creating a BOOTP/DHCP Server Entry

The BOOTP/DHCP Server Entry allows you to configure a Router as a BOOTP/DHCP Relay Agent between a BOOTP/DHCP server and the requesting client.

You can create a BOOTP/DHCP Server entry using either the Web Agent or the CLI.

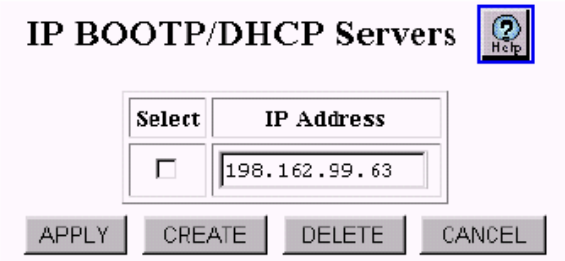
* **Note:** BootP/DHCP must first be enabled in the **IP Global Configuration.**

Creating a BOOTP/DHCP Server Entry Using the Web Agent

To create a BOOTP/DHCP entry using the Web Agent:

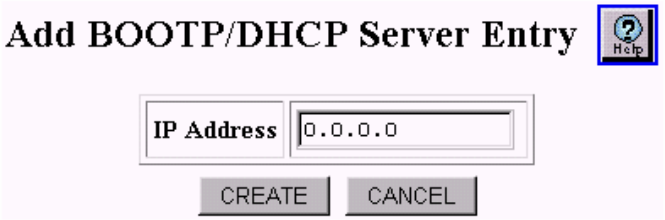
1. Select **BOOTP/DHCP Servers** from the **Routing** > **IP** > **Configuration** group on the Web Agent window. The **IP BOOTP/DHCP Servers** dialog box opens (seeFigure 9-13).

Figure 9-13. IP BOOTP/DHCP Server Dialog Box



2. Select **CREATE**. The **Add BOOTP/DHCP Server Entry** dialog box opens (Figure 9-14).

Figure 9-14. Add BOOTP/DHCP Server Entry Dialog Box



3. Enter the BOOTP/DHCP server IP address in the **IP Address** field.
4. Click **CREATE** to save your changes, or **CANCEL** to restore previous settings.

* **Note:** It is possible to create multiple BOOTP/DHCP Server Entries if necessary.

Creating a BOOTP/DHCP Server Entry Using the CLI

To create a BOOTP/DHCP entry using the CLI, enter the following command in Configure mode:

```
<configure># ip boot-dhcp server
<ip-address>
```

Refer to the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1* for details about this command.

Option 82 for DHCP

Option 82 for DHCP includes two options:

- **Circuit Info**, identifies the slot and physical port number from which the DHCP request was received.
- **Agent Info**, identifies the IP address and, if available, the system name of the switch.

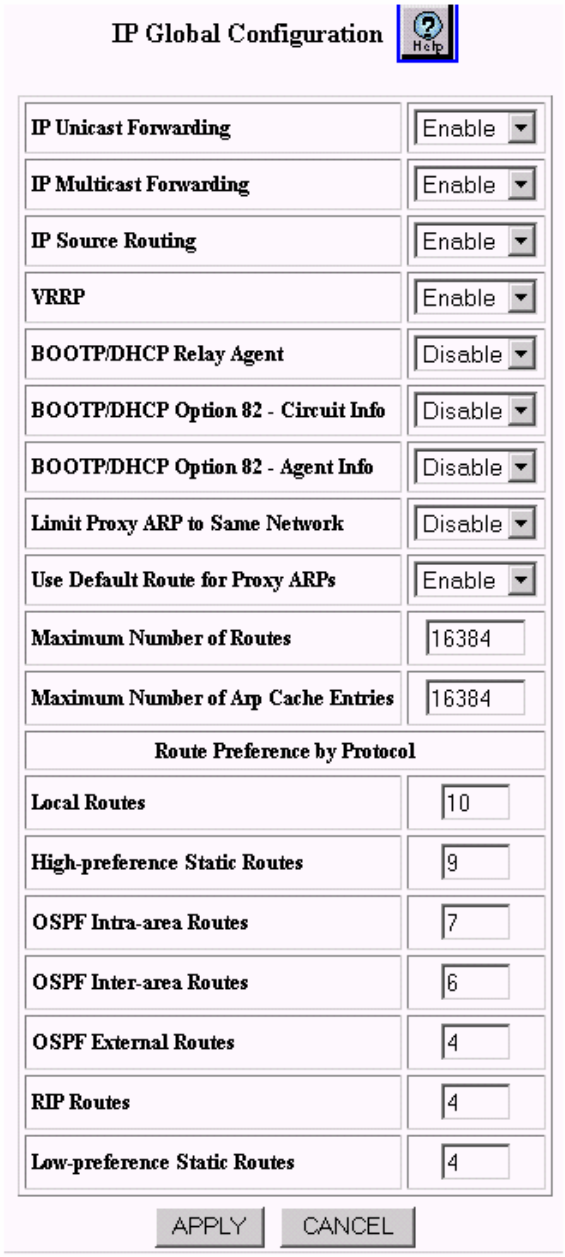
By default, both of these suboptions are disabled. You can enable either or both suboptions by using the Web Agent or the CLI.

Enabling Option 82 by Using the Web Agent

To use the Web Agent to change the status of option 82:

1. Select **Global** from the **Routing** >**IP** > **Configuration** group. The **IP Global Configuration** dialog box opens (Figure 9-15).

Figure 9-15. IP Global Configuration Dialog Box



2. Open the pull-down menus from the **DHCP Option - Circuit Info** and **DHCP Option 82 - Agent Info** fields.
3. Select **Enable**.

* **Note:** BOOTP/DHCP relay Agent must be set to enable, and must be enabled on the desired IP interface (enabled by default).

Enabling Option 82 by Using the CLI

To use the CLI to enable Option 82, enter Global Configuration mode and use the following commands:

- To enable circuit info 1, use the following command:

  <configure># ip bootp-dhcp circuit-info

- To enable agent info 2, use the following command:

  <configure># ip bootp-dhcp agent-info

- To disable circuit info 1, use the following command:

  <configure># no ip bootpdhcp circuit-info

- To disable agent info 2, use the following command:

  <configure># no ip bootp-dhcp agent-info

For detailed information on how to enter Global Configuration command mode, see "Accessing/Exiting the Command Modes" in Chapter 1, "*Overview*," of the *Command Reference Guide for the Avaya P550R, P580, P880, and P882 Multiservice Switches, Version 5.3.1.*

IP Multicast

IP Multicast enables a single host to distribute information to multiple recipients. To do this, multicast protocols use class D IP addresses to specify specific multicast groups to which information is sent. The class D IP address used by multicast routing protocols, ranges from 224.0.0.1 to 224.0.0.255. The class D IP addresses available for general use are 224.0.1.0 to 239.255.255.255.

In addition, IP multicasting distributes information to multicast groups in two specific ways:

- **Multicast Forwarding** - allows a switch to forward multicast traffic from the local multicast server to group members on directly attached subnetworks. If a multicast packet is forwarded to multiple interfaces on one VLAN, only one Forwarding Entry is added on the VLAN for the packet. One copy of the packet is sent to the VLAN.To configure interfaces for multicast forwarding select Internet Group Management Protocol (IGMP) for the multicast protocol.

ANEXO C

Metodología para determinar causantes de errores en las pruebas de verificación del servicio DHCP

Ante los problemas presentados durante las pruebas de verificación de los mensajes intercambiados en el desarrollo del protocolo y los tiempos empleados para este propósito, fue necesario plantear algunas hipótesis acerca de la causa que los estaba originando. Basándose en un esquema de red como el que se presenta en la figura 1, el cual se implementó en todas las pruebas anteriores, se pudo plantear las siguientes posibles causas:

La primera consideración que se contempló fue que estos problemas se estuvieran presentando debido a errores de configuración del servidor.

Como segunda opción se planteó la posibilidad de fallas en el funcionamiento de algún dispositivo intermedio de la red, como por ejemplo el switch Cajun P333R al cual se encontraban conectados tanto el servidor como los clientes, y que éste no fuera capaz de direccionar correctamente los mensajes de las transacciones.

En última instancia se estimó que equipos clientes mal configurados podrían generar dichas anomalías, o bien, que esto se debiera a la complejidad de la red de datos.

Sin embargo, a pesar de tener planteadas estas tres hipótesis, resultaba muy difícil establecer la causa del problema, ya que no se tenía ninguna fundamentación válida para afirmar o descartar alguna. Inicialmente se planteó un análisis más a fondo de las cabeceras de cada uno de los mensajes para encontrar alguna variable que se pudiera analizar, pero se

abortó el proceso por el comportamiento impredecible de parámetros que se asumió podrían tenerse en cuenta, como el elipse time.

Entonces, fue necesario plantear una metodología inductiva, generando escenarios desde el más simple al más complejo, que permitieran establecer ciertos indicios que condujeran a alguna suposición válida; dicha estrategia se dividió en 5 niveles los cuales son presentados a continuación.

Nivel 1

Como primera medida, se pensó en realizar pruebas con una red que excluyera dispositivos intermedios, logrando de esta manera un modelo de conectividad muy sencillo y así empezar a descubrir cuál era el elemento que en realidad estaba ocasionando los percances mencionados anteriormente. El escenario que se desarrolló se muestra en la figura 1, que consiste en un esquema de red con un solo cliente y un servidor DHCP conectados por un cable cruzado.

Figura 1. Servidor DHCP y un cliente comunicados por cable cruzado.

Los resultados de esta prueba se muestran en la tabla 6, obtenidos al revisar las capturas realizadas tanto en el servidor como en el cliente, las cuales permitieron ver que la concesión de parámetros de red únicamente se realizaba con los 4 mensajes necesarios y que el tiempo en realidad era muy bueno (inferior a 1 segundo), debido a que no se presentó pérdida ni repetición de mensajes.

Tabla1. Resultados de verificación del servicio DHCP en una red servidor- un cliente.

Equipo	Tiempo (seg.)		Mensajes				No. De Bytes
	Config.	Total	Config.	Totales	Repetidos	Perdidos	
Equipo 1 (192.168.45.19)	0,761045	0,761045	4	4	0	0	**1380**

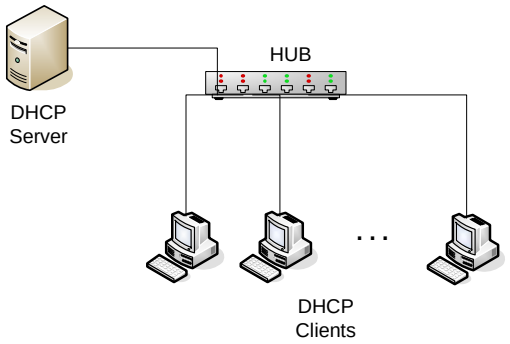
Con esto, se empezaba a considerar la incidencia mínima o nula del servidor y los clientes en los problemas ocasionados, ya que los datos registrados fueron óptimos, siendo necesario resultados para más clientes.

Siguiendo la metodología planteada anteriormente, resultó necesario ir aumentando gradualmente la complejidad del esquema de red mostrado en la figura1, por lo tanto se procedió al desarrollo del nivel 2.

Nivel 2

Para el desarrollo de esta parte se utilizó un hub o concentrador, al cual se conectaron los clientes y el servidor, construyendo el esquema que se muestra en la figura 2; es importante resaltar que el hub no estaba conectado a la red de la UIS, sino que los dispositivos estaban funcionando como una red independiente. Para poder observar el comportamiento progresivo de las transacciones, fue necesario aumentar el número de clientes en el hub, iniciando con 1 solo cliente hasta obtener un máximo de 7.

Figura 2. Esquema de red servidor y clientes DHCP conectados a un hub.



Al finalizar estas pruebas, se efectuó un cuidadoso estudio de las capturas obtenidas, apreciando que los resultados eran buenos y que estaban de acuerdo a lo esperado, ya que en ningún momento se estaban presentando los mensajes DHCP Offer y DHCP ACK en broadcast, además los mensajes repetidos y/o perdidos fueron muy pocos. La tabla 7 muestra los resultados obtenidos en estas pruebas.

Tabla 7. Resultados verificación de parámetros para servidor y siete clientes DHCP.

No. De Equipos	Equipo	Tiempo (seg)		Mensajes				No. De Bytes Conf.
		Config.x cliente	Promedio	Config.	Perdido config.	Adicional	Totales	
1	Equipo 1 (192.168.45.19)	0,003205	0,003205	4	0	0	4	**1380**
2	Equipo 1 (192.168.45.19)	0,931511	0,719801	4	0	0	8	1380
	Equipo 2 (192.168.45.16)	0,508092		4	0	0		1380
							TOTAL BYTES	**2760**
3	Equipo 1 (192.168.45.19)	0,93101	0,337156	4	0	0	12	1380
	Equipo 2 (192.168.45.16)	0,002624		4	0	0		1380
	Equipo 3 (192.168.45.18)	0,077834		4	0	0		1380
							TOTAL BYTES	**4140**
4	Equipo 1 (192.168.45.14)	0,508173	0,3677	4	0	0	20	1380
	Equipo 2 (192.168.45.16)	0,329026		4	0	0		1380
	Equipo 3 (192.168.45.18)	0,057367		4	0	1 Req, 1 Ack		1380

	Equipo 4 (192.168.45.17)	0,576549		4	0	2 Inform		1380
	TOTAL BYTES DE CONFIGURACION							**5520**
	TOTAL BYTES DE TODOS LOS MENSAJES							**6888**
5	Equipo 1 (192.168.45.14)	0,506532	0,462103	4	0	0	24	1380
	Equipo 2 (192.168.45.16)	0,281186		4	0	0		1380
	Equipo 3 (192.168.45.18)	0,02257		4	0	1 Req, 1 Ack		1380
	Equipo 4 (192.168.45.17)	0,576411		4	0	2 Inform		1380
	Equipo 5 (192.168.45.19)	0,923816		4	0	0		1380
	TOTAL BYTES DE CONFIGURACION							**6900**
	TOTAL BYTES DE TODOS LOS MENSAJES							**8268**
6	Equipo 1 (192.168.45.14)	0,503133	0.33312	4	0	0	32	1380
	Equipo 2 (192.168.45.16)	0,315767		4	0	0		1380
	Equipo 3 (192.168.45.18)	0,203688		4	0	1 Req, 1Ack		1380
	Equipo 4 (192.168.45.17)	0,934365		4	0	1Req,1Ack 2 Inform		1380
	Equipo 5 (192.168.45.12)	0,031836		4	0	1 Req, 1Ack		1380
	Equipo 6 (192.168.45.13)	0,009969		4	0	0		1380
	TOTAL BYTES DE CONFIGURACION							**8280**
	TOTAL BYTES DE TODOS LOS MENSAJES							**11016**
7	Equipo 1 (192.168.45.14)	0,48981	0,437944	4	0	1 Req, 1 Ack	37	1380
	Equipo 2 (192.168.45.16)	0,00252		5	1Discov. 1Offer	0		2064
	Equipo 3 (192.168.45.18)	0,952527		4	0	0		1380
	Equipo 4 (192.168.45.17)	0,568133		4	0	2 Inform		1380
	Equipo 5 (192.168.45.12)	0,572654		4	0	0		1380
	Equipo 6 (192.168.45.13)	0,010711		4	0	0		1380
	Equipo 7 (192.168.45.11)	0,469258		4	0	1Req, 1Ack		1380
	TOTAL BYTES DE CONFIGURACION							**10344**
	TOTAL BYTES DE TODOS LOS MENSAJES							**12738**

Como se puede observar en la tabla anterior, la columna correspondiente a "Mensajes" está divida en 4 categorías: Mensajes de Configuración,

Mensajes Perdidos en la configuración, Mensajes Adicionales y Mensajes Totales. Los mensajes de configuración hacen referencia a los mensajes que fueron necesarios para que cada cliente obtuviera su propia configuración de red, incluyendo solicitudes como Discover y Offer que abortaron el proceso, pero que tenían el mismo identificador de las transacciones de la configuración exitosa . Los mensajes perdidos fueron transacciones que se abortaron, pero registraban diferente identificación al proceso completo, como si hubiera existido algún conflicto como colisiones o fuera ocasionado por algún aspecto del canal (se presenta en la prueba con 6 clientes). Los mensajes adicionales fueron considerados como mensajes que aumentaban innecesariamente el tráfico generado, pues sucedían después de que todos los clientes estaban configurados. Los mensajes totales fueron capturados por el servidor durante cada prueba, es decir, deben corresponder a la sumatoria de mensajes de las columnas ya descritas, originados por las transacciones de cada cliente.

Se apreciaron 2 situaciones bastante interesantes que estaban ocurriendo. La primera era la solicitud de renovación que enviaban algunos clientes (DHCP Request) y la respuesta a éstos por parte del servidor (DHCP ACK); este intercambio de mensajes ocurría aproximadamente 7 segundos después de que los clientes obtenían su configuración. Este comportamiento se empezó a presentar durante la prueba que se realizó con 4 clientes y se mantuvo hasta la última prueba, es decir, la correspondiente a la activación de la conexión en 7 clientes; en todos los casos el equipo con dirección IP 192.168.45.18 generó tal situación y en las últimas 2 pruebas (con 6 y 7 clientes), intervinieron los clientes con direcciones 192.168.45.12, 192.168.45.14 y 192.168.45.17 con este intercambio de mensajes.

La segunda observación importante fue que el cliente con dirección IP 192.168.45.17 enviaba 2 mensajes DHCP Inform al servidor pasados 50 segundos después de obtener su configuración de red. Al igual que el

primer caso, este empezó a ocurrir en la prueba en que se activaba la conexión para 4 clientes en un mismo instante de tiempo.

A pesar que las dos situaciones mencionadas acarreaban ciertas consecuencias sobre el tráfico generado por las transacciones, no se consideraron realmente graves, ya que efectivamente se presentaron varios segundos después del intervalo de tiempo considerado crítico en cuanto a la configuración de cliente y el incremento de tráfico.

Al terminar estas pruebas y analizar sus resultados, se pudo concluir que eran bastante satisfactorios, ya que no presentaban los inconvenientes en el primer escenario considerado , donde se contaba con acceso a la red y los clientes y el servidor se conectaban al Cajun P333R. Con esta conclusión se descartó completamente que los problemas presentados anteriormente fueran a causa del mal funcionamiento del servidor, de esta manera se prosiguió al siguiente nivel de la metodología.

Nivel 3

En esta parte se planteó la necesidad de descartar la posibilidad de que los problemas con las transacciones fueran originados por los clientes, o en otras palabras, que se debieran a alguna falla del sistema operativo con el que estaban trabajando los clientes en las anteriores pruebas. Usando el mismo esquema de la figura 3, se decidió repetirlas, sólo que en esta oportunidad los clientes se encontraban trabajando con sistema operativo Linux Red Hat 9.0, el mismo con el que estaba operando el servidor DHCP, pensando en que se reducirían incompatibilidades entre sistemas operativos, si era que existían.

Durante la realización de las pruebas se notó un suceso bastante interesante, y fue que los clientes Linux, sólo realizaban la solicitud de configuración una vez; después de esto, cuando se desactivaba y activaba

la interfaz de red, a diferencia de los clientes Windows XP, enviaban mensajes Request para efectuar renovación, nunca concesión.

Ante esta situación se optó por definir otro rango a los clientes que ya habían recibido parámetros y se incorporaron nuevos clientes; los hosts antiguos no iniciaban el proceso inmediatamente, antes enviaban algunos Request intentando adquirir la dirección previa y posteriormente si realizaban las cuatro transacciones. Para que iniciaran el proceso en el instante de activación de la interfaz fue necesario eliminar el archivo dhcpd.leases de las estaciones clientes, para que no tuviera registro de la anterior configuración; y cuando nuevamente se activaba la conexión, realizaban la renovación de los parámetros. La tabla 8 muestra los resultados obtenidos.

Tabla 8. Verificación parámetros de configuración para clientes Linux

No. De Equipos	Clientes	Tiempo (seg)		Mensajes				No. De Bytes
		Config x cliente	Promedio	Config.	Perdido Config.	Perdidos	Totales	
1	Estación 1 (192.168.45.14)	0,468403	0,468403	4	0	0	4	1368
2	Estación 1 (192.168.45.9)	0,03114	0,221197	4	0	0	8	1368
	Estación 2 (192.168.45.10)	0,411255		4	0	0		1368
							TOTAL DE MENSAJES	**2736**
3	Estación 1 (192.168.45.14)	0,50693	0,385496	4	0	0	12	1368
	Estación 2 (192.168.45.17)	0,175953		4	0	0		1368
	Estación 3 (192.168.45.16)	0,473605		4	0	0		1368
							TOTAL DE MENSAJES	**4104**
4	Estación 1 (192.168.45.85)	0,200179	0,518826	4	0	0	16	1368
	Estación 2 (192.168.45.84)	0,986374		4	0	0		1368
	Estación 3 (192.168.45.83)	0,240151		4	0	0		1368
	Estación 4 (192.168.45.82)	0,648603		4	0	0		1368
							TOTAL DE MENSAJES	**5472**

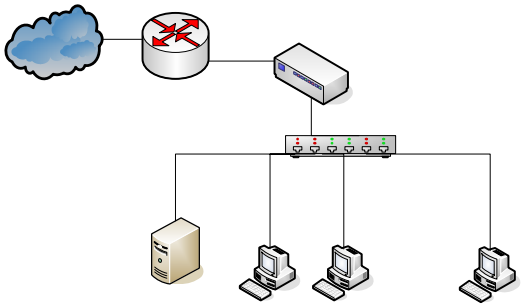
En la tabla anterior se puede ver que los resultados son bastante buenos, ya que los tiempos de configuración son cortos y no se está presentando

pérdida ni repetición de mensajes. Hasta este punto todo indicaba que en realidad era algún dispositivo intermedio de la red el causante de los problemas que se habían presentado en las pruebas de verificación, ya que según los últimos resultados había quedado claro que ni el servidor ni los clientes eran los culpables de esta situación. Debido a esto se procedió al desarrollo del nivel 4, en el que la red independiente con la que se habían desarrollado los 2 niveles anteriores, empieza a ser parte de la LAN de la Universidad.

Nivel 4

En este nivel, se determinó que era momento de que esta red empezara a formar parte de la red de datos de la Universidad y de esta manera observar cómo se daban los mensajes en las transacciones ante la presencia de dispositivos intermedios, en consecuencia, se obtuvo un esquema de red como el de la figura 4, donde los clientes, al obtener su configuración de red por parte del servidor DHCP obtienen también total acceso a la red.

Figura 4. Clientes y servidor conectados a la Red de Datos.



Como se puede observar, para esta prueba se prescindió del switch Cajun P333R, es decir, el hub al que estaban conectados los clientes y el servidor fue conectado directamente al switch departamental del edifico Eléctrica Antigua (Cajun P330T), buscando de esta manera obtener resultados que

indicaran la responsabilidad del Cajun P333R ante los problemas de las pruebas de verificación.

Los resultados se presentan en la tabla 9 permitieron reafirmar las posibles causas de los problemas ocurridos durante las pruebas de verificación, ya que, como se puede observar, los tiempos de configuración fueron bastante bajos, además todos los mensajes fueron direccionados de la manera adecuada, así mismo no se presentaron mensajes perdidos ni repetidos en gran cantidad; éstos se vieron únicamente durante la prueba con 6 clientes y fueron los causantes del alto tiempo de configuración de los equipos.

Tabla 9. Resultados obtenidos en la prueba con Clientes y servidor conectados a la Red de Datos.

No. De Equipos	Equipo	Tiempo (seg)		Mensajes				No. De Bytes Conf.
		Config.x cliente	Promedio	Config.	Perdido config.	Adicional	Totales	
1	Equipo 1 (192.168.45.240)	0,672896	0,672896	4	0	0	4	**1380**
2	Equipo 1 (192.168.45.240)	0,05417	0,10086	4	0	0	8	1380
	Equipo 2 (192.168.45.239)	0,147551		4	0	0		1380
							TOTAL BYTES	**2760**
3	Equipo 1 (192.168.45.238)	0,003527	0,057823	4	0	0	12	1380
	Equipo 2 (192.168.45.240)	0,152191		4	0	0		1380
	Equipo 3 (192.168.45.239)	0,017753		4	0	0		1380
							TOTAL BYTES	**4140**
4	Equipo 1 (192.168.45.236)	0,199009	0,438814	4	0	0	18	1380
	Equipo 2 (192.168.45.240)	0,656973		4	0	0		1380
	Equipo 3 (192.168.45.237)	0,293461		4	0	2 Inform		1380
	Equipo 4 (192.168.45.239)	0,635844		4	0			1380
							TOTAL BYTES DE CONFIGURACION	**5520**
							TOTAL BYTES DE TODOS LOS MENSAJES	**6888**
5	Equipo 1 (192.168.45.236)	0,198630	0,46987	4	0	0	22	1380

	Equipo 2 (192.168.45.237)	0,731869		4	0	2 Inform		1380
	Equipo 3 (192.168.45.240)	0,648954		4	0	0		1380
	Equipo 4 (192.168.45.238)	0,406118		4	0	0		1380
	Equipo 5 (192.168.45.239)	0,36378		4	0	0		1380
	TOTAL BYTES DE CONFIGURACION							**6900**
	TOTAL BYTES DE TODOS LOS MENSAJES							**7584**
6	Equipo 1 (192.168.45.239)	0,992717	0.33312	4	0	0	29	1380
	Equipo 2 (192.168.45.236)	0,198384		4	0	0		1380
	Equipo 3 (192.168.45.237)	0,889232		4	0	2 Inform		1380
	Equipo 4 (192.168.45.240)	0,631092		4	0	0		1380
	Equipo 5 (192.168.45.235)	0,612154		4	0	0		1380
	Equipo 6 (192.168.45.238)	0,58998		5	1 Disc, 1Offer	0		1722
	TOTAL BYTES DE CONFIGURACION							**8622**
	TOTAL BYTES DE TODOS LOS MENSAJES							**9990**

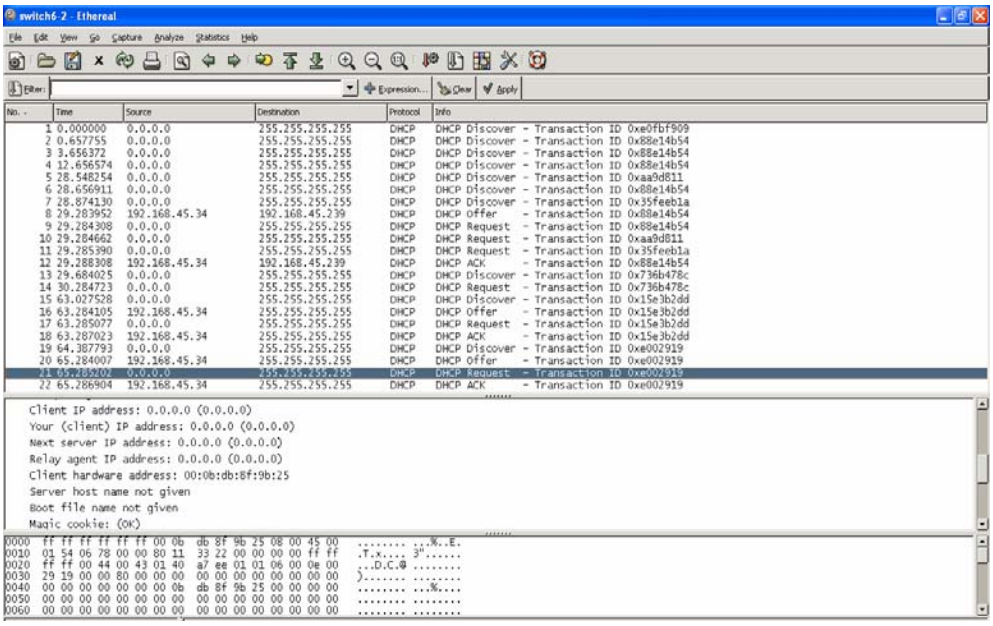
De la prueba con 4 clientes en adelante hubo un cliente que envió al servidor 2 mensajes DHCP Inform, pero como en los casos anteriores, estos fueron enviados varios segundos después de que el cliente ya había obtenido su configuración de red, por lo tanto no fueron considerados como parte del tráfico que se generó gracias a las transacciones con el servidor.

Al finalizar la prueba del nivel 4 se pudo tener certeza del origen de los problemas ya mencionados, creyendo que era necesario realizar una última prueba que permitiera comprobar que efectivamente era el Cajun P333R el responsable de los problemas presentados, de esta manera se pasó al quinto y último nivel de esta metodología.

Nivel 5

Una vez terminada la toma de resultados en el nivel 4, se procedió a realizar una última prueba, la cual se basó en el esquema mostrado en la figura 1, el mismo que se implementó para las pruebas de verificación. Estas pruebas fueron llevadas a cabo con el fin de comprobar una vez más que era el switch Cajun P333R el causante de las fallas que se observaron en las pruebas iniciales de este capítulo. La figura 5 muestra los resultados obtenidos en este nivel y claramente demuestran que las transacciones entre los clientes y el servidor se realizan incorrectamente; excepto un Ack y un Offer, los demás mensajes de este tipo, que deben enviar en unicast, fueron direccionados en broadcast, además se presentan demasiados mensajes para la concesión, especialmente Discover que se repiten y/o pierden, lo cual ocasionó elevados tiempos de configuración de los clientes (más de 1 minuto).

Figura 5. Captura para 6 clientes utilizando el switch P333R



Con las apreciaciones ya mencionadas, quedó comprobado que efectivamente el switch Cajun P333R posee problemas en su

funcionamiento y fue el causante de los malos resultados obtenidos durante las pruebas de verificación y que el protocolo DHCP funcionó correctamente en los demás esquemas expuestos. La certeza del adecuado comportamiento del servicio tanto el cliente como servidor permite avanzar con claridad en el desarrollo del proyecto.

En el momento que se realizaron las pruebas de verificación no fue posible revisar el dispositivo para establecer las posibles fallas; sin embargo, posteriormente se efectuó una actualización del software del switch P333R de la versión 3.9 a la versión 3.12 a través de una sesión por consola. Después de esto se hicieron unas pruebas para el servicio y aunque los tiempos de configuración mejoraron en los clientes, algunos mensajes del protocolo no se direccionaban correctamente.

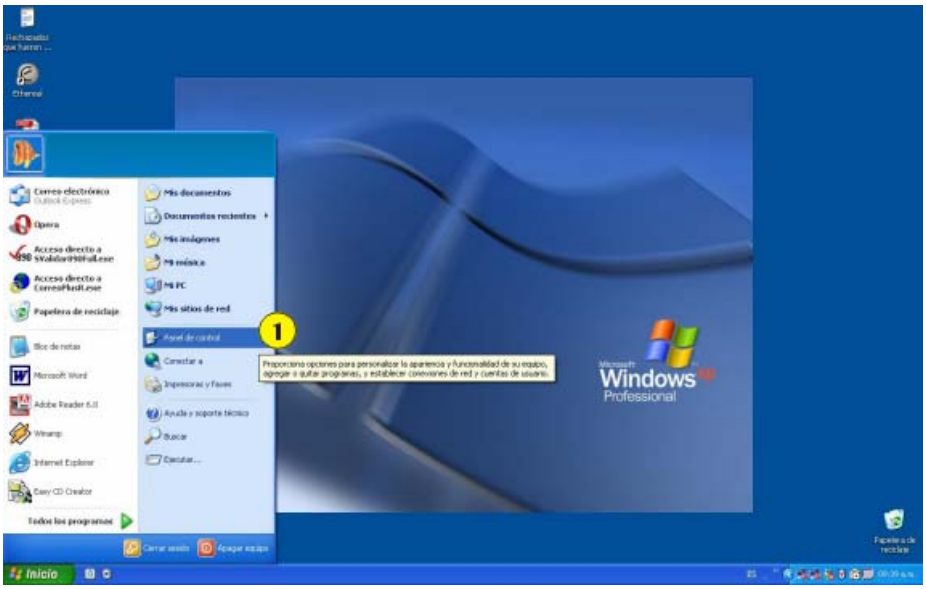
ANEXO D

Configuración de estaciones como clientes DHCP

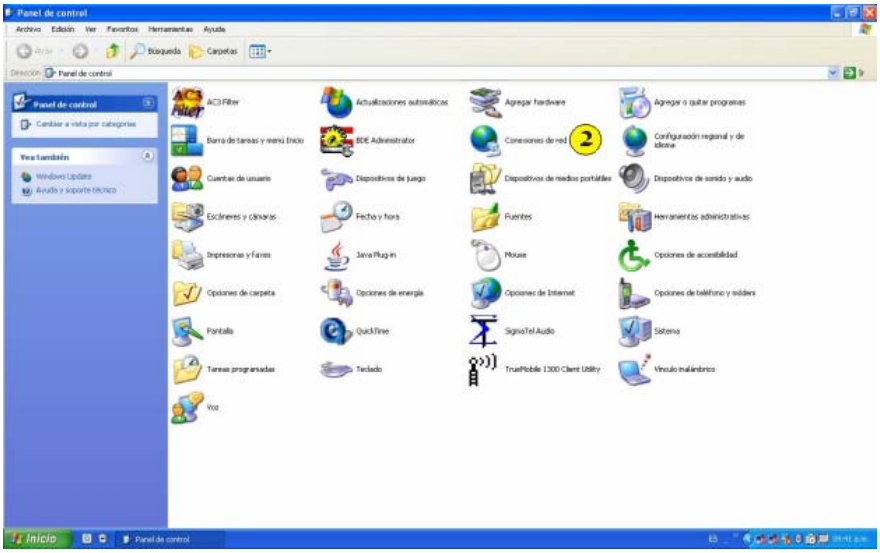
Para que una estación de trabajo tenga la posibilidad de obtener sus parámetros de configuración desde un servidor DHCP, es necesario que sus propiedades de conexión se encuentren habilitadas adecuadamente. A continuación se presentará una guía fácil que le permitirá a los usuarios habilitarse como clientes DHCP.

- **Clientes Windows XP.**

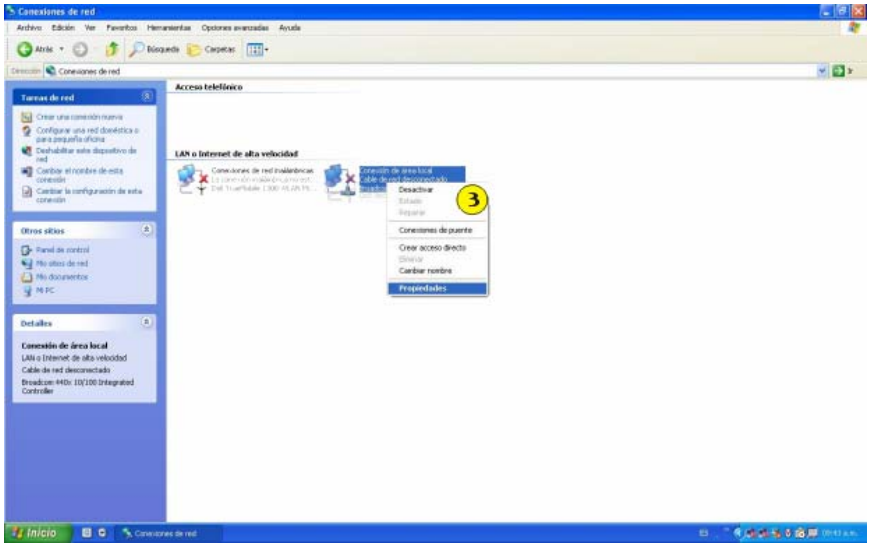
1. En el menú de inicio es necesario dirigirse a panel de control, donde se permiten personalizar las opciones del equipo.



2. Posteriormente, efectúe doble clic en la opción “conexiones de red”.



3. En el ícono de conexiones de área local, con click derecho podrá seleccionar “propiedades” lo cual le permitirá acceder a las propiedades de configuración.



4. Una vez realizada la anterior acción se visualizará la ventana de propiedades de conexión de area local, en “General” se selecciona el elemento “Protocolo Internet (TCP/IP)” y da clic izquierdo en propiedades.

NOTA: si dentro del listado de elementos que utiliza la conexión no aparece "Protocolo Internet (TCP/IP)", quiere decir que el equipo no es apto para operar en una red TCP/IP.

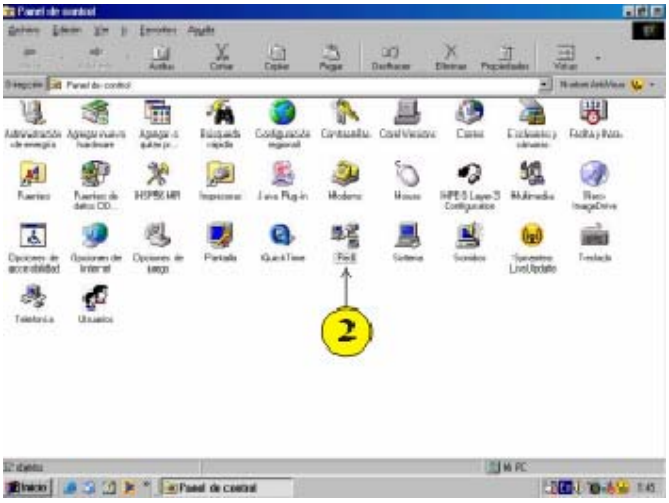
5. Al ingresar a las propiedades de Protocolo Internet (TCP/IP) habilite las opciones "Obtener una dirección IP automáticamente" y " Obtener la dirección del servidor DNS automáticamente", las cuales le permitirán obtener los parámetros de red adecuados desde un servidor DHCP.

Los equipos que trabajan con Sistema Operativo Windows XP no necesitan ser reiniciados después de modificar sus propiedades de conexión, al dar clic en "Aceptar" el equipo estará habilitado como cliente DHCP.

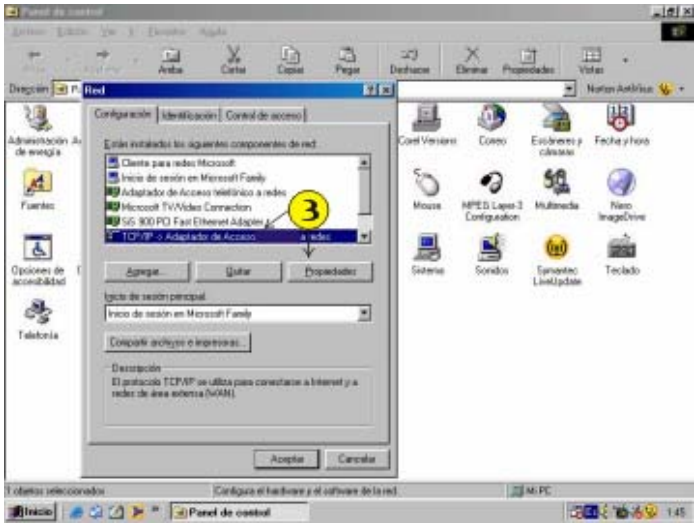
- **Clientes Windows 98.**

1. En inicio, despliegue las opciones en “Configuración” y seleccione “Panel de control”.

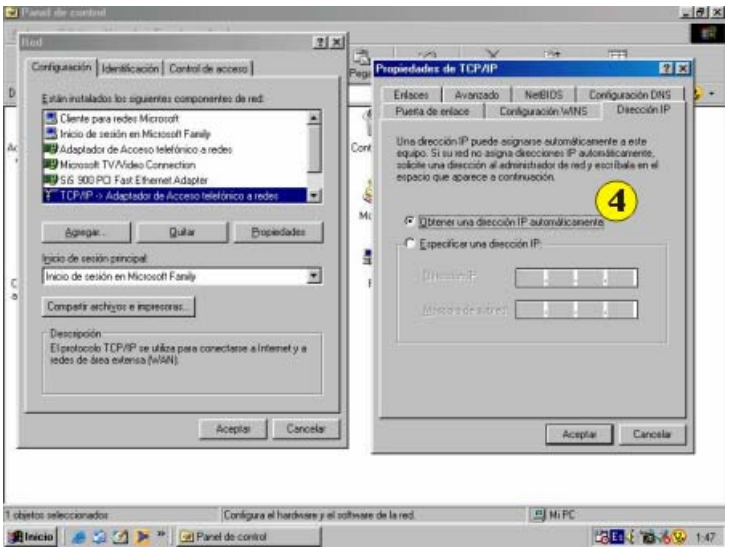
2. En panel de control, de doble clic en “Red”.



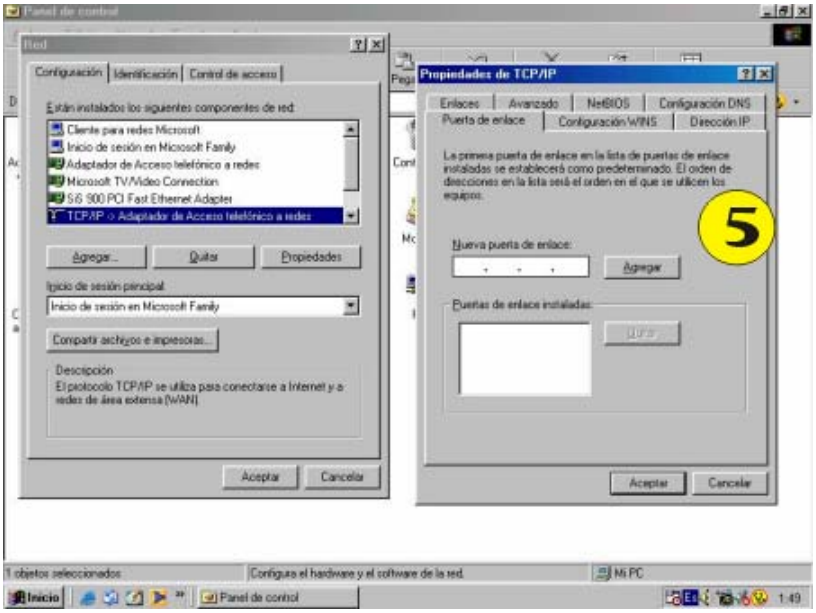
3. Una vez abierta la ventana de configuración de red, en la lista de componentes de red que se encuentran instalados, seleccione “Protocolo TCP/IP” y de clic en propiedades.



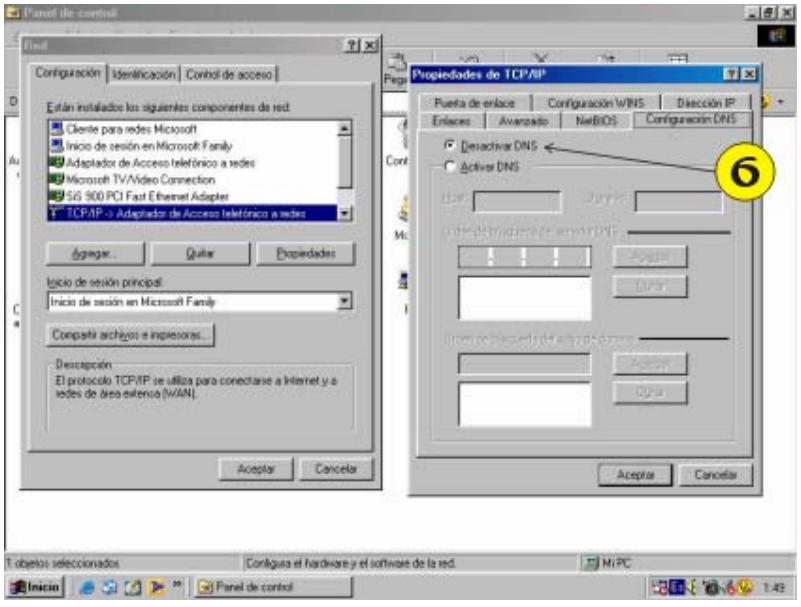
4. Dentro de las propiedades de TCP/IP, es necesario habilitar las opciones que le permitirán al equipo adquirir una dirección IP automáticamente. En la siguiente gráfica se muestra la opción para habilitar el equipo a que adquiera una dirección IP desde un servidor DHCP.



5. Recuerde que no debe tener definida ninguna dirección para la puerta de enlace, ya que éste es otro parámetro que será asignado por el servicio DHCP.



6. Es necesario desactivar el DNS, para que de esta manera sea posible la obtención de este parámetro desde un servidor DHCP.



7. Al terminar la configuración del equipo como cliente DHCP es necesario reiniciar el sistema.

ANEXO E

Elementos que brindarán soporte a los usuarios de la red

En el capitulo 5 se formularon las diferentes políticas que se implementarán conjuntamente con el servicio DHCP; como consecuencia a esto, se plantearon también diferentes elementos que van a facilitar a los usuarios el aprovechamiento de la red de datos institucional.

A continuación se presentan los mecanismos que ayudarán tanto a usuarios como a personal de soporte a solucionar inconvenientes frecuentes que se puedan presentar en la conexión.

El primero de ellos es una interfaz HTML, a la cual se podrá acceder desde la página web de la universidad. Dicha interfaz presenta la solución a las dudas más frecuentemente consultadas por los usuarios al personal de soporte de la red de datos de la universidad. Sin duda, ésta es una herramienta que prestará un gran beneficio a la comunidad universitaria, además, se le realizarán actualizaciones periódicas de acuerdo a las sugerencias de los usuarios. Así mismo, los usuarios podrán descargar un software desde esta web, que les permitirá conocer los parámetros de red que el servidor DHCP les ha asignado a sus estaciones de trabajo.

Otra forma de facilitar a los usuarios el entendimiento de algunos inconvenientes que se les pueden presentar con su conexión de red, consiste en la ubicación de un stiker en cada estación de trabajo, el cual presentará información de soporte para soluciones de actividades de red.

Por último se presenta el formulario que permitirá a la DSI llevar correctamente el proceso de migración hacia el servicio DHCP y que propiciará la recolección de la información necesaria para este fin.

PROBLEMAS DE CONECTIVIDAD A LA RED

Si ha venido experimentando inconvenientes a la hora de hacer uso de los servicios de red, antes de ponerse en contacto con el personal de Soporte Técnico siga los procedimientos descritos a continuación, los cuales le proporcionarán información valiosa cuando realice el reporte. Estos procedimientos se especifican para estaciones con Windows 98 y Windows XP.

- **Problemas con el Entorno de Red y el Grupo de Trabajo**

Lo que se observa en el Entorno de Red está directamente relacionado con su capacidad para hacer uso de impresoras o para compartir archivos con otros equipos de la red.

Windows 98:

1. Desde el escritorio, de clic en **ENTORNO DE RED** o **MIS SITIOS DE RED**, posteriormente en **TODA LA RED**. Una lista de equipos unidos a la red, grupos de trabajo y servidores aparecerá.

2. Si recibe el mensaje **"NO SE PUEDE EXAMINAR LA RED"** y no ha reiniciado el equipo, es necesario que lo haga. (Asegúrese de no presionar **CANCELAR** en cualquier prompt donde se solicite alguna contraseña, ya que si cancela el login de Windows, se puede evitar el acceso a la red)

3. Si aún así la red es inaccesible en **TODA LA RED**, proceda a revisar la conexión física de su computador.

Windows XP:

1. Desde el escritorio, dando doble clic en el icono de **MIS SITIOS DE RED,** donde aparecerán listados los equipos que actualmente hacen parte de su entorno de red.

2. En la parte izquierda de la ventana, dentro de las **TAREAS DE RED**, seleccione **VER EQUIPOS DEL GRUPO DE TRABAJO**. Si no aparece ningún equipo, quiere decir que usted o no pertenece a ningún grupo de trabajo en esos momentos o que posiblemente su problema se deba a algún fallo en la conexión física. Para solucionarlo, proceda a revisar la conexión física de su computador.

Conclusiones: Si los equipos conectados fueran visibles en TODA LA RED, usted ha confirmado que:

1. El toma de conexión (walljack) se encuentra activo.
2. Los cables están conectados.
3. La tarjeta de red se encuentra funcionando adecuadamente.

Por el contrario, si no logra conectarse con su Entorno de Red, continúe con la siguiente sección.

- **Problemas en el funcionamiento de TCP/IP.**

TCP/IP es el protocolo usado por todas las aplicaciones de Internet como e-mail, web browsers, telnet, etc.

Windows 98 y Windows XP:

1. Utilice una aplicación de Internet diferente, es decir, si el problema se está presentando con Outlook, utilice Internet Explorer o viceversa. Si lo intenta con Internet Explorer, la prueba más segura consiste en ingresar a una página web que no haya sido visitada recientemente. Podría intentarlo con http://ask.com o alguna otra que resulte fácil de digitar. Si cualquier aplicación de Internet funciona, entonces TCP/IP está operando adecuadamente y posiblemente su problema se deba a la mala configuración de Outlook.

2. Descargue el archivo HOST.exe y cópielo en el escritorio de su equipo, este archivo le permitirá conocer los parámetros de configuración de red de su equipo. Al ejecutarlo, le aparecerá una ventana como la siguiente:

- Si una dirección IP es mostrada en la anterior ventana, cerciórese que comience con el número "192.", de no ser así, el equipo no está recibiendo una dirección IP desde el servidor DHCP. Las direcciones IP que comienzan con "169." son erróneas. Si alguno de estos fenómenos se está presentando, continúe con Problemas de DHCP.
- La dirección MAC que aparecerá listada no proporciona información alguna acerca de la correcta configuración de red del equipo, sin embargo es importante que la recuerde para cuando se comunique con Soporte Técnico.

- **Problemas de DHCP.**

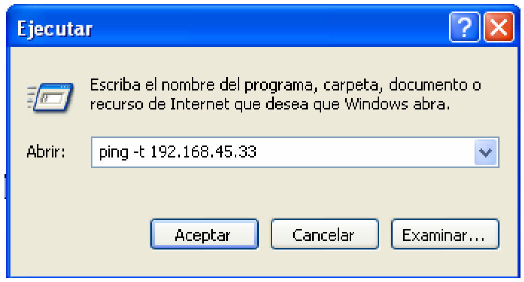
DHCP es usado para asignar direcciones IP a cada equipo dentro de una red, ya que sin ellas las aplicaciones de Internet no podrían funcionar. Generalmente, los problemas de conectividad debidos a DHCP pueden ser resueltos de manera más rápida si se proporciona la siguiente información al personal de Soporte Técnico cuando se haga el reporte.

1- **El problema que se ha encontrado se está presentando en más de un computador?** Algunas veces, los servicios de Internet podrán ser interrumpidos en la red de datos institucional o en un edificio o locación particular debido a mantenimiento o modificaciones que se están realizando, sin embargo, cerciórese de que otros computadores cercanos al suyo estén habilitados para revisar emails o para conectarse a páginas web, si no es así, puede que exista un problema que debe ser reportado a la División de Servicios de Información, para lo cual debe comunicarse con la extensión 2558.

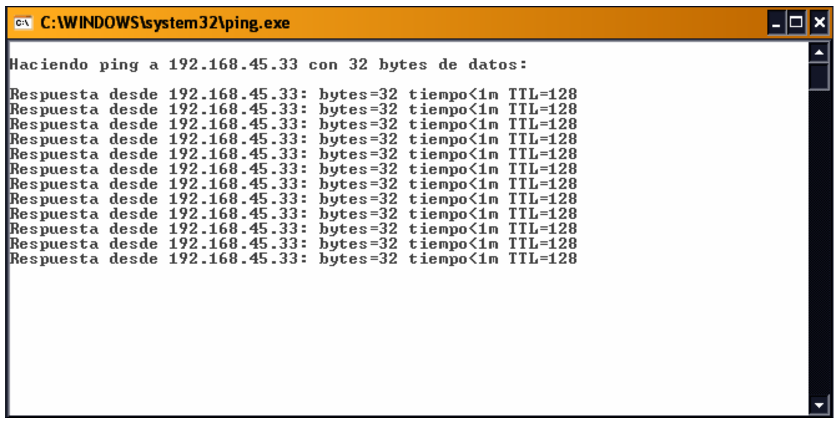
2- **Algún otro equipo está utilizando su dirección IP?** Cuando esto suceda, usted estará totalmente impedido para establecer conectividad con cualquier otro equipo de la red o para hacer uso de los diferentes servicios de Internet. Sin embargo, es posible que usted pueda obtener cierta información que es valiosa a la hora de realizar el reporte. A continuación se indican ciertos procedimientos que ayudarán a detectar si alguien más está haciendo uso o no de su dirección IP y posiblemente detectará cual equipo es el equipo responsable.

1. Desde otro computador que sí tenga servicio de Internet, siga la ruta **INICIO/EJECUTAR**

2. Digite el comando "**ping –t"** seguido de la dirección IP que usualmente le ha sido asignada y de clic en **Aceptar**.



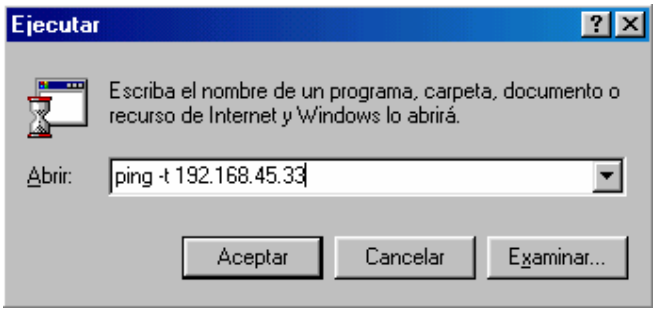
3. Si recibe respuesta desde esa dirección, debe observar una ventana como la que se muestra a continuación y es evidente que su dirección IP se encuentra siendo usada en esos momentos.



Windows 98:

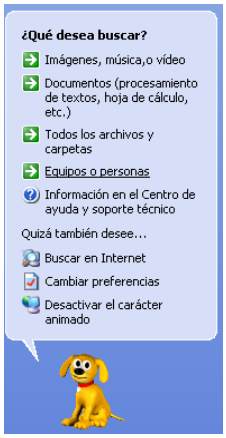
1. Desde un computador que sí tenga acceso a Internet, siga la ruta **INICIO/EJECUTAR**

2. Digite el comando "**ping –t**" seguido de la dirección IP que usualmente le ha sido asignada y de clic en **Aceptar**.

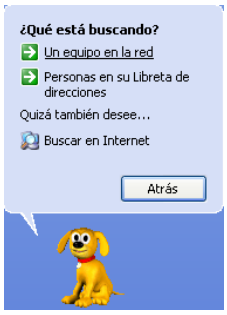


Windows XP:

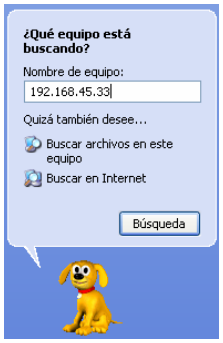
1. Siguiendo la ruta **INICIO/BUSCAR,** se abrirá la ventana de búsqueda, dónde aparece una ventana en la que se le preguntará **¿Qué desea buscar?,** seleccione la opción **EQUIPOS O PERSONAS.**



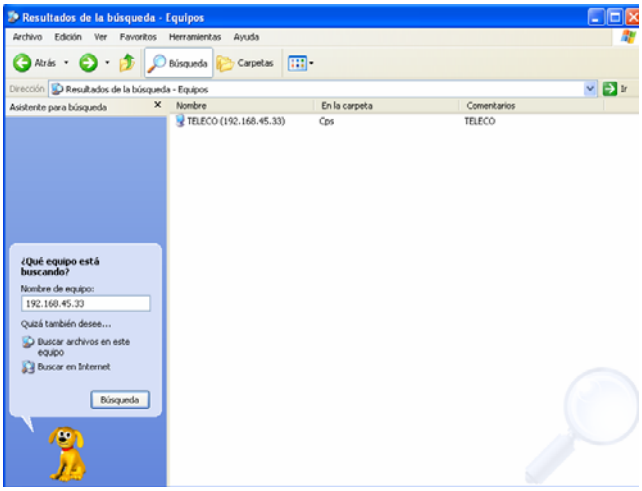
2. Posteriormente se mostrará otro menú de opciones, en el que se le pregunta **¿Qué está buscando?**, seleccione la opción **Un equipo en la red.**



3. Después de esto, usted podrá observar una ventana donde se le pregunta **¿Qué equipo está buscando?**. En el espacio en blanco, escriba la Dirección IP que generalmente se le ha asignado y de clic en **Búsqueda**.



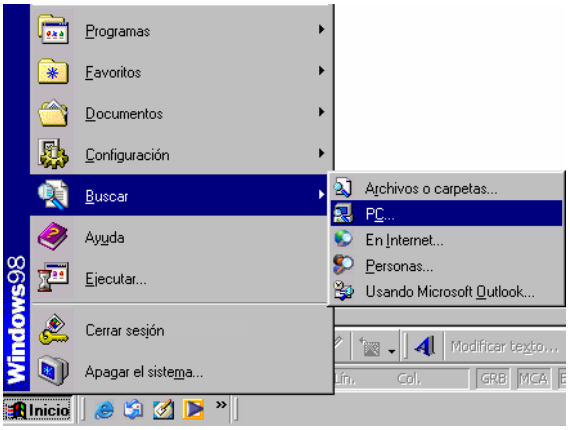
4. Al realizar la anterior acción usted debe observar una ventana como la que se muestra a continuación, en la que se muestra información referente al equipo que se encuentra haciendo uso de su dirección IP actualmente, recuerde dicha información y adjúntela a su solicitud, para lo cual debe comunicarse con la extensión 2558 o enviar la solicitud en linea.



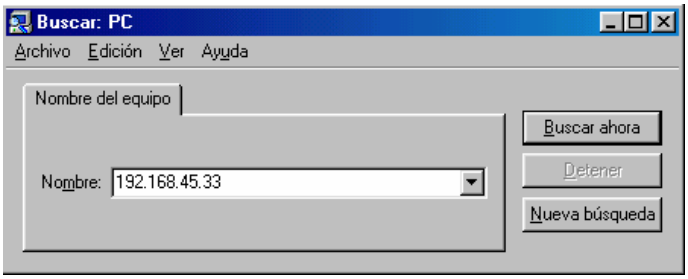
5. Finalmente, si usted ha determinado que el problema de conectividad de su equipo se debe a DHCP, es importante que lo reporte inmediatamente al personal de Soporte Técnico de la División de Servicios de Información de la Universidad, para esto, comuníquese con las extensiones 2567,2164 o 2558 o envíe su Solicitud En-linea.

Windows 98

1. Siguiendo la ruta **INICIO/BUSCAR/PC**



2. Digite la dirección IP que usualmente le ha sido asignada y de clic en **Buscar ahora**.



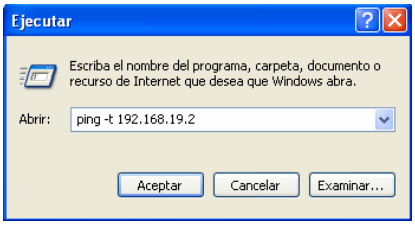
3. Posterior a esto, se abrirá una ventana donde se visualizará información importante del equipo que actualmente está haciendo uso de su dirección IP, por lo tanto es importante que usted tenga en cuenta esta información cuando realice el reporte con el personal encargado en las extensiones 2567,2164 o 2558 o envíe su Solicitud En-linea.

- **Problemas del DNS.**

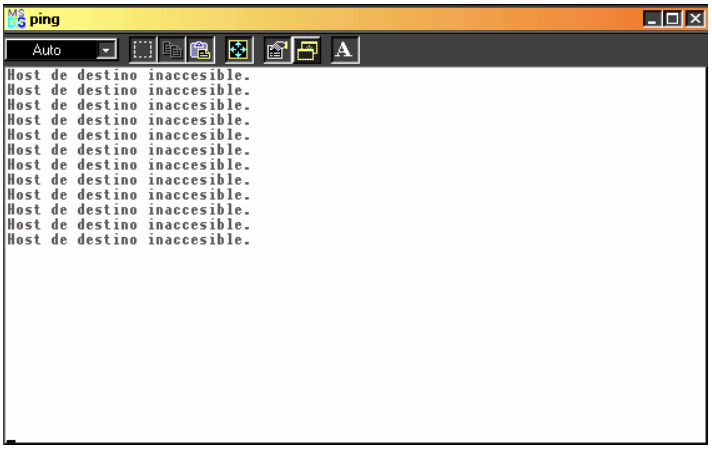
Si el DNS no se encuentra funcionando, usted estará habilitado para adquirir una dirección IP desde el servidor DHCP, pero no podrá contactar páginas de Internet como www.uis.edu.co

Windows 98 y Windows XP

Para verificar si su problema de conectividad se debe a alguna interrupción en el servicio DNS, siga la ruta **INICIO/EJECUTAR** y digite "**ping –t 192.168.19.2**", posteriormente de clic en **ACEPTAR**, como se aprecia en la imagen siguiente:



Si desde su computador usted visualiza una ventana como la que se muestra a continuación, es evidente que el servidor DNS se encuentra fuera de servicio, por lo tanto, usted no debe reportar este fallo a la División de Servicios de Información y deberá esperar a que el personal encargado solucione este problema.



Conclusiones: si sólo una aplicación de Internet se encuentra fallando, el problema es ocasionado por algún fallo en ella misma. Si ninguna aplicación de Internet funciona correctamente, pero usted sabe que la conexión física está bien ya que el entorno de red es reconocido, entonces probablemente el origen del problema es algún fallo del servicio DHCP, un problema de configuración o quizás se deba a la interrupción del funcionamiento de un router de la red institucional. Si determina que la configuración TCP/IP presenta fallos y que el entorno de red tampoco se encuentra, proceda a detectar problemas en la conexión física.

- **Problemas en la conexión física.**

1. Siga el cable de red desde la parte posterior de su computador hasta el toma en el que se conecta a la canaleta. Normalmente se encontrarán conectados 2 computadores en cada toma, por lo tanto es necesario que esté totalmente seguro que el que usted revise corresponda al de su computador.

2. Revise una luz titilante en la tarjeta de red en la parte trasera de la CPU de su computador. Al lugar donde se encuentra conectado el cable de red, deben haber al menos 2 luces: una que permanece encendida constantemente y que indica si se está conectado a la red y otra, la cual titila indicando el tráfico de la red que atraviesa la tarjeta de red.

3. Si usted puede observar las luces descritas anteriormente, es correcto afirmar que el toma de red se encuentra activo y que la conexión física está bien, por lo tanto proceda a revisar Problemas en la tarjeta de red.

4. Si no observa que las luces de enlace y tráfico de la tarjeta de red se encuentran encendidas, consiga un cable de red que usted conozca que se encuentra en buen estado y pruébelo en su computador y revise nuevamente si las luces de la tarjeta de red se encuentran encendidas.

5. Si estas luces encienden, desconecte por un momento el cable de red y observe si se apagan, de no ser así, proceda a Problemas en la tarjeta de red.

6. Si es posible, **conecte otro computador conocido a trabajar en la red desde el mismo toma** al que se encuentra conectado su computador. Si aún así usted no obtiene conexión, es probable que el toma no se encuentre activo en ese momento, por lo tanto debe comunicarse con el personal encargado de la División de Servicios de Información a la extensión 2558 o envíe su Solicitud en línea.

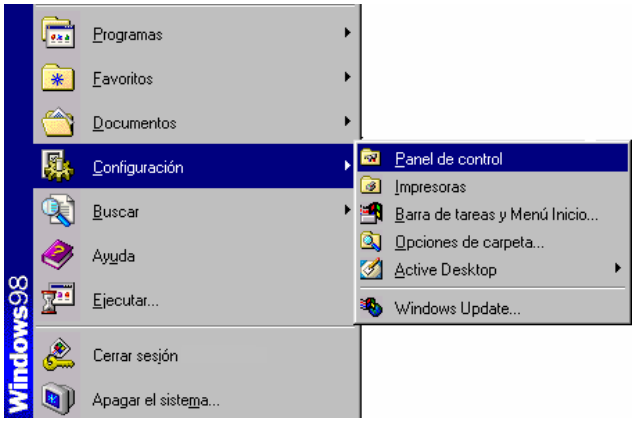
- **Problemas en la tarjeta de red.**

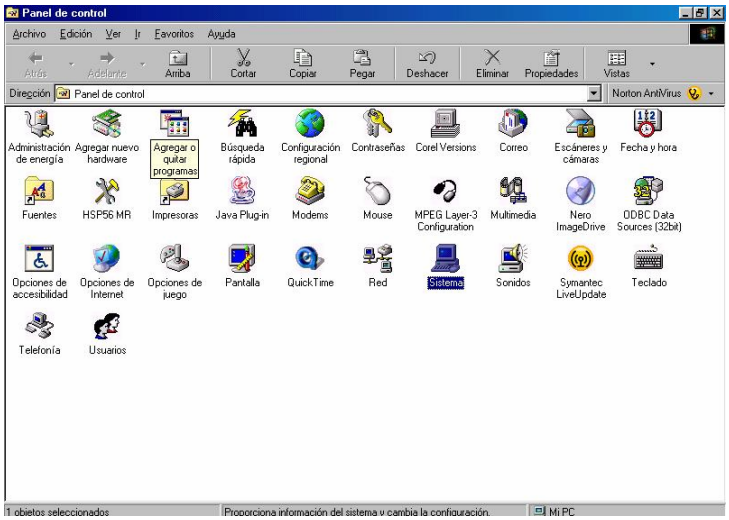
La tarjeta de interfaz de red (NIC) proporciona la interfaz física entre el computador y la red. Use el administrador de dispositivos para revisar los drivers instalados para la tarjeta.

1. **Diríjase al administrador de dispositivos en el Panel de Control** para verificar que los drivers de la tarjeta de red estén correctamente instalados.

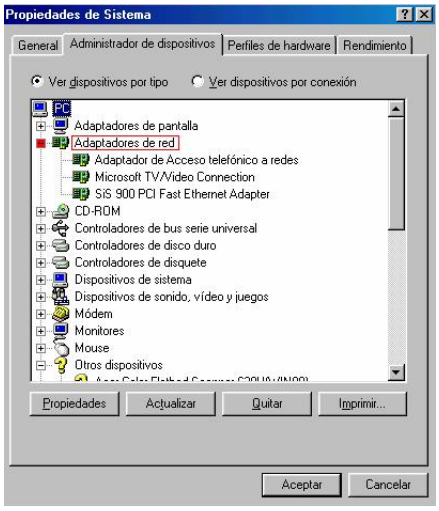
Windows 98

2. Siga la ruta **Inicio/Configuración/Panel de control** y desde ahí de clic en **Sistema.**





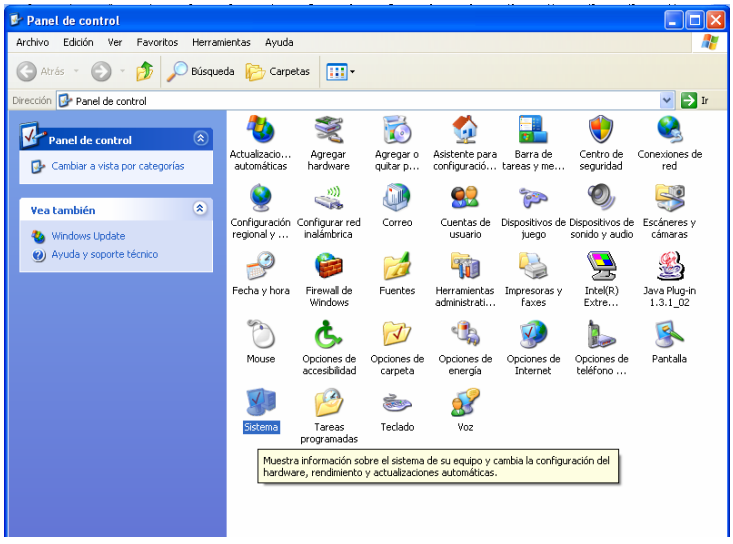
3. De clic en **Administrador de Dispositivos.**



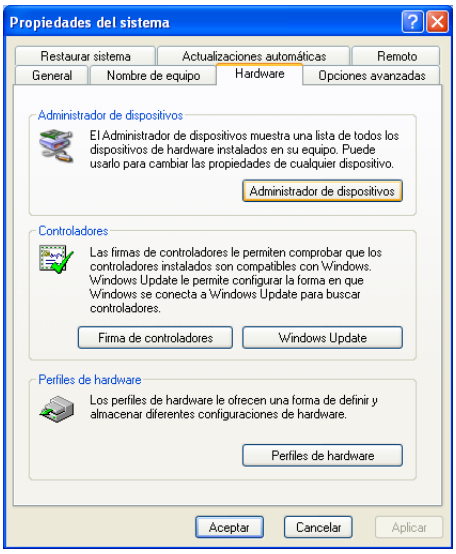
4. Desde ahí de clic sobre el signo **"+"** frente a **ADAPTADORES DE RED.** Usted debe observar entonces una lista de los dispositivos de la tarjeta de red. Si usted ve un signo de exclamación amarillo ubicado frente al listado, significa que existe algún problema con los drivers o un conflicto de recursos. Por lo tanto, es necesario remover y posteriormente reinstalar correctamente los drivers.

Windows XP

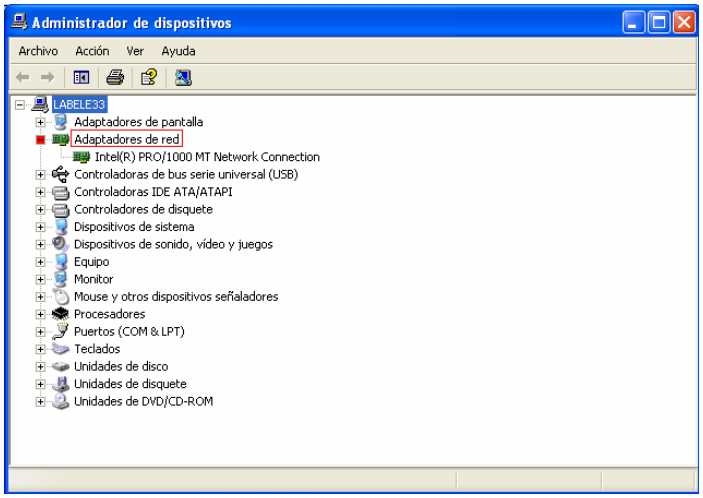
1. Siga la ruta **Inicio/Panel de control** y desde ahí de clic en **Sistema.**



2. Seleccione la página **HARDWARE** y de clic en la opción **ADMINISTRADOR DE DISPOSITIVOS.**



3. Posteriormente, se abrirá la ventana mostrada a continuación. Desplegando las opciones en **ADAPTADORES DE RED** se podrá observar el nombre de la interfaz de red que se encuentra instalada, si no se observa nada anormal, es decir, no existe una anotación que indique problemas en la configuración de ella, se considera que la tarjeta de red esta correctamente instalada en el computador.



Conclusiones: si usted pudo identificar que el toma de la canaleta se encuentra activo, pero la configuración TCP/IP y el entorno de red aún no funcionan, el única alternativa es reinstalar o remplazar la tarjeta de red.

- Sticker de soporte para servicios de red.

- Ventana de visualización de HOST.exe:

- Formulario para inscripción de equipos al servicio DHCP.

UNIVERSIDAD INDUSTRIAL DE SANTANDER

DIVISION DE SERVICIOS DE INFORMACION - DSI

Formulario para inscripción de equipos al servicio DHCP

Dir. De red:_____ Ubicación:_____ Nombre:_____

	DIRECCIÓN FÍSICA (MAC)	HOSTNAME	No. INVENTARIO	DIR. IP ACTUAL	SIST. OPERATIVO	OBSERVACIONES (Ubicación y Responsable)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						

ANEXO F
Configuración del Servidor DHCP

Para ejecutar el servicio DHCP es necesario instalar el demonio dhcpd, el cual, una vez instalado y configurado, se puede manipular con el *script* del mismo nombre en el directorio /etc/rc.d/init.d.

La configuración del servicio se hace a través del fichero /etc/dhcpd.conf, donde se establecen los campos que se asignan a través del servicio a los clientes. Una vez iniciado, dhcpd lee este fichero y almacena en memoria una lista de las direcciones disponibles en cada subred. El funcionamiento del servidor DHCP está dirigido por el correcto manejo e interacción entre dos ficheros, el dhcpd.leases y dhcpd.conf.

1. FICHERO dhcpd.conf

El fichero de configuración de dhcpd, se encuentra en la ruta /etc/dhcpd.conf y consta de un conjunto de sentencias, las cuales se clasifican en parámetros y declaraciones. Los parámetros expresan cómo hacer algo, si se hace algo o no, así como los atributos que se le asignan al cliente. Las declaraciones, en cambio, se emplean para describir la topología de la red, a un conjunto de clientes o para aplicar determinados parámetros a un grupo de declaraciones. Las declaraciones tienen la forma:

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

y los parámetros:

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

Los parámetros que inician con la palabra reservada “option” describen aquellos datos que brinda el servidor al cliente como parte del protocolo, es decir las opciones DHCP, y los que no, describen y controlan las características del servidor DHCP (ejemplo, tiempo de lease)

1.1 SENTENCIAS DECLARATIVAS

A continuación se describen las sentencias declarativas:

- **shared-network**

Permite agrupar un conjunto de subredes que compartan la misma red física. El único atributo de esta sentencia es un nombre que sólo se utiliza para las trazas del servicio. Es necesaria siempre que se utilice agente relay.

Sintaxis:

```
shared-network <nombre> {
[parámetros]
[declaraciones]
}
```

- **subnet**

Permite agrupar las características que van a tener los clientes de una misma subred; pueden declararse varios rangos.

Sintaxis:

```
subnet <dirección de red> netmask <máscara de red> {
```

[parámetros]
[declaraciones]
}

- **range**

Permite definir un rango de direcciones IP a otorgar a clientes pertenecientes a una subred. Si se especifica el atributo dynamic-bootp se indica que estas direcciones se pueden asignar también a clientes BOOTP. Cuando se especifica una sola dirección IP se omite la dirección máxima.

Sintaxis:

range [dynamic-bootp] <dirección IP mínima> [dirección IP máxima]

- **host**

Permite describir aquellos *hosts* a los que se les asignará su dirección manualmente. Todos los clientes que usan BOOTP deben tener asociada una sentencia host. Un cliente se corresponde con una declaración host si la opción dhcp-client-identifier indicada en la declaración posee el valor del identificador que brinda el cliente a través del protocolo. De no ser así entonces se emplearía la dirección MAC del cliente especificada a través de el atributo hardware; dentro de una subred, un cliente con “host” puede trabajar con diferente nombre de dominio y diferente nombre de dominio de servidor definida para la subred.

Sintaxis:

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

- **group**

Permite agrupar a otras declaraciones para aplicarles varios parámetros comunes. Puede ser utilizada para agrupar *hosts*, subredes, redes compartidas y otros grupos.

Sintaxis:

```
group {
  [parámetros]
  [declaraciones]
}
```

1.2 PARÁMETROS

Los parámetros principales son:

- **lease-file-name <filename>;**

Indica el nombre del fichero donde se almacenan los contratos. Este parámetro tiene alcance global por lo que se debe especificar fuera de todos los ámbitos (declaraciones) para que tenga efecto real. Por defecto es /var/lib/dhcp/dhcpd.leases

- **default-lease-time <time>;**

Expresa el tiempo en segundos por defecto que tendrán los contratos a los clientes que no soliciten un tiempo específico para la expiración de sus contratos.

- **max-lease-time <time>;**

Expresa en segundos la duración máxima de un contrato, necesario cuando los clientes solicitan lease.

- **min-lease-time <time>;**

Expresa en segundos la duración mínima de un contrato.

- **min-seconds <seconds>;**

Indica el número de segundos que debe esperar el servidor de DHCP para responder al pedido de los clientes. Se utiliza cuando se tiene un segundo servidor y se desea que este responda después que el otro haya hecho su oferta al cliente.

- **hardware <type> <address>;**

Indica la dirección física (MAC) de un cliente particular (declaraciones tipo host). El atributo type expresa el tipo de arquitectura de la interfaz de red, actualmente puede ser: *ethernet* o *token-ring*. La dirección MAC se expresa utilizando seis números hexadecimales (números desde 00 hasta ff) separados por el caracter "**;**".

- **server-name <servername>;**

Indica el nombre que se ofrecerá a los clientes como identificador del servidor que emplean.

- **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.

- **dynamic-bootp-lease-cutoff <date>;**

Indica la fecha en que expiran los contratos de todos los clientes BOOTP. Como se ha expresado anteriormente los contratos con este tipo de cliente no expiran nunca ni se renuevan pero puede que en ciertas situaciones sea necesario interrumpirlos. El formato del atributo date es idéntico al que se emplea en el fichero de contratos descrito anteriormente.

- **get-lease-hostnames <flag>;**

Indica si el servidor resolverá o no las direcciones IP de los clientes a nombres de dominio y usará estos nombres como la opción host-name del protocolo. Si el valor es verdadero entonces la resolución se hará para todas las direcciones en el mismo alcance (*scope*). Un valor verdadero se expresa con “on”, mientras que falso se indicará con “off”. Por defecto es falso.

- **use-host-decl-names <flag>;**

Indica si se asume que el nombre provisto en cada una de las declaraciones tipo host dentro del mismo ámbito, es el nombre del cliente correspondiente (opción host-name del protocolo).

- **authoritative;**
- **non authoritative;**

Indican si el servidor está autorizado o no para realizar sus funciones. Por defecto un servidor DHCP asume que la información que brinda a una subred determinada no es correcta ni está autorizado para ello. Esto permite que si un usuario inexperto instala un servidor de DHCP en la red este no sea escuchado por los clientes como lo es un servidor legítimo que se le indique explícitamente que está autorizado. El administrador de red que configure adecuadamente su servidor debe colocar este parámetro al comienzo del fichero, aunque puede ser conveniente en algunas ocasiones declarar al servidor autorizado de acuerdo a los segmentos de red definidos y no de forma global.

- **always-broadcast <flag>;**

Se emplea para algunos clientes de DHCP/BOOTP que no recepcionan las respuestas del servidor si no son en forma de *broadcast*. Se debe tratar de colocar este parámetro a ``on'' sólo para los clientes que realmente lo necesiten pues provoca demasiado tráfico en la red.

- **ddns-update <flag>;**

Indica si se realizan o no actualizaciones dinámicas al DNS siempre que se establezca un contrato. Por defecto este parámetro tiene valor “on”.

- **allow <request>;**
- **deny <request>;**
- **ignore <request>;**

Se emplean para controlar la respuesta del servidor de DHCP ante distintos tipos de pedidos: allow permite, deny niega e ignore ignora la solicitud. Algunas de las posibles solicitudes (atributo request) son:

*** unknown-clients :** se emplea para indicar al servidor si acepta o no las solicitudes de los clientes desconocidos. Un cliente desconocido es aquel que no tiene asociado una declaración tipo host. Por defecto las solicitudes de estos clientes se aceptan.

*** bootp :** se utiliza para señalar si se aceptarán o no los pedidos de los clientes BOOTP. Por defecto se aceptan.

*** booting :** se emplea en las declaraciones del tipo host para indicar si se aceptará o negará la solicitud del *host* correspondiente, es decir restringir un cliente particular. Por defecto se aceptan para todos los *hosts*.

*** declines :** se utiliza para indicar si el servidor acepta o no los mensajes del tipo DHCPDECLINE de los clientes. Cuando un servidor recibe este tipo de mensajes asume que la dirección que ofrece no es válida pues al parecer alguien no autorizado la está utilizando y entonces la declara como abandonada. Desafortunadamente un cliente "malicioso'' o con una implementación incorrecta puede agotar todo el *spool* de direcciones a otorgar que posee el servidor y antes de que este decida emplear las direcciones abandonadas ya se habrán provocado algunos trastornos en el servicio.

1.3 OPCIONES DE DHCP

Entre los parámetros que se le pueden otorgar a un cliente a través del protocolo y que van precedidos por la palabra "option", se encuentran:

- **option domain-name <domain name>;**

Indica el nombre del dominio que empleará el cliente.

- **option domain-name-servers <ip address> [, <ip address> ...];**

Indica los servidores de nombres de dominio a emplear por el cliente.

- **option host-name <hostname>;**

Indica el nombre que empleará el *host* cliente.

- **option subnet-mask <ip address>;**

Indica la máscara de red que se le asignará al cliente.

- **option routers <ip address> [, <ip address> ...];**

Indica las direcciones IP de los *routers* (*gateway*) que empleará el cliente.

- **option broadcast-address <ip address>;**

Indica la dirección de *broadcast* que utilizará el cliente.

- **option dhcp-client-identifier <string>;**

Indica el identificador que puede emplear el cliente como alternativa a su dirección MAC.

2. FICHERO dhcpd.leases

Con el objetivo de recordar los contratos establecidos, siempre que se renueve el servicio, dhcpd los almacena en forma de base de datos en un fichero nombrado dhcpd.leases y que se guarda en el directorio /var/lib/dhcp; el fichero de contratos tiene un formato de texto ASCII y contiene todas las declaraciones de los contratos efectuados por asignación dinámica. Siempre que un contrato se establezca, se renueve o expire se genera una nueva entrada al final del fichero; por tanto si aparece más de una entrada para un mismo contrato se asume como válida la que se encuentre más cercana al final del fichero.

Cuando se instala dhcpd, normalmente no existe la base de datos de contratos (dhcpd.leases), sin embargo ésta es imprescindible para que el servicio inicie correctamente. Para crear el fichero, se utiliza desde el terminal de comandos:

```
# touch /var/lib/dhcp/dhcpd.leases
```

Para prevenir que el fichero de contratos crezca indefinidamente, cada cierto tiempo todos los contratos conocidos son trasladados hacia otro con el nombre dhcpd.leases~, y entonces se comienzan a almacenar los nuevos contratos en el fichero principal.

El fichero de contratos consta sólo de un tipo de sentencias. Estas tienen la forma:

lease <dirección IP> { <sentencias> }

Las sentencias, que se separan por el caracter "**;**", definen a quién se le asignó el contrato y que tiempo durará éste. A continuación se listan y ejemplifican las principales sentencias:

- ***starts <fecha>;***
- ***ends<fecha>;***

Las cuales especifican las fechas de comienzo y final del contrato. Estas fechas poseen el siguiente formato:

W YYYY/MM/DD HH:MM:SS

Donde:

W es el día de la semana. Se especifica con números entre 0 y 6 donde el 0 se corresponde con el domingo.

YYYY/MM/DD es la fecha formada por el año, que se expresa con cuatro dígitos, el mes, que oscila entre 1 y 12, y el día que lo hace entre 1 y 31.

HH:MM:SS representa el tiempo formado por la hora que se moverá en el rango de 0 a 23, y los minutos y segundos, que lo harán de 0 a 59.

Las anteriores fechas se especifican de acuerdo al uso horario de *Greenwich* (GMT : *Greenwich Mean Time*) y no del tiempo local.

- ***Hardware <tipo> <dirección MAC>;***

Permite indicar la dirección MAC de la interfaz de red del cliente con el que se hizo el contrato. Las direcciones MAC se expresan utilizando seis números hexadecimales separados por dos puntos.

- ***Uid <identificador>;***

Es otro parámetro que permite identificar al cliente.

- ***client-hostname <nombre del host>;***

Almacena el nombre de *host* del cliente. Se refiere a los nombres del DNS.

- ***hostname <nombre del host>;***

Almacena el nombre de *host* del cliente, pero esta sentencia hace referencia a los nombres *NetBios* de los ambientes Windows.

- ***abandoned;***

Esta sentencia se emplea para indicar que una dirección está siendo mal usada debido a que el cliente que la poseía la abandonó o que el servidor al tratar de reasignar dicha dirección descubrió que estaba siendo utilizada por un cliente no autorizado. Las direcciones abandonadas son reasignadas únicamente cuando ya no quedan direcciones libres disponibles.