TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

DESARROLLO DE PRÁCTICAS CON IPv6

Este anexo describe las practicas desarrolladas como soporte a la teoría descrita en la monografía del trabajo de grado “IPv6 para manejo de redes multiservicio”. Las prácticas se realizaron utilizando el sistema operativo Windows XP Y Windows 2000 junto con el stack del protocolo IPv6 para Windows 2000, el cual se puede obtener de la página de Microsoft MSDN online:

http://msdn.microsoft.com/downloads/sdks/platform/tpipv6/start.asp

Nota: El sistema operativo Windows XP ya trae el stack del protocolo IPv6.

D.1 Características del protocolo IPv6 para Windows XP/2000.

El protocolo IPv6 para Windows XP/2000 incluye las siguientes características:

- Túnel 6to4
- Protocolo de direccionamiento automático de túnel dentro de un sitio
- Túnel 6over4
- Direcciones anónimas
- Prefijos de sitio en los anuncios de enrutador
- Compatibilidad con DNS
- Compatibilidad con IPSec
- Compatibilidad con aplicaciones
- Compatibilidad con RPC
- Compatibilidad con enrutador estático

D.2 Instalación y configuración del protocolo IPv6 en Windows XP.

A continuación se describirá paso por paso la forma de instalar el protocolo en Windows XP, y la forma de configurar el protocolo para sus diferentes formas de funcionamiento.

D.2.1 Instalación del protocolo IPv6 en Windows XP.

1. Abra el símbolo del sistema (command).
2. En el símbolo del sistema, escriba:

   ipv6 install

D.2.2 Configuración los atributos de la interfaz

1. Abra el símbolo del sistema.
2. En el símbolo del sistema, escriba:

   ipv6 if, Para obtener el índice de la interfaz cuyos atributos va a configurar

Cuando se teclea ipv6 if, se puede ver una lista de todas las interfaces IPv6:

Interfaz 1 es una pseudo–interfaz que se usa para el loopback (llamada la interfaz Loopback Pseudo–Interface).
Interfaz 2 es una pseudo–interfaz que se usa por túneles automáticos (llamada la interfaz Automatic Tunneling Pseudo–Interface).
Interfaz 3 es una pseudo–interfaz que se usa para túneles 6to4 (llamada la interfaz 6to4 Tunneling Pseudo–Interface).

Otras interfaces son enumeradas secuencialmente en el orden en el que ellas se crean. Este orden varía entre una computadora y otra.

Las interfaces con una dirección link–layer de la forma aa-bb-cc-dd-ee-ff son interfaces Ethernet o Fiber Distributed Data Interface (FDDI). Por ejemplo, se tendrá una interfaz Ethernet para cada adaptador de Ethernet instalado en la computadora. Las direcciones de enlace local (link–local) se dirigen de una interfaz Ethernet que usa el identificador de interfaz IPv6 derivado de la dirección de control de acceso al medio Ethernet (Emac).

3. En el símbolo del sistema, escriba:

   ipv6 ifc ÍndiceDeInterfaz [atributo]

   Donde índiceDeInterfaz es el número de la interfaz y atributo es uno o varios de los atributos siguientes:

   - forwards

   Habilita el reenvío de los paquetes recibidos en esta interfaz.

   - -forwards

   Deshabilita el reenvío de los paquetes recibidos en esta interfaz.

   - advertises

   Habilita el envío de mensajes de anuncio de enrutador en la interfaz.

   - -advertises

   Deshabilita el envío de mensajes de anuncio de enrutador en la interfaz.

   - mtu bytes

   Establece el tamaño en bytes de la unidad máxima de transmisión para el vínculo, que se envía como la opción MTU en el mensaje de anuncio de enrutador.

- site identificadorDelSitio

  Establece el identificador del sitio. El identificador del sitio sirve para distinguir entre interfaces que pertenecen a diferentes regiones administrativas que utilizan direcciones locales del sitio.

D.2.3 Como ver la configuración de la interfaz.

1. Abra el símbolo del sistema.
2. En el símbolo del sistema, escriba:

   ipv6 if

D.2.4 Como configurar IPv6 con direcciones manuales.

1. Abra el símbolo del sistema.
2. En el símbolo del sistema, escriba:

   ipv6 if

   Para obtener el índice de la interfaz a la que va a agregar una dirección manual.

3. En el símbolo del sistema, escriba:

   ipv6 adu [índiceDeInterfaz]/[dirección]

   En donde índiceDeInterfaz es el número de la interfaz y dirección es la dirección IPv6. Existen parámetros adicionales para la línea de comandos.

D.2.5 Como agregar una ruta IPv6.

1. Abra el símbolo del sistema.
2. En el símbolo del sistema, escriba:

   ipv6 if

   Para obtener el índice de la interfaz a través de la que se puede llegar a las direcciones del prefijo de ruta.

3. En el símbolo del sistema, escriba:

   ipv6 rtu prefijo índiceDeInterfaz/direcciónDeSaltoSiguiente

   Donde:

   - Prefijo es el prefijo de la ruta.

- IndiceDeInterfaz es el número de la interfaz.
- DirecciónDeSaltoSiguiente es la dirección de un enrutador local.

D.3 Desarrollo de las prácticas utilizando los atributos de Windows XP.

Las siguientes prácticas se desarrollaron utilizando las características para soportar IPv6 implementadas en el sistema operativo Windows XP/2000. Utilizando diferentes tipos de configuración y utilizando las direcciones establecidas en cada interfaz se implementaron varias practicas que permitieron ir estableciendo una base para el desarrollo de practicas mas avanzadas como la implementación de la Isla IPv6 y el servidor Web IPv6, es así como comenzando desde una simple conexión de dos equipos sobre el mismo segmento de red se llego a la implementación de toda una red (Isla) IPv6 utilizando un equipo con Windows XP con pila dual, u equipo con Windows 2000 server y varios host con pila dual.

D.3.1 Práctica No 1: Subred única con direcciones locales del vínculo.

Esta configuración sólo requiere la instalación del protocolo IPv6 en al menos dos nodos del mismo segmento de red como se observa en la Figura D.1 (también denominado vínculo o subred) sin enrutadores intermedios.

En la Figura D.1 se muestra la configuración de dos nodos de una subred única con direcciones locales del vínculo.

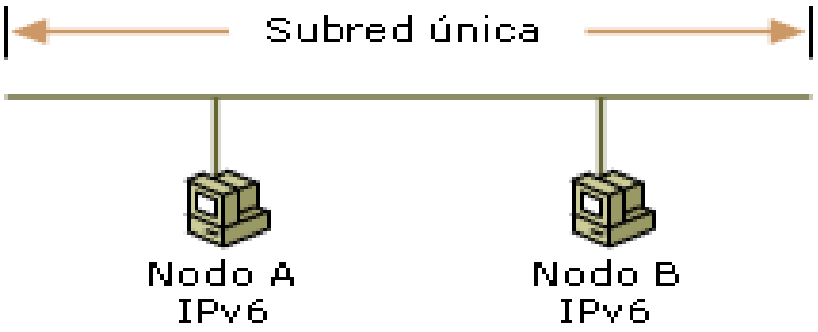

Figura D.1 Configuración de dos nodos de una subred única

De forma predeterminada, el protocolo IPv6 para Windows XP configura direcciones locales de vínculo para cada interfaz correspondiente a un adaptador de red Ethernet instalado. Las direcciones locales de vínculo tienen el prefijo de FE80::/64. Los últimos 64 bits de la dirección IPv6 se denominan identificador de interfaz. Se deriva de la dirección MAC de 48 bits del adaptador de red.

Para crear el identificador de interfaz IPv6 a partir de la dirección MAC de Ethernet de 48 bits (6 bytes) se procede de la siguiente manera:

- Los dígitos hexadecimales 0xFF-FE se insertan entre el tercer y cuarto byte de la dirección MAC.
- Se complementa el bit Universal o local (el segundo bit de orden inferior del primer byte de la dirección MAC). Si es 1, se establece en 0; y si es 0, se establece en 1.

Por ejemplo, para la dirección MAC de 00-60-08-52-F9-D8:

- Los dígitos hexadecimales 0xFF-FE se insertan entre 0x08 (el tercer byte) y 0x52 (el cuarto byte) en la dirección MAC, con lo que se forma la dirección de 64 bits de 00-60-08-FF-FE-52-F9-D8.
- Se complementa el bit Universal o local, el segundo bit de orden inferior de 0x00 (el primer byte) de la dirección MAC. El segundo bit de orden inferior de 0x00 es 0 que, una vez complementado, se convierte en 1. El resultado es que, para el primer byte, 0x00 se convierte en 0x02.

En consecuencia, el identificador de interfaz IPv6 que corresponde a la dirección MAC de Ethernet de 00-60-08-52-F9-D8 es 02-60-08-FF-FE-52-F9-D8.

La dirección local de vínculo de un nodo es la combinación del prefijo FE80::/64 y el identificador de interfaz de 64 bits expresado en notación hexadecimal con dos puntos. Como resultado, la dirección local de vínculo de este nodo de ejemplo, con el prefijo de FE80::/64 y el identificador de interfaz 02-60-08-FF-FE-52-F9-D8, es FE80::260:8FF:FE52:F9D8.

La dirección local del vínculo se puede ver mediante ipv6 if, como se muestra en el ejemplo siguiente:

Interface 4: Ethernet: Local Area Connection
uses Neighbor Discovery
link-layer address: 00-b0-d0-23-47-33
preferred link-local fe80::2b0:d0ff:fe23:4733, life infinite
multicast interface-local ff01::1, 1 refs, not reportable
multicast link-local ff02::1, 1 refs, not reportable
multicast link-local ff02::1:ff23:4733, 1 refs, last reporter, 6 seconds until report
link MTU 1500 (true link MTU 1500)
current hop limit 128
reachable time 36500ms (base 30000ms)
retransmission interval 1000ms
DAD transmits 1
Interface 3: 6to4 Tunneling Pseudo-Interface
does not use Neighbor Discovery
preferred global 2002:9d3c:89d9::9d3c:89d9, life infinite
link MTU 1280 (true link MTU 65515)
current hop limit 128
reachable time 0ms (base 0ms)
retransmission interval 0ms
DAD transmits 0

Interface 2: Automatic Tunneling Pseudo-Interface
does not use Neighbor Discovery
preferred link-local fe80::200:5efe:157.60.137.217, life infinite
preferred global ::157.60.137.217, life infinite
link MTU 1280 (true link MTU 65515)
current hop limit 128
reachable time 0ms (base 0ms)
retransmission interval 0ms
DAD transmits 0
Interface 1: Loopback Pseudo-Interface
does not use Neighbor Discovery
link-layer address:
preferred link-local ::1, life infinite
preferred link-local fe80::1, life infinite
link MTU 1500 (true link MTU 1500)
current hop limit 128
reachable time 40500ms (base 30000ms)
retransmission interval 1000ms
DAD transmits 1

La interfaz 4 es una interfaz que corresponde a un adaptador Ethernet instalado con una dirección local de vínculo de FE80::2B0:D0FF:FE23:4733.

Probar la conectividad entre dos hosts locales del vínculo

Puede realizar un simple ping (un intercambio de mensajes de solicitud de eco y respuesta de eco de ICMPv6) con IPv6 entre dos hosts locales de vínculo si lleva a cabo los pasos siguientes:

1. Utilice el comando ipv6 install en el Símbolo del sistema para instalar el protocolo IPv6 en dos equipos host que ejecuten Windows XP (host A y host B) y que estén en el mismo vínculo (subred).
2. Utilice ipv6 if en el host A para obtener la dirección local del vínculo y el Id. de la interfaz Ethernet.

   Por ejemplo, la dirección local del vínculo del host A es *FE80::210:5AFF:FEAA:20A2* y el Id. de la interfaz Ethernet es 4.

3. Utilice ipv6 if en el host B para obtener la dirección local del vínculo y el Id. de la interfaz Ethernet.

   Por ejemplo, la dirección local del vínculo del host B es *FE80::260:97FF:FE02:6EA5* y el Id. de la interfaz Ethernet es 3.

4. En el host A, utilice Ping6.exe para hacer ping al host B.

   Por ejemplo, ping6 FE80::260:97FF:FE02:6EA5%4

Al especificar una dirección de destino local de vínculo o local del sitio, debe especificar el Id. de ámbito para hacer específico el ámbito (área de la red) del tráfico.

- Por ejemplo, en un equipo con varios adaptadores Ethernet que estén conectados a vínculos independientes, se asigna una dirección local de vínculo a cada adaptador Ethernet. En esta configuración, las direcciones de destino locales de vínculo son ambiguas porque una dirección local de vínculo específica se puede asignar a varios nodos ubicados en los vínculos a los que se puede llegar desde todos los adaptadores Ethernet instalados. Al definir el área de la red a la que va dirigido el destino, el Id. de ámbito se utiliza para indicar el adaptador Ethernet a través del que se envía y recibe el tráfico. En el protocolo IPv6 de Windows XP, el Id. de ámbito es el identificador de interfaz obtenido mediante el comando ipv6 if. El identificador de interfaz se define localmente en cada host IPv6. Por este motivo, el identificador de interfaz que utiliza el host A para llegar al host B puede no ser el mismo que el identificador de interfaz que utiliza el host B para llegar al host A.
- Cuando se utilizan direcciones locales del sitio, es posible estar conectado a varios sitios. En este caso, cada sitio tiene asignado un identificador de sitio. Al definir el área de la red a la que va dirigido el destino, el Id. de ámbito se utiliza para indicar el identificador de sitio. En el protocolo IPv6 de Windows XP, el Id. de ámbito es el identificador de sitio obtenido mediante el comando ipv6 if. Si está conectado a un único sitio, el identificador de sitio predeterminado es 1 y no es necesario especificar el Id. de ámbito. El identificador de sitio se define localmente en cada host IPv6. Por este motivo, el identificador de sitio que utiliza el host A para llegar al host B puede no ser el mismo que el identificador de sitio que el host B utiliza para llegar al host A.

La notación que se utiliza para especificar el Id. de ámbito de una dirección es dirección%idDeÁmbito.

D.3.2 Práctica No 2: Tráfico IPv6 entre nodos de diferentes subredes de un conjunto de redes IPv4.

El protocolo IPv6 para Windows XP proporciona los siguientes métodos de comunicación entre nodos IPv6 de subredes diferentes de un conjunto de redes IPv4:

- Utilizar direcciones compatibles con IPv4
- Utilizar direcciones de Protocolo de direccionamiento automático de túnel dentro de un sitio
- Utilizar 6to4

  Aunque 6to4 se diseñó principalmente para permitir la comunicación entre sitios independientes habilitados para IPv6, los hosts 6to4 que utilicen el protocolo IPv6 de Windows XP pueden utilizar también direcciones 6to4 y túneles 6to4 para comunicarse en un conjunto de redes IPv4 o en Internet.

En todos los casos anteriores, aunque el tráfico IPv6 se transporta como la carga de un paquete IPv4 (la infraestructura IPv4 se considera como un nivel de vínculo IPv6), sigue siendo tráfico IPv6. Las aplicaciones que utilizan las direcciones asociadas con estos métodos utilizan las mismas funciones de Windows Sockets que si se utilizaran direcciones IPv6 globales y una infraestructura IPv6. Estos métodos se pueden utilizar para comprobar la funcionalidad IPv6 en las aplicaciones sin tener que implementar enrutadores IPv6 en una organización.

Utilizar direcciones compatibles con IPv4.

Las direcciones compatibles con IPv4 derivadas de direcciones IPv4 públicas proporcionan un método para conectar hosts o sitios IPv6 a través de la infraestructura existente de la red Internet IPv4. Cuando el tráfico IPv6 se utiliza con direcciones compatibles con IPv4, no requiere que se agreguen enrutadores IPv6. El tráfico se encapsula con un encabezado IPv4.

En la Figura D.2 se muestra la configuración de dos nodos de subredes independientes que utilizan direcciones compatibles con IPv4 para comunicarse a través de un enrutador IPv4.

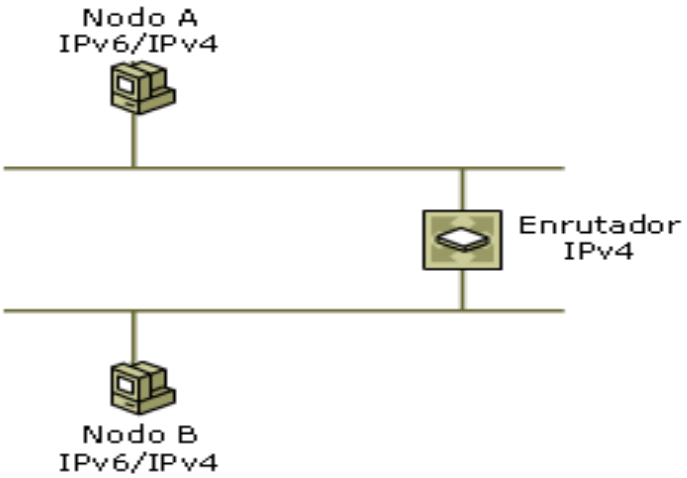

Figura D.2 Configuración de dos nodos de subredes independientes

De forma predeterminada, el protocolo IPv6 en Windows XP configura automáticamente direcciones compatibles con IPv4 para las direcciones IPv4 públicas en la Pseudointerfaz de túnel automático (Id. de interfaz 2). Una dirección compatible con IPv4 tiene el formato ::w.x.y.z, donde w.x.y.z es una dirección IPv4 pública asignada a una interfaz del equipo. El protocolo IPv6 para en Windows XP también crea automáticamente una ruta ::/96 que reenvía todo el tráfico que utiliza direcciones compatibles con IPv4 mediante la Pseudointerfaz de túnel automático (Id. de interfaz 2). Todo el tráfico que reenvía este host a los destinos compatibles con IPv4 se encapsula con un encabezado IPv4.

Cuando se envía tráfico a una dirección compatible con IPv4, el tráfico se envía desde una dirección compatible con IPv4 y se encapsula con un encabezado IPv4. El campo Protocol del encabezado IPv4 se establece en 41 para indicar que la carga es un paquete IPv6. El encabezado IPv4 permite que el tráfico viaje por una infraestructura IPv4. Las direcciones IPv4 incrustadas en las direcciones compatibles con IPv4 de origen y destino del encabezado IPv6 se convierten en las direcciones IPv4 de origen y destino del encabezado IPv4.

Por ejemplo, cuando el host A (que está configurado con la dirección IPv4 de 172.16.130.92) utiliza direcciones compatibles con IPv4 para enviar tráfico IPv6 al host B (que está configurado con la dirección IPv4 de 172.16.70.21), las direcciones de origen y destino de los encabezados IPv4 e IPv6 son las que se muestran en la tabla D.1.

La infraestructura de enrutamiento IPv4 reenvía el paquete del host A al host B, en función de la dirección IPv4 de destino de 172.16.70.21. Cuando se recibe en el host B, la carga del paquete IPv4 (el paquete IPv6) se pasa al protocolo IPv6.

Utilice el comando ping6 para probar la conexión. Por ejemplo, el host A utilizaría el siguiente comando para hacer ping al host B mediante su dirección compatible con IPv4:

ping6 ::172.16.70.21

Campo	Valor
Dirección de origen en el encabezado IPv6	::172.16.130.92
Dirección de destino en el encabezado IPv6	::172.16.70.21
Dirección de origen en el encabezado IPv4	172.16.130.92
Dirección de destino en el encabezado IPv4	172.16.70.21

Tabla D.1 Direcciones compatibles con IPv4 de origen y destino de los encabezados IPv4 e IPv6.

Utilizar direcciones de Protocolo de direccionamiento automático de túnel dentro de un sitio

Otro mecanismo de asignación de direcciones y túnel que se puede utilizar para la comunicación entre nodos IPv6 e IPv4 de una red IPv4 es el que se describe en el borrador de Internet titulado "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)" [Protocolo de direccionamiento automático de túnel dentro de un sitio (ISATAP)], que corresponde al archivo draft-ietf-ngtrans-isatap-00.txt. Estas direcciones se llaman direcciones de Protocolo de direccionamiento automático de túnel dentro de un sitio (ISATAP, Intrasite Automatic Tunnel Addressing Protocol). Tienen el formato prefijoDe64Bits:200:5EFE:w.x.y.z donde:

- La parte prefijoDe64Bits es un prefijo de 64 bits válido para direcciones IPv6 de unidifusión. Esto incluye el prefijo de direcciones locales del vínculo (FE80::/64), los prefijos locales del sitio y los prefijos globales.

- La parte 200:5EFE es el identificador único global de interfaz de 64 bits formado por la combinación del Identificador de la unidad organizativa (OUI, Organizational Unit Identifier) asignado a la Autoridad de números asignados de Internet (IANA, Internet Assigned Numbers Authority) (00-00-5E) y un tipo que indica una dirección IPv4 incrustada (FE).
- La parte w.x.y.z es una dirección IPv4 de unidifusión que incluye direcciones públicas y privadas.

Al igual que las direcciones compatibles con IPv4, las direcciones 6over4 y las direcciones 6to4, las direcciones ISATAP contienen una dirección IPv4 incrustada que se utiliza para determinar las direcciones IPv4 de origen o destino en el encabezado IPv4 cuando se envía tráfico IPv6 con direcciones ISATAP a través de una red IPv4.

De forma predeterminada, el protocolo IPv6 para en Windows XP configura automáticamente la dirección ISATAP de FE80::200:5EFE:w.x.y.z en la Pseudointerfaz de túnel automático para cada dirección IPv4 asignada al nodo. Esta dirección ISATAP local del vínculo permite que dos hosts se comuniquen a través de una red IPv4 mediante sus direcciones ISATAP respectivas.

Por ejemplo, el host A está configurado con la dirección IPv4 de 172.16.130.92 y el host B está configurado con la dirección IPv4 de 172.16.70.21. Cuando se inicia el protocolo IPv6 de Windows XP, el host A se configura automáticamente con la dirección ISATAP de FE80::5EFE:172.16.130.92 y el host B se configura automáticamente con la dirección ISATAP de FE80::5EFE:172.16.70.21. Cuando el host A envía tráfico IPv6 al host B mediante la dirección ISATAP del host B, las direcciones de origen y destino de los encabezados IPv4 e IPv6 son las que se muestran en la tabla siguiente.

Campo	Valor
Dirección de origen en el encabezado IPv6	FE80::5EFE:172.16.130.92
Dirección de destino en el encabezado IPv6	FE80::5EFE: 172.16.70.21
Dirección de origen en el encabezado IPv4	172.16.130.92
Dirección de destino en el encabezado IPv4	172.16.70.21

Tabla D.2 Direcciones ISATAP de origen y destino de los encabezados IPv4 e IPv6.

Utilice el comando ping6 para probar la conexión. Por ejemplo, el host A utilizaría el siguiente comando para hacer ping al host B mediante su dirección ISATAP local del vínculo:

ping6 FE80::5EFE:172.16.70.21%2

La parte %idDeÁmbito del comando se utiliza para especificar el índice de la interfaz desde la que se envía el tráfico. En este caso, %2 especifica la interfaz 2, que es el Id. de interfaz asignado a la Pseudointerfaz de túnel automático del host A.

El uso de direcciones ISATAP locales del vínculo permite que los hosts IPv6 e IPv4 de un conjunto de redes IPv4 se comuniquen entre sí, pero no con otros hosts IPv6 fuera del sitio. Para comunicarse fuera del sitio, es necesaria la configuración adicional siguiente:

- Un host debe recibir un anuncio del enrutador de borde del sitio que contenga un prefijo de dirección global. El enrutador de borde del sitio es el enrutador situado entre la intranet e Internet o 6bone. Un enrutador de borde del sitio suele ser un enrutador 6to4 que está conectado a Internet. Al recibir el anuncio del enrutador, se agregan de forma automática direcciones ISATAP adicionales basadas en el prefijo global.

  Por ejemplo, si el sitio está conectado a 6bone y el host A recibe el prefijo global de 3000::/64 en un anuncio de enrutador, se configura automáticamente la dirección ISATAP de 3000::200:5EFE:172.16.70.21. Sin un prefijo de dirección global y una conexión a 6bone, un sitio puede utilizar un prefijo de dirección global basado en 6to4 para conectar a otros sitios 6to4, hosts 6to4 y al 6bone, mediante la red Internet IPv4. Si el sitio utiliza el prefijo de dirección 6to4 de 2002:c81e:4720:1::/64 (basado en la dirección pública de 200.30.71.32 y un Id. de SLA de 1), se configura automáticamente la dirección ISATAP de:

  2002:c81e:4720:1:200:5EFE:172.16.70.21

  Sin embargo, actualmente no existe ningún mecanismo para la propagación del anuncio de enrutador desde el enrutador de borde del sitio a los hosts ISATAP en una red IPv4.

  El protocolo IPv6 para Windows XP se debe configurar manualmente para la dirección ISATAP global en la Pseudointerfaz de túnel automático (Id. de interfaz 2) mediante el comando ipv6 adu. Si se utiliza el prefijo 6to4 del ejemplo anterior, el comando para el host A será el comando ipv6 adu 2/2002: c81e:4720:1:200: 5EFE:172.16.70.21. El prefijo global de 64 bits, que utiliza la Pseudointerfaz de túnel automático (Id. de interfaz 2), se debe agregar manualmente a la tabla de enrutamiento IPv6 mediante el comando ipv6 rtu. Si se utiliza el prefijo 6to4 del ejemplo anterior, el comando para el host A será ipv6 rtu 2002:c81e:4720:1::/64 2.

  Un host debe tener una ruta predeterminada que apunte a una dirección ISATAP correspondiente a la interfaz de intranet del enrutador de borde del sitio.

  Por ejemplo, si la interfaz de intranet del enrutador de borde del sitio está configurada con la dirección IPv4 de 172.16.130.92, el host A se debe configurar con una ruta predeterminada (::/0) que utilice la dirección ISATAP de FE80::200:5EFE:172.16.130.92 como dirección para el salto siguiente. En consecuencia, todo el tráfico IPv6 que tenga esta ruta predeterminada como la ruta con mejor correspondencia se encapsula y reenvía al enrutador de borde del sitio. Después, el enrutador de borde del sitio reenvía el tráfico. Si el enrutador de borde del sitio es un enrutador 6to4, encapsulará el tráfico IPv6 y lo reenviará a Internet.

El protocolo IPv6 para Windows XP se debe configurar manualmente mediante el comando ipv6 rtu para una ruta predeterminada (::/0), que utiliza la Pseudointerfaz de túnel automático (Id. de interfaz 2) y tiene una dirección de salto siguiente establecida como una dirección ISATAP correspondiente a la interfaz de intranet del enrutador de borde del sitio. En el ejemplo anterior, el comando para el host A será ipv6 rtu ::/0 2/FE80::200:5EFE:172.16.130.92.

D.3.3 Práctica No 3: Tráfico IPv6 entre nodos de sitios diferentes en Internet (6to4)

6to4 es una técnica de túnel que se describe en el documento RFC 3056. Cuando se utiliza 6to4, el tráfico IPv6 se encapsula con un encabezado IPv4 antes de enviarse a través de un conjunto de redes IPv4, como Internet.

6to4 utiliza el prefijo de dirección global de 2002:WWXX:YYZZ::/48, donde WWXX:YYZZ es a la vez la parte Agregador de siguiente nivel (NLA, Next Level Aggregator) de una dirección global y la representación hexadecimal con dos puntos de una dirección IPv4 pública (w.x.y.z) que está asignada al sitio o host. La dirección 6to4 completa de un host 6to4 es 2002:WWXX:YYZZ:[Id. de SLA]:[Id. de interfaz].

En el documento RFC 3056 se definen los términos siguientes:

- Host 6to4

  Host IPv6 que está configurado con al menos una dirección 6to4.

- Enrutador 6to4

  Enrutador IPv4 o IPv6 que reenvía el tráfico con direcciones 6to4 entre los hosts 6to4 de un sitio y otros enrutadores 6to4 o enrutadores de retransmisión 6to4 en un conjunto de redes IPv4, como Internet.

- Enrutador de retransmisión 6to4

  Enrutador IPv4 o IPv6 que reenvía tráfico con direcciones 6to4 entre enrutadores 6to4 en Internet y hosts en 6bone.

Cuando se utilizan hosts 6to4, una infraestructura de enrutamiento IPv6 en sitios 6to4, un enrutador 6to4 en los límites del sitio y un enrutador de retransmisión 6to4, son posibles los tipos de comunicación siguientes:

1. Un host 6to4 se puede comunicar con otro host 6to4 en el mismo sitio.

   Este tipo de comunicación está disponible mediante la infraestructura de enrutamiento IPv6, que proporciona accesibilidad a todos los hosts del sitio.

2. Un host 6to4 se puede comunicar con hosts 6to4 de otros sitios de la red Internet IPv4.

Este tipo de comunicación se produce cuando un host 6to4 reenvía al enrutador 6to4 del sitio local el tráfico IPv6 que está destinado a un host 6to4 de otro sitio. El enrutador 6to4 del sitio local encapsula el tráfico IPv6 con un encabezado IPv4 y lo envía al enrutador 6to4 del sitio de destino en Internet. El enrutador 6to4 del sitio de destino quita el encabezado IPv4 y reenvía el paquete IPv6 al host 6to4 correcto mediante la infraestructura de enrutamiento IPv6 del sitio de destino.

3. Un host 6to4 se puede comunicar con hosts de 6bone.

   Este tipo de comunicación se produce cuando un host 6to4 reenvía al enrutador 6to4 del sitio local el tráfico IPv6 que está destinado a un host de 6bone. El enrutador 6to4 del sitio local encapsula el tráfico IPv6 con un encabezado IPv4 y lo envía a un enrutador de retransmisión 6to4 que está conectado a la red Internet IPv4 y a 6bone. El enrutador de retransmisión 6to4 quita el encabezado IPv4 y reenvía el paquete IPv6 al host de 6bone correcto mediante la infraestructura de enrutamiento IPv6 de 6bone.

Todos estos tipos de comunicación utilizan tráfico IPv6 sin el requisito de obtener una conexión directa a 6bone o un prefijo de dirección global IPv6 de un proveedor de servicios Internet (ISP).

El servicio 6to4 que se incluye con el protocolo IPv6 en Windows XP proporciona compatibilidad con hosts y enrutadores 6to4. El servicio 6to4 lleva a cabo las acciones siguientes:

- Configura automáticamente direcciones 6to4 en la interfaz que tiene el nombre Pseudointerfaz de túnel 6to4 (Id. de interfaz 3) para todas las direcciones IPv4 públicas que están asignadas a las interfaces del equipo.
- Crea automáticamente una ruta 2002::/16 que reenvía todo el tráfico 6to4 con la Pseudointerfaz de túnel 6to4 (Id. de interfaz 3). Todo el tráfico que reenvía este host a los destinos 6to4 se encapsula con un encabezado IPv4.
- Realiza automáticamente una consulta de Sistema de nombres de dominio (DNS, Domain Name System) del nombre 6to4.ipv6.microsoft.com para obtener la dirección IPv4 del enrutador de retransmisión 6to4 de MIcrosoft en Internet.

Al utilizar la configuración automática del servicio 6to4, un host que ejecute el protocolo IPv6 en Windows XP y esté configurado con una dirección IPv4 pública se configurará automáticamente como host 6to4. Un host 6to4 puede crear su propio túnel para alcanzar hosts 6to4 de otros sitios o hosts de 6bone.

Si Conexión compartida a Internet (ICS, Internet Connection Sharing) está habilitado en una interfaz que tiene asignada una dirección IPv4 pública, el servicio 6to4 lleva a cabo las acciones siguientes:

- Habilita el enrutamiento en la interfaz privada.
- Envía anuncios de enrutador que contienen prefijos de direcciones 6to4 basados en la dirección IPv4 pública de la interfaz pública. El Id. de SLA del prefijo de la

dirección 6to4 se establece como el Id. de la interfaz en la que se envían los anuncios.

En Windows XP, al habilitar ICS se puede utilizar un equipo que ejecute el protocolo IPv6 como enrutador 6to4, que es capaz de encapsular y reenviar el tráfico 6to4 a otros hosts o sitios 6to4 de Internet, y reenviar el tráfico de 6bone a un enrutador de retransmisión 6to4 de Internet.

En la Figura D.3 se muestra cómo se utiliza 6to4 para la comunicación entre dos sitios 6to4.

Cada sitio utiliza un equipo que ejecuta Windows XP con ICS habilitado en la interfaz pública para crear un enrutador 6to4. Los equipos host que ejecutan Windows XP en los segmentos de la red privada reciben el anuncio de enrutador que envía el enrutador 6to4 de su sitio y que contiene un prefijo de dirección 6to4. El resultado es que dos hosts 6to4 se pueden comunicar mediante direcciones 6to4 a través de Internet.

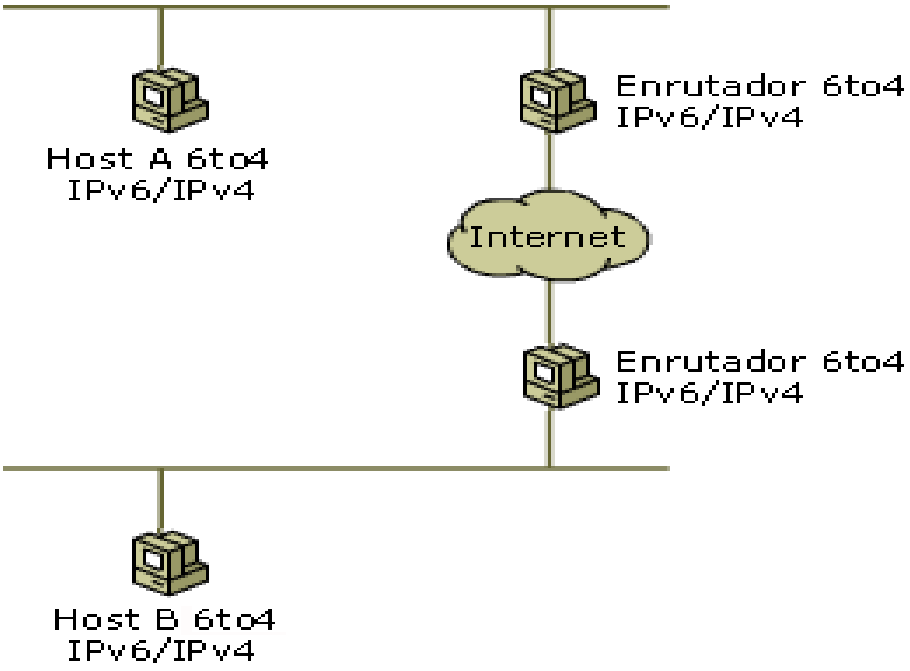

Figura D.3 Comunicación entre dos sitios 6to4.

D.3.4 Práctica No 4: Conectarse con el 6bone.

La manera más sencilla de conectarse al 6bone es utilizar el servicio 6to4 que se incluye con el protocolo IPv6 en Windows XP. Puede utilizar el servicio 6to4 como host 6to4 o como enrutador 6to4 si habilita Conexión compartida a Internet (ICS, Internet Connection Sharing) en un equipo que esté conectado a Internet. El servicio 6to4 se configura automáticamente con las direcciones 6to4 adecuadas y utiliza un enrutador de

retransmisión 6to4 específico en Internet. Para obtener más información. En la Figura D.4 se muestra la configuración de un host que utiliza 6to4 para comunicarse al 6bone mediante un enrutador de retransmisión 6to4.

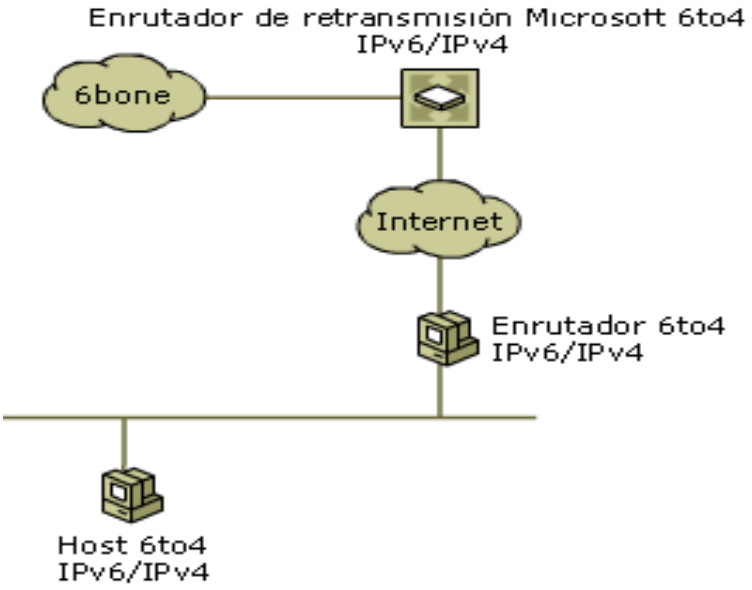

Figura D.4 Configuración de un host que utiliza 6to4 para comunicarse al 6bone mediante un enrutador de retransmisión 6to4.

Con 6to4, se puede hacer ping a otros equipos de 6bone (por ejemplo, ping6 ipv6.research.microsoft.com). En el sitio Web de IPv6 se proporciona una lista de servidores que tienen acceso a IPv6 para comunicarse en 6bone. Además, el registro de 6bone contiene los nombres de otros equipos de 6bone.
Es posible que no se pueda tener acceso a algunos sitios de 6bone. También es posible que surjan problemas de conectividad. En ambos casos, el comando tracert6 -d dirección puede resultar útil. El parámetro -d impide la búsqueda DNS inversa en direcciones de enrutadores intermedios.

D.4 Desarrollo de prácticas utilizando TSP y Apache.

A continuación se describirán dos prácticas más, implementadas con el fin de probar una forma diferente a las configuraciones típicas que trae Windows XP para establecer un túnel de IPv6 sobre IPv4 y probar además aplicaciones habilitadas para IPv6. Una de las prácticas utiliza TSP (protocolo de establecimiento de túnel) y la otra consiste de un servidor Web Apache que corre sobre IPv6 y sobre IPv4.

D.4.1 Conexión al 6Bone utilizando el Protocolo de establecimiento de túnel (TSP, Tunnel Setup Protocol).

Freenet6's TSP es una nueva iniciativa lanzada por Viagénie, una compañía privada en Canadá involucrada en IPv6 desde 1996, para facilitar un despliegue más rápido de

Internet Ipv6. Internet se despliega sobre Ipv4 a nivel mundial, por consiguiente este proyecto tiene como meta principal desplegar Ipv6 a una escala más grande usando túneles configurados.

El túnel configurado es un método de transición regularizado por la IETF para usar Ipv6 en coexistencia con Ipv4 encapsulando paquetes Ipv6 sobre Ipv4. Cualquier host ya conectado a Internet con IPv4 y teniendo el stack IPv6 poda establecer un enlace a Internet IPv6.
Freenet6, desarrollado por Viagénie en 1999-2000, fue el primer servicio de servidor de túnel público y uno de los mas usados en el mundo para delegar automáticamente una sola dirección Ipv6 a cualquier host simplemente conectado a una red Ipv4 sobre un túnel configurado llenando un registro Web ejecutando un script. el TSP de Freenet6 representa otro paso importante para acelerar el despliegue a gran escala de Ipv6 en la red.

En lugar de una interfaz Web para pedir túneles configurados y direcciones Ipv6, el TSP de Freenet6 es nuevo modelo basado en un acercamiento cliente/servidor. Un protocolo se usa para pedir una sola dirección Ipv6 de un prefijo Ipv6 desde un cliente a un servidor de túnel según el modelo Ipv6 broker. El protocolo podría integrarse directamente en el sistema operativo para dar un servicio como DHCP pero para pedir direcciones Ipv6 o prefijos sobre una red Ipv4 (Internet).

Como trabaja TSP.

Procedimiento general para la Implementación del protocolo TSP de Freenet6

Las peticiones son iniciadas por hosts o servidores con la pila IPv6 conectados a Internet. El cliente TSP (tspc) lee un archivo de configuración (tspc.conf), entonces envía una petición (usando TCP) al servidor de TSP especificado en el archivo de configuración. El servidor de TSP procesa la petición y (según su política local), asigna una sola dirección IPv6 o un prefijo IPv6 completo al solicitante. Luego, el servidor de TSP establece un nuevo túnel configurado (IPv6 sobre IPv4) según la información enviada en la petición.

Cuando el cliente recibe la información de túnel, configura localmente su interfaz del túnel y predefine una ruta IPv6. El cliente tiene conectividad IPv6 completa ahora.

Cómo configurar localmente el túnel del cliente.

Se guarda la información recibida en variables de ambiente y un script de línea de comandos (shell script, archivo por lotes para Windows) se ejecuta. El shell script ejecutará los comandos necesarios para establecer el túnel. Este shell script se llama una plantilla.

El cliente ejecutará la plantilla especificada en el archivo de configuración. Los usuarios pueden personalizar las plantillas según sus preferencias locales.

Direcciones IPv6 asignadas por el servidor de TSP

Con el servicio Freenet6 servicio ha habido abusos de usuarios (spamming, intrusiones y otros tipos de abusos). Con este viejo sistema, era imposible para los administradores rastrear a los usuarios maliciosos sobre IPv4 excepto localizando a los administradores del servidor de túnel.

El equipo de trabajo de Freenet6 era consciente de este problema y propuso una solución limpia para este problema. las direcciones IPv6 de Freenet6 para el cliente anónimo tendrán la dirección IPv4 dirección del cliente embebida en él. de esta manera, el administrador podrá avisar al proveedor real del ofensor o filtrar el prefijo IPv4 del ISP del infractor.

Requerimientos del servidor TSP

Para poder usar Freenet6, hay requisitos básicos que los host y redes deben cumplir para conseguir conectividad IPv6. Este documento da una apreciación global de los requisitos necesitados.

- Léxico:

IPv4: IP versión 4, la versión actual de usó en Internet
IPv6: IP versión 6, la próxima generación en el protocolo IP
Túnel configurado: Mecanismo para llevar paquetes IPv6 sobre paquetes IPv4
Servidor del túnel: Sistema que despliega conectividad IPv6 usando un túnel configurado sobre redes IPv4
Freenet6: una implementación de servidor de túnel
Requisitos del host para usar Freenet6

- Pila IPv6:

Cada host debe tener una pila IPv6 que corre bajo el sistema operativo. IPv6 es soportado por diferentes sistemas operativos, IPv6 esta disponible para la mayoría de las plataformas.

- Dirección IPv4:

Para recibir conectividad IPv6 desde un servidor de túnel a través de Internet (IPv4), los host deben tener una direccion unicast global de Internet lo que significa que direccinamiento privado (10.x.x.x, 172.16.x.x, 192.168.x.x) no es aceptado por el servidor del túnel. El direccionamiento privado se usa a menudo detrás de una compuerta NAT, servidores proxy, firewall y enrutadores porque no hay suficientes direcciones IPv4en el mundo para cada computadora.

- Privilegios de Root/administrador:

Para instalar la pila IPv6 y poder configurar correctamente la conectividad IPv6 al servidor del túnel, los usuarios deben tener privilegios de root o de administrador en sus computadoras.

Requisitos de la red para usar Freenet6.

Túnel configurado.
Mecanismo del túnel configurado (IPv6 sobre IPv4), la forma en que Freenet6 entrega paquetes IPv6 a las computadoras remotas sobre una red IPv4 (Internet) es un protocolo estandarizado por la IETF. El número del protocolo es 41. La información técnica está disponible en el RFC 2893 sobre el túnel configurado.

Protocolo de establecimiento de túnel (TSP).
El Protocolo de establecimiento de túnel es un protocolo diseñado por Viagénie para automatizar el despliegue a gran escala de IPv6 sobre IPv4 con el mecanismo de túneles configurados en lugar de usar configuración manual o scripts Web/CGI para establecer los túneles. TSP usa TCP con el puerto número 4343. Éste no es un puerto definido por IANA.

Requisitos de seguridad.

- Firewall.

Para poder recibir conectividad IPv6 de Freenet6, el firewall que protege la red debe tener reglas especiales para permitir el protocolo número 41 y el puerto TCP 4343 entre Freenet6 y la red del usuario final. Observe en el archivo de configuración (tspc.conf) para saber la dirección del servidor del túnel.

- Enrutador

El enrutador que usa lista de acceso para proteger la red debe tener reglas especiales para permitir el protocolo número 41 y el puerto TCP 4343 entre Freenet6 y la red del usuario final. Observe en el archivo de configuración (tspc.conf) para saber la dirección del servidor del túnel.

Traducción de Dirección de red (NAT)
Si un usuario final está detrás de una compuerta NAT (Network Address Translation), no es posible recibir tráfico IPv6 sobre IPv4 desde cualquier servidor de túnel excepto en estas dos situaciones:

1. la compuerta NAT maneja direccionamiento NAT estático y el administrador de la red podría trazar una única IP unicast global de Internet al host del usuario final detrás del NAT. Esto significa que el administrador de la red local controla y autoriza esta configuración especial para los usuarios finales.

2. la compuerta NAT corre bajo cualquier plataforma BSD y el usuario final maneja la entrada. Es posible establecer reglas IPfilter para remitir IPv6 sobre paquetes IPv4 a un host específico detrás del NAT.

Descargar e instalar el cliente TSP.

La última versión es Freenet6-0.9.7. Se puede obtener de la siguiente dirección:

http://www.freenet6.net/download.shtml.

Instrucciones para instalar la distribución binaria Windows NT/2000/XP.

Descomprima el paquete en un directorio, abra un interprete de comandos, cd a ese directorio y ejecuta el cliente (el último paso requiere privilegios de administrador).

- C:\> cd \to\the\target\directory
- C:\to\the\target\directory> unzip freenet6-bin-0.xx.zip
- C:\to\the\target\directory> cd freenet6
- C:\to\the\target\directory\freenet6> tspc -vf tspc.conf

Petición de direcciones y prefijos.

Como pedir un prefijo IPv6 /48.

Un prefijo IPv6 /48 permite a un sitio desplegar 65 535 subredes (prefijo IPv6 /64). Cada subred podría manejar 2^64 nodos (18 446 744 073 709 551 616 IPv6 direcciones), por consiguiente, el número de direcciones IPv6 unicast que se podría usar con sólo un prefijo /48 es increíble: ¡65 535 subredes * 18 446 744 073 709 551 616!!!

¿Que es un sitio? ¡Hay muchas discusiones en la IETF sobre lo que debe ser un sitio pero en la aplicación actual se considera que un sitio puede estar en un rango que va desde una red muy grande con mil nodos a una red local con sólo 2 nodos.

Como descargar e instalar el cliente tspc.

1. descargue e instale el cliente tsp.

Seleccione una distribución del sistema operativo Instálelo en su computadora (vea los requisitos primero).

2. cree una cuenta.

Se va al formulario Web de la pagina www.freenet6.net y se crea una cuenta se digita un userid (e.g ipv6unicauca) se digita la dirección de e-mail (Ej. ip6ucauca@ucauca.edu.co), Freenet6 generara una contraseña al azar, que se enviará a su dirección de e-mail.

3. agregue userid y contraseña.

Agregue el userid a tspc.conf (e.g userid=ipv6unicauca)
Agregue su contraseña a tspc.conf (e.g passwd=F83% ?fs21)

4. agregue paramatetros especiales para pedir un prefijo /48.

Agregue host_type=router en tspc.conf
Agregue prefixlen=48 en tspc.conf
Agregue if_prefix= LA_INTERFAZ_DE_RED_A_USAR en tspc.conf

El campo YOUR_NETWORK_INTERFACE se acostumbra configurar la computadora apropiadamente para actuar como enrutador IPv6. El reenvió IPv6 se habilitarán entre esta interfaz y el túnel configurado (IPv6 sobre IPv4). Se activarán anuncios de enrutador IPv6 en esta interfaz para permitir a host que estén conectados con este equipo autoconfigurar sus direcciones IPv6. Sin embargo, el nombre de la interfaz de red no es la misma para cada sistema operativo. En la tabla D.3 se pueden observar diferentes sistemas operativos con sus correspondientes interfaces de red.

Plataforma	Posible nombre de la INTERFAZ_DE_RED
Unix	eth0,eth1,fxp0,ep0,ed0,le0,lnc0,...
Windows 2000/NT/XP	3,4,5,...Lea información al respecto en la pagina de Microsoft
Cisco	tunnelxx, ethernet0/1, fast-ethernet0/1

Tabla D.3 Interfaz de red para diferentes sistemas operativos.

Hay algunas políticas sobre el servidor TSP. Estas políticas son útiles para controlar que y cómo los usuarios tienen acceso al servidor TSP a través del protocolo TSP. Las políticas son relacionadas con la dirección fuente IPv4 que solicita un túnel, longitud del prefijo, formato de la dirección IPv6 asignada, delegación y autenticación del prefijo.

Direcciones fuente IPv4 no aceptadas para establecer un túnel.

La dirección fuente no debe ser:

- Direcciones de lazo cerrado (127.0.0.0 - 127.255.255.255)
- Rangos de direcciones privadas (10.0.0.0/8 o 172.16.0.0/12 o 192.168.0.0/16)
- Multicast o direcciones clase D anteriores (224.0.0.0 - 239.255.255.255)
- Direcciones clase E (240.0.0.0 - 254.255.255.255)
- Direcciones Broadcast (255.255.255.255)

Longitud del prefijo del túnel configurado.

La longitud del prefijo de cada túnel configurado es de 64 bits (/64). Esto es válido para los túneles anónimos y los túneles autenticados que proveen una dirección IPv6 a cualquier nodo. La Tabla D.4 muestra la longitud del prefijo de cada túnel configurado.

Túnel #	IPv6 prefijo asignado para el túnel (64 bits)	Hosts (64 bits)
00001	3FFE:0B80:0002:0001	xxxx:xxxx:xxxx:xxxx
00002	3FFE:0B80:0002:0002	xxxx:xxxx:xxxx:xxxx
...	...	xxxx:xxxx:xxxx:xxxx
65534	3FFE:0B80:0002:FFFF	xxxx:xxxx:xxxx:xx

Tabla D.4 Longitud del prefijo de cada túnel configurado

Longitud del prefijo IPv6 asignado.
La Tabla D.5 muestra la longitud del prefijo de cada prefijo IPv6 asignado de 48 bits (/48).

/48 prefijo #	Espacio IPv6 (48 bits)	Subredes (16 bits)	Hosts (64 bits)
00001	3FFE:0B80:0003::	xxxx	xxxx:xxxx:xxxx:xxxx
00002	3FFE:0B80:0004::	xxxx	xxxx:xxxx:xxxx:xxxx
...	..... ::	xxxx	xxxx:xxxx:xxxx:xxxx
65532	3FFE:0B80:FFFF::	xxxx	xxxx:xxxx:xxxx:xxxx

Tabla D.5 Longitud del prefijo de cada prefijo IPv6 asignado.

Formato de la dirección IPv6.
Todos los túneles anónimos asignados tienen un formato especial como el que se puede observar en la Figura D.6. Este formato se propuso para rastrear a los usuarios maliciosos en la capa IPv4. La dirección fuente IPv4 de los usuarios finales de Freenet6 esta incluida dentro de las direcciones IPv6 asignadas por el servidor TSP en este formato:

Los bits 96 a 128 de la parte del host son usados para realizar esta función.

| <-------red------------------> | <------------host-----------> |
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:AABB:CCDD

Figura D.6 Formato de dirección IPv6.

Ejemplo: Si la dirección fuente IPv4 del usuario es 24.200.194.27

La asignación IPv6 final puede parecerse a la direccion que se muestra en la Figura D.7:

| <--------red------------> | <----------host----------->|
|<- IPv4 ->|
3FFE:0B80:0002:0001:0000:0000:18C8:C21B

AA => 24 => 0x18
BB => 200 => 0xC8
CC => 194 => 0xC2
DD => 27 => 0x1B

Figura D.7 Ejemplo de una dirección IPv6 y la forma de conversión de la direccion IPv6 a hexadecimal

Autenticación.
Actualmente, se llevan a cabo túneles anónimos, túnel autenticado y asignación de prefijo. En el modo autenticado, el protocolo TSP usa SASL-DIGEST-MD5 para llevar información confidencial (userid/password) de los usuarios finales a Freenet6.
Los usuarios autenticados tendrán una dirección IPv6 estática asignada a ellos (dirección IPv6 permanente). Ellos podrán actualizar su túnel cada vez que su IPv4 cambie ejecutando el cliente TSP.

Vida del túnel configurado.
Los túneles anónimos expirarán 5 días después de la última conexión del cliente TSP (ellos se anulan automáticamente).

Los túneles autenticados expirarán 3 meses después de la última conexión del cliente TSP (ellos se anulan automáticamente).

Registro DNS.

Túnel anónimo
Cada túnel consigue un registro AAAA y PTR en el servidor DNS de Freenet6. El FQDN asociado a este registro usa este formato (túnel anónimo): anonymous-IPv4_address-server_name.freenet6.net donde IPv4_address es la direccion IPv4 del host, y el server_name es el servidor TSP que proporciona conectividad (tsps1). El Ejemplo con 192.168.100.1 da: anonymous-192-168-100-1.tsps1.freenet6.net.

Túnel autenticado.
El FQDN asociado para el túnel autenticado usa este formato:

userid.server_name.freenet6.net donde el userid es la cuenta del usuario final, y el server_name es el servidor TSP que proporciona conectividad (tsps1). el Ejemplo con incredibleipv6 da: incredibleipv6.tsps1.freenet6.net

Como crear una cuenta.
Las cuentas son obligatorias en Freenet6 en dos casos:

1. Túnel autenticado.

- Proporciona una sola y permanente direccion IPv6 a un nodo.
- Los usuarios siempre pueden guardar la misma direccion IPv6 dirección aunque sus direcciones IPv4 cambien.
- Cualquier cambio de la dirección IPv4 será manejado por el protocolo TSP con una cuenta válida.

2. Asignacion del prefijo IPv6 /48.

- Freenet6 tienen la capacidad para delegar un prefijo /48 a cualquier usuario final para direccionamiento del sitio.
- Se delegan prefijos del espacio de direccion del pTLA de Viagénie (3ffe:0b80::/32).
- Un usuario final debe tener por lo menos una computadora que actúe como un enrutador IPv4/IPv6 para su sitio.
- Cualquier cambio a la direccion IPv4 (enrutador fronterizo) es manejado por el protocolo TSP con una cuenta válida.

Política de Userid/Password.

- Userid: El usuario final tendrá que seleccionar un userid. Los userid se usarán para el DNS el registro AAAA
- Los carácteres aceptados para el userid son: cualquier carácter alfanumérico y [-]
- Tamaño del userid: mínimo 8 carácteres y máximo 63
- Contraseña: Freenet6 generará una contraseña al azar para cada userid pedido y lo enviarán a la dirección de e-mail especificada

userid	
e-mail	

Figura D.8 Formulario para obtener un prefijo /48 de freenet6.

Manual de gestión del sistema TSPC.

NOMBRE
tspc - protocolo de establecimiento de túnel - cliente

SINOPSIS
tspc [-h] [-?]
tspc [-v] [-f config_file] [-i tunnel_interface] [-s source_interface] [-r retry_delay]

DESCRIPCIÓN
El tspc proporciona algunos términos para configurar un túnel obtenido de un servidor de túnel, estos términos son adaptables al protocolo de establecimiento de túnel (TSP). El tspc se conecta a un servidor de túnel y pide un túnel según las especificaciones dentro el archivo de configuración.

Si se ejecuta sin el parámetro se usarán valores predefinidos por cada opcion.

Las opciones siguientes están disponibles:

- -h -? Despliega un corto resumen del uso y desconexión.

- -v Verbose flag.

El funcionamiento predefinido de tspc no produce salidas estándar. El nivel verboso es establecido según el número de v's en la línea de comando. asi -v es el verboso normal y -vv es verboso extra.

- -s source_interface.

Al pedir un túnel la primera dirección IPv4 de esta interfaz se usará como la fuente del extremo final del túnel. Esto anulara el valor para la fuente IP proporcionada por la opción cliente_v4 en el archivo de configuración.

- -i tunnel_interface.

Esta opción anula la opción if_tunnel del archivo de configuración.

- -f Configuration_file.

Especifica un archivo de configuración diferente a ser usado en lugar del archivo predefinido tspc.conf.

- -r Retry_delay.

Especifica reintentar después del segundo retry_delay en caso del fracaso. El valor por defecto es 0: ningún reintento.

Manual de la estructura del archivo "TSPC.CONF".

NOMBRE.
tspc - archivo de configuración tspc.

SINOPSIS.
tspc.conf.

DESCRIPCIÓN.
Los tspc es un programa cliente que le permite a un host solicitar a un servidor de túnel establecer un túnel entre el host y el servidor. El archivo de configuración tspc contiene información que es leída por el tspc para especificar la información del servidor y el túnel a ser establecido.

Este archivo se diseño para ser fácilmente legible y puede ser editado por cualquier editor de texto. El archivo consiste en entradas y valores, las cuales están separadas por el signo igual. Cada par de entrada-valor debe estar en su propia línea. Los valores pueden abarcar más de una línea con la ayuda del identificador de bloque de salida. El procesador del archivo de configuración agregará todas las líneas siguientes a la entrada hasta que encuentre un solo punto "." en la primera columna de una línea. Aquí esta un ejemplo del uso del identificador de bloque de salida:

- multiline = <<
- Ésta es la primera línea, y no incluirá ' << ' en la línea anterior
- Ésta es la segunda línea
- aa=bb
- La línea anterior también será incluida
- Ésta es la última línea.
- **.** Éste es el punto de terminar y no será incluido

En este ejemplo, las entradas multilínea contendrán todas las líneas (incluyendo el retorno de carro y la línea de entrada) que esta entre" <<" y".". Se ignoran líneas de espacio en blanco y las líneas que empiezan con la señal de la libra son consideradas como comentarios.

En este manual los corchetes cuadrados son usados para mostrar argumentos opcionales y la línea vertical para mostrar argumentos de un grupo solamente.

Las diferentes opciones de la configuración son:

- tsp_version.

La versión actual de tspc. La instalación actual es la versión 1.0.0. Esta variable podría parecerse algo a esto:

tsp_version=1.0.0

Esta variable es OBLIGATORIA.

- tsp_dir.

El directorio actual donde el programa tspc y las plantillas están localizadas. Esta variable podría parecerse algo a esto:

tsp_dir=c:\freenet6-1.0.0

Esta variable es OBLIGATORIA.

- client_v4.

Dirección IPv4 del punto final del túnel del cliente. Si el host tiene más de una dirección IPv4, se recomienda establecer manualmente esta variable con la dirección IPv4 local como valor. Si se establece en auto, se usará la IP de la fuente usada cuando se estableció la comunicación con el servidor. Esta variable podría parecer algo como esto:

client_v4=[nnn]. [nnn]. [nnn]. [nnn]

client_v4=auto

Mire las políticas del servidor para una lista de direcciones permitidas.

Esta variable es OBLIGATORIA.

- server.

Nombre y número del puerto del servidor del túnel. Esta variable es usada para especificar el servidor TSP a ser requerido. Una dirección IPv4 dirección o FQDN (Fully Qualify Domain Name) puede ser usado. El número del puerto es opcional. Por defecto, el tspc usa 4343 como valor de puerto. Se recomienda que nunca se especifique el numero de puerto cuando no se este registrado todavía con el IANA. La sintaxis es:

server=host[:port]
server=tsps1.freenet6.net
server=tsps1.freenet6.net:4343
server=192.168.1.1
server=192.168.1.1:4343

Esta variable es OBLIGATORIA

- retry_delay.

La opción de retry_delay se usa para poner el número de segundos para dormir antes de intentar de nuevo una peticion de túnel al servidor tsp después del fracaso de la petición, se intentara hasta tener éxito. Se Pone a 0 si no se desea reintentar. La sintaxis es:

retry_delay=30

Esta variable es OPCIONAL

- Userid.

El userid es usado para la autenticación en el servidor. Por defecto el tspc usa anónimo como el userid. El protocolo TSP permite establecer ambos tipos de túneles anónimo y autenticado. La sintaxis es:

userid=anonymous|user_name

Esta variable es OBLIGATORIA.

- Passwd.

La contraseña es acostumbrada para la autenticación en el servidor. Por defecto el tspc anónimo como el userid y entonces no se requiere ninguna contraseña. Sin embargo, cuando se ingresa un userid válido esta entrada debe usarse para ser autenticado por el servidor. La sintaxis es:

passwd=aslkjd821

Esta variable es OPCIONAL

- if_tunnel.

Nombre de la interfaz Lógica que se usará para establecer el tunel configurado (IPv6 sobre IPv4). La sintaxis es:

if_tunnel=interface-nombre

Bajo FreeBSD,NetBSD,OpenBSD
if_tunnel=gif0

Bajo cualquier plataforma de Linux incluso la pila de USAGI
if_tunnel=sit1

Bajo Solaris
if_tunnel=ip.tun0

Bajo Cisco
if_tunnel=Tunnel0

Bajo Windows
if_tunnel=3,4,5...

Esta variable es OBLIGATORIA.

- Template.

Este parámetro se usa para decir qué plantilla de configuración debe usarse para configurar el túnel. La plantilla de configuración es un script, localizado en el directorio de la plantilla del paquete, que contiene el sistema de comandos para ser ejecutados para el establecimiento del túnel. Los parámetros se pasan al script como variables de ambiente. Normalmente los parametros de la plantilla se establecen cuando el paquete se construye para un sistema operativo específico. Observe en el directorio de la plantilla para ver cuáles están disponibles. El nombre de la plantilla debe ser el nombre de archivo sin el sufijo .sh o .bat.

template=name_of_the_template_used

Por ejemplo, para usar la plantilla checktunnel.sh que sólo despliega los valores pasados a la plantilla, usted debe especificar:

template=checktunnel

Plantillas disponibles para BSD, Linux, Solaris, Microsoft y Cisco son:

FreeBSD: freebsd4, freebsd44,
OpenBSD: openbsd

NetBSD: netbsd
Linux: linux
Solaris: solaris8
Microsoft: windowsNT-2k
Cisco: cisco.bat, cisco.sh,

Esta variable es OBLIGATORIA.

Esta sección describe parámetros para usar en orden para pedir prefijos IPv6 /48 o /64 al servidor. Antes de pedir un prefijo IPv6, es obligatorio tener userid válido y contraseña en el servidor.

- host_type.

Este parámetro se usa para pedir que la computadora al final del túnel (computadora cliente) actúe como un enrutador IPv6. El parámetro informa a la plantilla para habilitar los anuncios de enrutador IPv6 (ipv6_forwarding) en la computadora. El valor para habilitar este modo es "enrutador". La sintaxis es:

host_type=router

Este parámetro es OPCIONAL.

- Prefixlen.

Este parámetro se usa para especificar la longitud del prefijo pedido. Los prefijos disponible en Freenet6 solo son /48 y /64. Los /48 son recomendados para sitios grandes con multiples subredes mientras los /64 son para redes con sólo una subred. La sintaxis es:

prefixlen=48
prefixlen=64

Este parámetro es OPCIONAL.

- if_prefix.

Este parámetro se usa para habilitar los anuncios de enrutador automáticamente en una interfaz de red de la computadora. Con esta opción, el prefijo /64 conseguido será anunciado en una interfaz de red, entonces todos los nodos IPv6 conectados en la misma subred serán capaces de autoconfigurar su dirección IPv6 por si mismos. El valor a especificar es el nombre de la interfaz donde el prefijo puede anunciarse. El nombre de la interfaz puede variar y puede depender del sistema operativo en usó. La sintaxis es:

if_prefix=eth0

Ejemplos de nombres de interfaz existentes organizados por grupo de tecnología:

Unix: eth0,eth1,fxp0,ep0,ed0,le0,lnc0,..
Microsoft: 3,4,5,.. (Lea documentación de Microsoft)
Cisco: ethernet0/0, ethernet0/1, fastethernet0/1, fastethernet2/0,...

Este parámetro es OPCIONAL.

- dns_server.

Este parámetro se usa para especificar los servidores DNS que deben usarse para la asignacion del DNS inverso del prefijo asignado. Sólo el FQDN de un servidor DNS se acepta. La sintaxis es:

- dns_server=fqdn[:fqdn]...

Por ejemplo, para usar ns1.nowhere.net y ns1.nowhere.net como servidores dominantes de NS para DNS inverso del prefijo, esta línea se usaría en tspc.conf:

dns_server=ns1.nowhere.net:ns2.nowhere.net

Nunca use una dirección IP como un nombre de servidor DNS.

Esta variable es OPCIONAL.

D.4.2 Implementación de un servidor Web IPv6.

Con el propósito de probar alguna aplicación de tipo servidor que funcionara con el protocolo IPv6 y que además permitiera dar a conocer el trabajo de grado “IPv6 para manejo de redes multiservicio”, se decidió implementar un servidor Web que funcionara tanto con IPv6 como con IPv4 de tal forma que usuarios con cualquiera de los dos protocolos pudieran acceder a la primera pagina IPv6 de la Universidad del Cauca. La página muestra la misma información para los dos protocolos, pero esta informara al cliente que protocolo esta utilizando, dependiendo de si esta conectado con una dirección IPv6 o con una dirección IPv4, Además se utiliza una imagen estática para IPv4 y la misma imagen pero en movimiento para IPv6.

Instalación del servidor Web Apache.

Desde la página oficial de Apache www.apache.com se descarga la versión que se desee utilizar del servidor Web, para trabajar con Windows XP es recomendable descargar una de las últimas versiones, en el momento de escribir este documento la versión del servidor Web apache más reciente para Windows es: apache_2.0.45. Se puede descargar el paquete de instalación MSI (apache_2.0.45-win32-x86-no_ssl.msi).

Una ves se obtiene el paquete de instalación, se descomprime y se procede a instalar el servidor apache, este se instalara como un servidor Web para IPv4, se puede probar el servidor utilizando el Web browser digitando localhost o 127.0.0.1.

Para poder configurar el servidor para que funcione con IPv6 se debe descargar desde la pagina http://win6.jp/Apache2/index.html el parche para habilitar IPv6 en el servidor Web apache, se debe descargar la versión correspondiente a la versión de apache instalada en el computador, para la versión de apache_2.0.45 esta el paquete "httpd-2.0.45-win32-ipv6.zip" que contiene los archivos necesarios para habilitar IPv6 en esta versión de apache.

Instalación binaria para habilitar el servidor Web Apache con IPv6.

Sobre escriba los siguientes archivos sobre la versión de apache ya instalada correspondiente a este parche.

- bin/ * .exe
- include / * .h
- lib/ *
- modules/ * .so

Si es necesario (Ej. limitar el acceso), modifique el archivo conf/httpd.conf. Un ejemplo de configuración de muestra se encuentra en el paquete conf/httpd.conf

Requisitos del sistema:

Sistema operativo:
Microsoft Windows XP
Microsoft Windows 2000 SP2 + IPv6 Vista previa de la Tecnología (20001205)

Compilación de la fuente:

Microsoft Visual C++ 6.0 SP5 o superior
Plataforma de Microsoft SDK Nov. 2001 o superior (REQUERIDO)

Nota:
Si se desea que apache IPv6 se compacte y escuche los sockets tanto de IPv6 como de IPv4, se debe especificar en la configuración conf/httpd.conf de la siguiente manera

listen [::] :80
listen 0.0.0.0:80

Apache IPv6 se enlaza solo con sockets IPv6 por defecto.

La versión 2.xx de Apache tiene inicialmente características IPv6. En la plataforma Win32, sin embargo, IPv6 no esta activada. Este paquete contiene los parches necesarios para habilitar apache con IPv6.

Para probar que la configuración funciona correctamente con el protocolo IPv6 se deshabilita la opción para funcionar con IPv4 en el archivo de configuración de apache "httpd.conf" y se utiliza el Web browser de Internet Explorer con la opción del servidor

proxy deshabilitada y se digita localhost, si funciona con IPv6 el servidor informara que esta listo, en caso contrario repita los pasos anteriores.

El Web browser (Internet Explorer).

Forzar las conexiones IPv6 usando el Web browser (Internet Explorer).
Las nuevas extensiones DLL de Internet DLL, Wininet.dll, permite al Web browser acceder servidores Web IPv6 habilitados. Por ejemplo, Wininet.dll es usado por Microsoft Internet Explorer para hacer conexiones con un servidor Web para ver páginas Web. El Internet Explorer usa IPv6 para descargar paginas Web cuando el Sistema de Nombre de Dominio (DNS) la pregunta (o archivos de host) por el nombre del servidor Web en el URL retorna una dirección IPv6. Se puede conectar entonces a nombres que sólo se resuelven con IPv6. Para verificar que los DNS solicitan registros de direcciones IPv6, se intenta hacer ping al nombre de dominio del servidor Web usando la herramienta Ping6.exe.

Nota: con el Internet Explorer no se puede establecer conexiones usando una dirección IPv6 literal. Las URLs que usan el formato de direcciones IPv6 literales descrito en el RFC 2732, "Formato para las direcciones IPv6 Direcciones Literales en URLs" no podrán ser descargadas por Web browser ya que este formato no es soportado por la versión de Internet Explorer proporcionada con Windows XP.

Nota: El Internet Explorer no puede mostrar sitios Web IPv6 si se configuran para usar un servidor Proxy. Cuando el Internet Explorer se configura para usar un servidor proxy, todas las peticiones de resolución de nombres de los sitios Web se reenvían al servidor proxy.

La primera Pagina Web IPv6 de la Universidad del Cauca.
Teniendo en cuenta que el Internet Explorer proporcionado por Windows XP no soporta el formato de direcciones literales descrito en el RFC 2732 se hizo necesario la utilización de un nombre proporcionado por un servidor DNS con el cual cualquier persona con un equipo que soporte IPv6 y que utilice el Internet Explorer o cualquier otro Web browser que soporte IPv6 pudiera acceder a la primera pagina IPv6 de la Universidad del Cauca sin tener que utilizar el formato de direcciones literales.

Para solucionar este pequeño problema surgieron dos posibles soluciones: una era habilitar un servidor DNS para IPv6 utilizando Windows 2000 Server y la otra solución era utilizar el nombre proporcionado por freenet6 para poder acceder a la página IPv6 de la Universidad del Cauca de manera temporal mientras se adquiere experiencia en la configuración de un servidor DNS para IPv6.

La primera solución no se implemento debido a que esta fuera de los propósitos de este trabajo de grado, así que se decidió utilizar la segunda solución, ya que era más inmediata que la primera y no requería de experiencia en la configuración de un servidor DNS para IPv6 además era suficiente para probar el funcionamiento de las aplicaciones con IPv6. Utilizando el nombre proporcionado por freenet6 (ipv6unicauca) en el momento de la solicitud del túnel IPv6 sobre IPv4 se puede acceder desde cualquier equipo con IPv6 y con un Web browser que soporte IPv6 a la primera pagina IPv6 de la Universidad

del Cauca, desde cualquier lugar del mundo. La dirección completa para acceder al sitio desde cualquier lugar del planeta es de la forma userid.server_name.freenet6.net en donde userid es la cuenta de usuario final y server_name es el servidor TSP (tsps1) que provee la conectividad al sitio así la dirección de la pagina de la universidad será ipv6unicauca.tsps1.freenet6.net.

Como diferenciar la página Web con IPv4 de la página Web con IPv6.

Muchos sitios especializados en el protocolo IPv6 como lo es la página del foro de IPv6 (www.ipv6forum.com) ofrecen el servicio tanto para usuarios IPv4 como para usuarios IPv6. la forma que utilizan para diferenciar un protocolo del otro varia de un sitio a otro en algunos simplemente informan con una imagen diferente para cada protocolo como en el caso del ipv6forum en donde para IPv4 se puede observar un mundo estático y para IPv6 aparece el mismo logotipo pero en movimiento, otras lo hacen a través de un mensaje en donde informan que protocolo se esta utilizando como en el caso de www.kame.net para la pagina de la Universidad se utilizo una combinación de las dos a través del siguiente script php que permite diferenciar un protocolo del otro.

```
<?php
function protocolo() {
$ip = getenv ("REMOTE_ADDR");
if (substr_count($ip,":") > 0 && substr_count($ip,".") == 0){
	echo "You're using <a>IPv6</a>! Your address is $ip ";
}
else{
	echo "You're just using IPv4 $ip ";
}
}
?>
```

Utilizando este script php en la página se puede ver un mensaje como este:

"Usted está usando IPv6"

El script php muestra un pequeño mensaje al fondo de la pantalla que dice el protocolo que está usando: IPv4 o IPv6.

Se necesita un segundo substr_count () porque las direcciones IPv4 se colocan en la forma de ::FFFF:123.123.123.123.

Para observar el trafico IPv6 intercambiado a través de la pagina se utilizo Ethereal (el análisis y los procedimientos para utilizar Ethereal no se detallan en este documento ya que no es el propósito de este trabajo analizar este software ni los datos suministrados por este, solo se utiliza como una herramienta para observar el trafico IPv6), además de este software y del que se analiza en este anexo existen una gran variedad de sniffers y software para capturar cualquier tipo de paquetes incluyendo los paquetes TCP/IP como por ejemplo el “Analizer”, software creado en el Politécnico di Torino. Mas adelante en

este anexo se describirá de manera detallada un software que emula un analizador de protocolo para el análisis de las diferentes tramas IPv6. En la Figura D.9 se puede observar una captura con Ethereal del trafico IPv6 de la pagina IPv6 de la Universidad del Cauca. También se puede observar en la Figura D.10 una captura en tiempo real de trafico IPv6 con el Analizer.

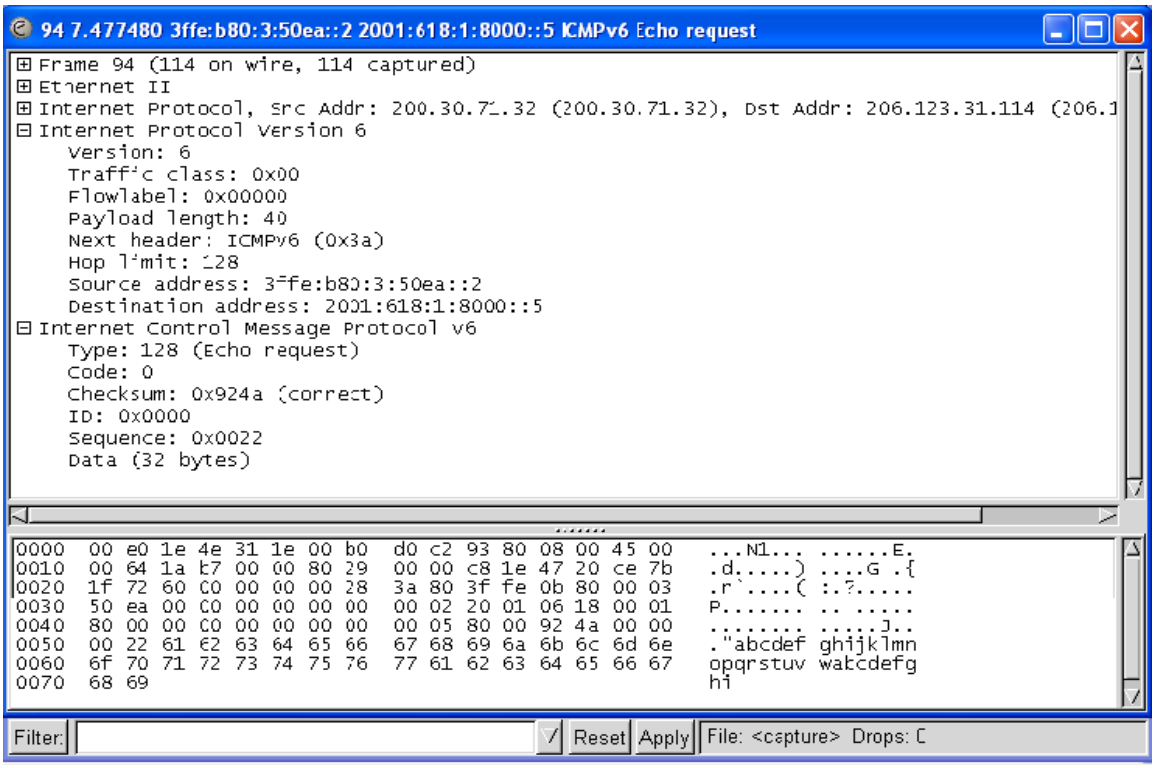

Figura D.9 Ejemplo de captura con Ethereal del trafico producido por la pagina Web IPv6 de la Universidad del Cauca.

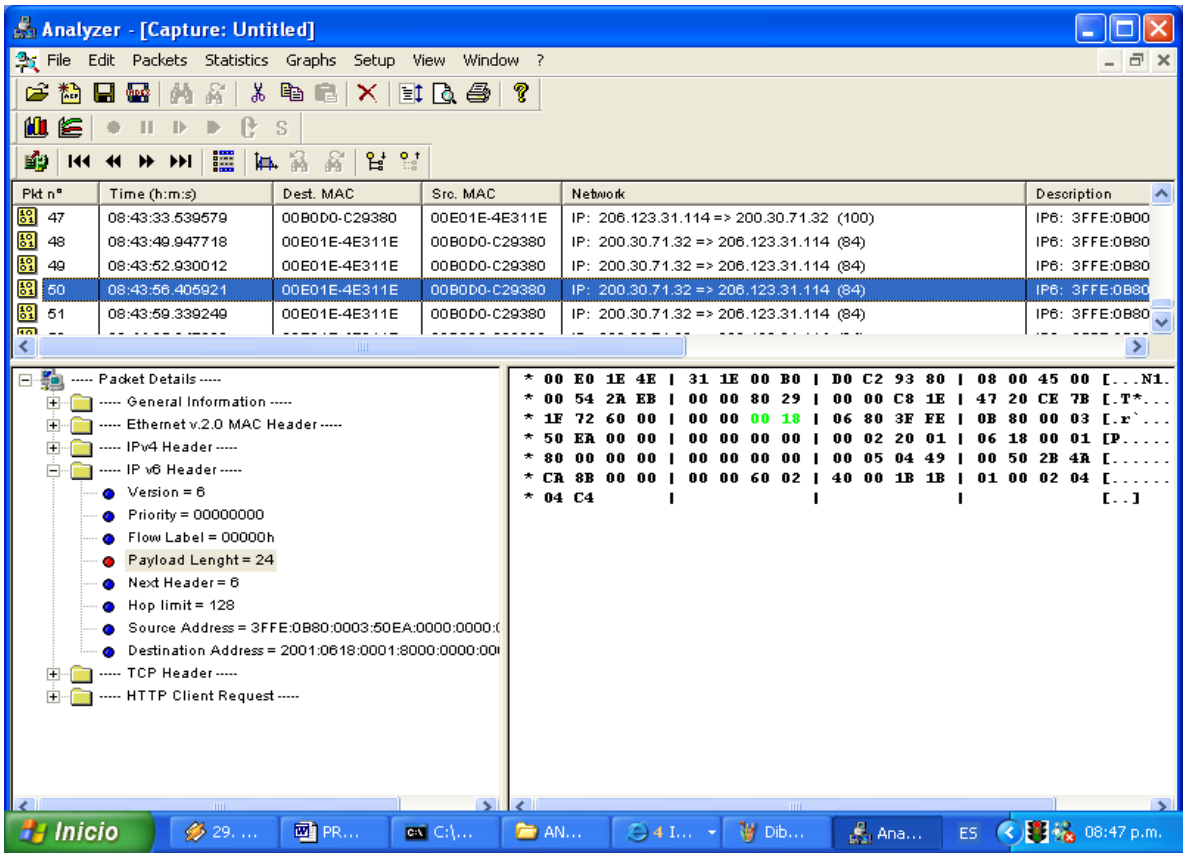

Figura D.10 Ejemplo de captura de trafico IPv6 desde la Universidad del Cauca utilizando Analizar.

D.5 Características generales del Analizador RC-100WL (Demo).

Antes de especificar las características generales del software RC-100WL y de describir las practicas hechas con el mismo, se van a dar los pasos para la instalación de este programa.

D.5.1 Instalación del software RC-100WL.

1. En el CD entregado con la monografía y los anexos del trabajo de grado: IPv6 para el manejo de Redes Multiservicio, buscar la carpeta llamada analizador.
2. En la carpeta analizador encontrara archivos comprimidos denominados **disk,** estos van desde el disk1 hasta el disk 11.
3. Dos de los archivos denominados disk, ya han sido descomprimidos: el disk 2 y 3 para ayudar con la instalación.
4. En la carpeta analizador, también existe un archivo llamado **set up**, el cual al ser ejecutado lleva al usuario a la instalación del programa, ejecute este archivo.
5. Siga los pasos que el set up le pida, recuerde que debe dar la ruta exacta para acceder al disk que se le pida, esto lo puede hacer utilizando el botón browse que le muestra el proceso del set up.

El objetivo de las prácticas con la aplicación RC-100WL, no es solo la visualización de los diferentes protocolos sino que también permite al usuario familiarizarse con las funcionalidades básicas de equipos que permiten el análisis de protocolos.

El analizador RC-100WL, puede ser utilizado en forma de DEMO o en forma real, para analizar los datos que fluyen por determinada red, sin embargo para poder hacer esto de manera real se necesita de un equipo HW para capturar las tramas, equipo con el cual no cuenta este grupo de trabajo, de todas formas si se puede utilizar el analizador en la forma DEMO, con lo cual podemos describir los paquetes IPv6 e IPv4, paquetes previamente bajados de la red y utilizados por el DEMO.

A continuación hacemos una descripción general de las capacidades de este analizador así como de los resultados de nuestra práctica con el DEMO.

D.5.2 Conceptos básicos.

Procesos: Los procesos son las diferentes operaciones realizadas para efectuar el análisis de una línea, ellos son: monitoreo y simulación, el monitoreo tiene por ejemplo: La captura de datos, estadísticas (colección y generación de información estadística), grabar y mostrar (capturar y almacenar datos directamente en el disco duro del PC), análisis (análisis en tiempo real) y la simulación (WAN, LAN, ATM, tramas determinadas según selección de usuario y establecimiento de parámetros). Todos los procesos son totalmente independientes uno del otro y pueden ser efectuados simultáneamente.

Clases de tramas: Una clase de trama esta determinada por ciertos criterios que definen específicos tipos de tramas para el analizador. Los filtros y los gatillos usan estas clases

de tramas en su definición. Ejemplos de clases de tramas son: Tramas erróneas o todas las tramas transmitidas en una determinada red a un destino específico (ejemplo, direcciones VCI/VPI). El analizador cuenta con un determinado grupo de clases definidas.

Filtros: Le permiten al operario el control de que datos, son manejados por procesos específicos. Los datos que no pasan por el filtro son ignorados. Con los filtros se garantiza que los recursos del analizador son utilizados lo mejor posible. Los filtros son definidos de acuerdo a las clases de trama y pueden ser utilizados en tiempo real y en procesos post captura Ejemplo: en captura, estadística y análisis. Los filtros definidos en un proceso pueden ser utilizados en otro proceso. Un ejemplo de un filtrado puede ser para todas las tramas erróneas que son transmitidas a una dirección específica. Los filtros son utilizados para concentrarse en un determinado objetivo particular o para buscar los problemas que suceden en la línea de transmisión.

Eventos: Un evento esta constituido por criterios que definen secuencias especificas en las ocurrencias de las tramas por un tiempo determinado. Por ejemplo se puede definir un evento para poder chequear una cantidad de 20 tramas erróneas en un periodo de 5 segundos. Existen eventos predefinidos en el software de simulación.

Gatillos: Los gatillos permiten controlar el comienzo y la parada o finalización de un proceso particular, estos se encuentran definidos de acuerdo a los eventos y son activados cuando determinado criterio del evento surta efecto.

D.5.3 Monitoreando procesos.

Monitorear una línea involucra la captura pasiva de los datos que fluyen entre dos entidades que se comunican. Los procesos para monitorear aseguran la completa transparencia de la línea, no se efectúa ningún cambio en los datos que se capturan, los procesos que se efectúan son los siguientes:

- Captura: Permite capturar datos de la línea que esta siendo objeto de análisis, claro esta de acuerdo a lo que se definió en los filtros y gatillos.

- Estadística: Permite informarse acerca de los datos que transcurren por la línea bajo análisis, en cuanto a bps transcurridos en determinado tiempo.

- Análisis: Permite obtener estadísticas descriptivas de los datos, en forma de tabla, gráfica lineal, en barras, gráficas 3D o en forma de torta.

- Registro del fondo: Permite capturar un número específico de tramas directamente al disco duro, esto es de particular utilidad para reservar las capacidades del buffer, cuando se tiene la parte HW del analizador.

- Estado de la línea: Muestra de una forma detallada los errores físicos detectados en la línea.

D.5.4 Proceso de simulación.

La simulación involucra directamente dos caminos de comunicación entre el analizador de protocolos y los equipos de comunicación con los cuales el analizador esta intercambiando datos. Para determinar las propiedades de la simulación (por ejemplo: Frecuencia, tamaño y contenido de las tramas transmitidas) este modo de operación es útil para probar los equipos de comunicación con el analizador.

El analizador provee el software de simulación básico para la transmisión del tipo de tramas HDLC or ATM, análisis de BER, análisis de redes WAN. Dependiendo de la configuración que se le realice y del HW que se tenga para realizar otro tipo de simulaciones como son: Frame Relay, X.25, Ethernet y ATM Signalling.

D.5.5 Estados de los procesos.

Proceso de monitoreo: Tiene tres posibles estados:

- Listo: En el cual el proceso esta listo para correr. En este estado se puede establecer los parámetros requeridos para el monitoreo usando el botón de set up.

- Corriendo: En esta etapa el proceso esta activo(o corriendo), recolectando datos de acuerdo a lo definido por el usuario. Este momento se activa cuando se hace click el botón GO, después de definir los parámetros de monitoreo en el estado listo.

- Análisis, vista de datos: Este estado es alcanzado cuando el proceso es detenido. Este proceso es completado haciendo click en el botón DONE que retorna al usuario al estado listo.

Estos tres procesos de monitoreo se ilustran en la Figura D.11.

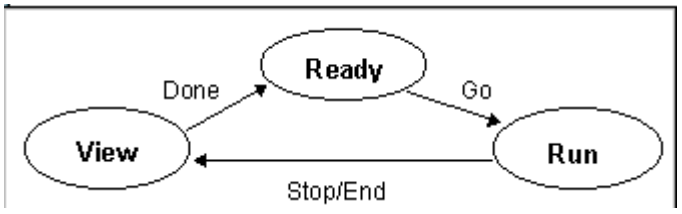

Figura D.11 Estados del proceso de monitoreo.

Proceso de simulación: Tiene dos posibles estados:

- Listo: En este estado se dan los parámetros para la simulación usando el botón de set up.

- Corriendo: En este estado el proceso esta corriendo y simulando datos, de acuerdo al modo de operación, este estado es activado cuando se selecciona el botón GO, después de definir los parámetros de simulación en el estado de listo.

Los dos estados de simulación se representan en la Figura D.12.

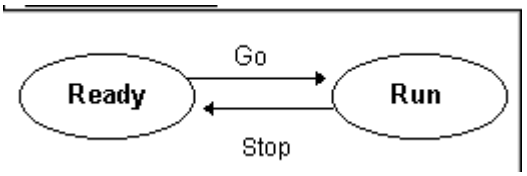

Figura D.12 Estados del proceso de simulación.

D.5.6 Modos de trabajo del analizador.

El modo de trabajo del analizador es monitor. Este modo de trabajo es el suficiente para la operación de los siguientes procesos.

- Captura
- Estadísticas
- Análisis
- Estado de línea
- Registro de fondo

A continuación se explicaran estos procesos más a fondo:

Proceso de captura.

Ventana del proceso de captura: La ventana del proceso de captura representa el estado de listo, del proceso de captura y es utilizada para definir la captura de parámetros y empezar con el proceso.

La ventana de captura contiene la información concerniente a la definición de los parámetros para el proceso de captura. El analizador contiene parámetros predefinidos que permite empezar con el proceso de captura inmediatamente, presionando el botón GO. Alternativamente se pueden definir otros parámetros por ejemplo: filtros para capturar cierto tipo de datos, usando el botón set up, ver Figura D.13.

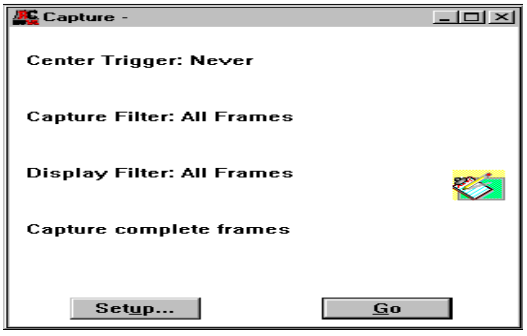

Figura D.13 Ventana del proceso de captura.

Entrando los datos de captura: Los parámetros de captura pueden ser definidos para determinar un rango de monitoreo, se pueden definir: filtros, gatillos y hasta la parte de cada trama a ser guardada en memoria. Los filtros determinan que tramas serán almacenadas en la memoria (por ejemplo capturar las tramas erróneas). El gatillo determina cuando el analizador empezará o parara a pasar tramas al filtro de captura. Para entrar los parámetros de la captura se da click en el botón set up en el estado de listo. El recuadro de set up es mostrado en la Figura D.14.

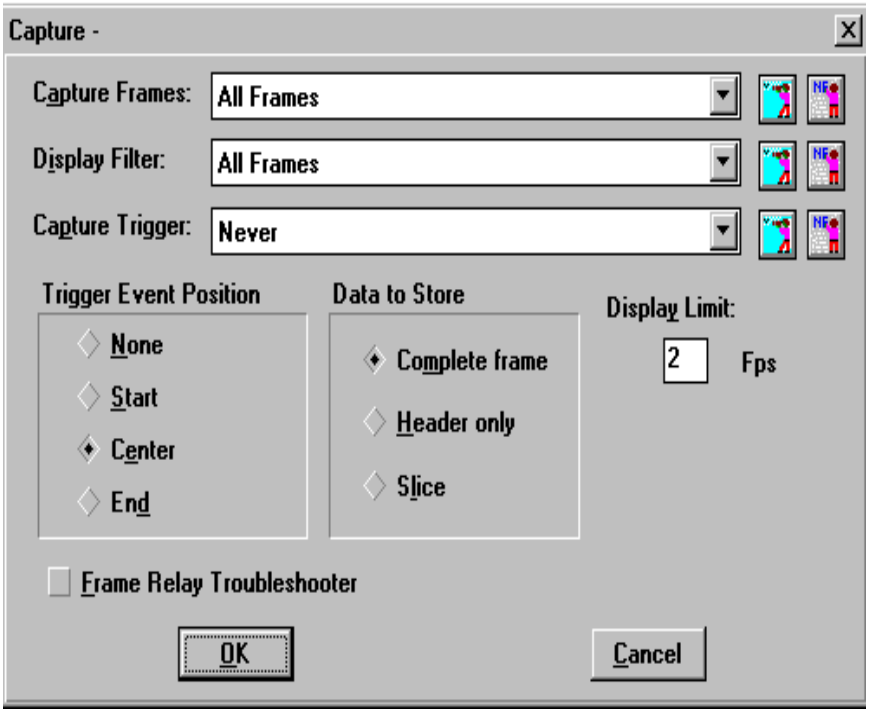

Figura D.14 Ventana del set up de datos para el proceso captura.

USAR LA OPCIÓN	PARA
CAPTURA DE TRAMAS	Determinar las tramas ha ser capturadas. Para especificar un filtro de captura, también puede seleccionar uno de los filtros existentes, modificar un filtro determinado, o crear un nuevo filtro.
DESPLIEGUE DE FILTRO	Determina que tramas serán mostradas durante el proceso de captura.
CAPTURA DE GATILLO	Especifica un evento en el cual el gatillo dará comienzo o parada a un proceso en particular.
POSICION EVENTO DEL GATILLO	El gatillo determina cuando las tramas serán aceptadas, acorde esto a los parámetros introducidos en el filtro. Ninguna, cuando el gatillo no ha sido especificado, el proceso de captura inicia inmediatamente y se detiene cuando la ram de captura se llena, o cuando se da click en el botón de parar. Inicio: El proceso de captura se hace de acuerdo a la definición de los filtros.
DATOS ALMACENADOS	Especifica la parte de las tramas capturadas que será almacenada en la ram. Trama completa, almacena la totalidad de la trama, únicamente cabecera, guarda unos 80 bytes desde el inicio de la tramas. Slice, almacena una parte especifica de la trama, desde el inicio de la misma, cuando esta opción ha sido seleccionada, una ventana que pregunta del tamaño de la selección se abre, tamaño que se da en bytes.
LIMITE A MOSTRAR	Especifica el número de tramas a ser mostradas, por segundo en tiempo real en pantalla. Este valor esta entre 1 y 50 tramas
PROBLEMAS EN LAS TRAMAS	Con esta selección se autoriza al analizador para que detecte las tramas fallidas de ciertos protocolos.

Tabla D.6 Descripción de las opciones de la ventana del set up del proceso de captura.

Corriendo el proceso de captura: Una vez completado el set up y haciendo click en el boton GO corre este proceso, la Figura D.15 ilustra esto:

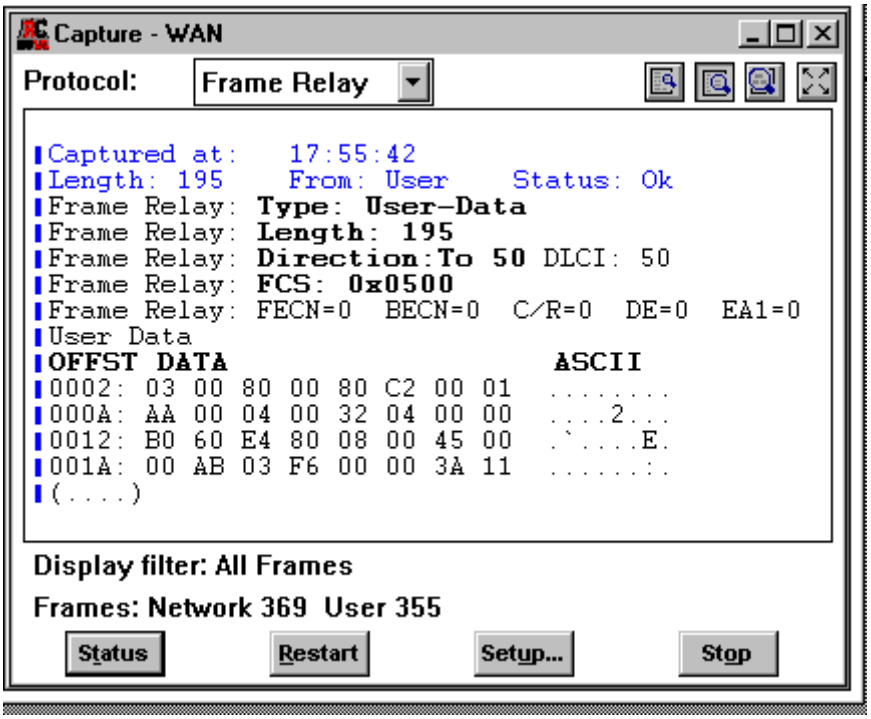

Figura D.15 El proceso de captura corriendo.

Registro de fondo.

La Ventana de registro de fondo es utilizada para definir la captura de parámetros y comenzar con esta, se ilustra en la Figura D.16.

Entrada de datos al registro de fondo: Los parámetros que se definen aquí le permiten al analizador saber cuales son los datos que se grabaran en el disco. Se deben especificar los filtros para permitir que el analizador se enfoque en cierto tipo de datos. Además se debe definir la cantidad y las partes especificas de los datos a ser grabados.

Para entrar los datos al registro de fondo se debe dar click en el botón set up, ver Figura D.17.

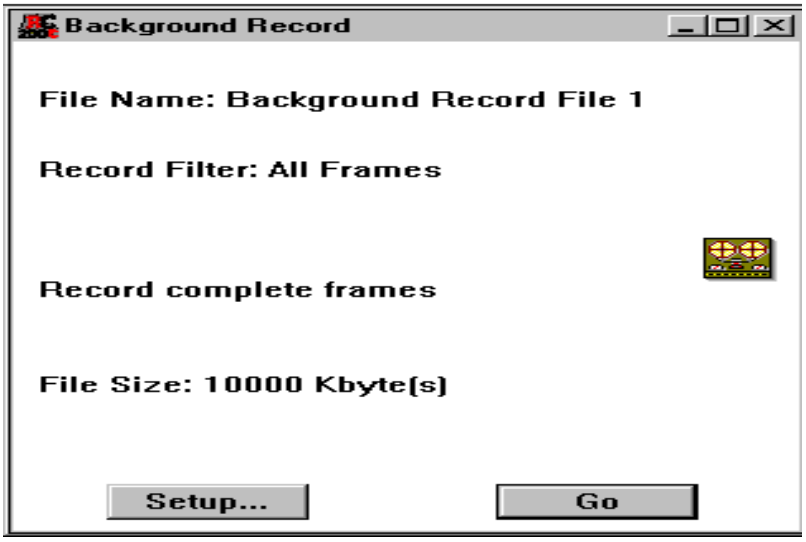

Figura D.16 Ventana del proceso de registro de fondo.

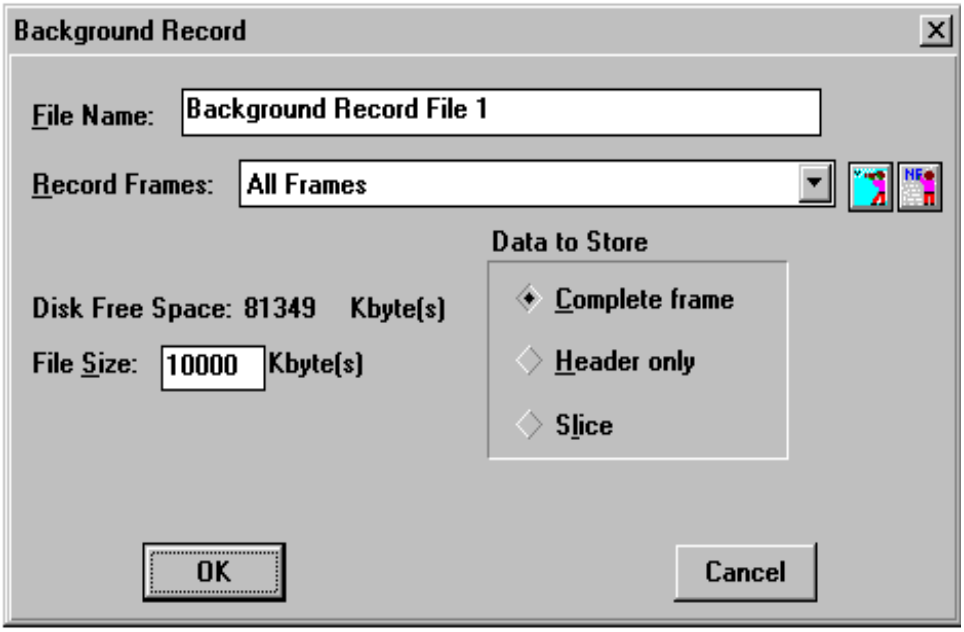

Figura D.17 Ventana del set up del registro de fondo

USAR LA OPCION	PARA
NOMBRE DEL ARCHIVO	Se utiliza para darle algún nombre a los datos grabados.
TRAMAS GRABADAS	Especifica los filtros de captura, que se pueden escoger de una lista, también se pueden crear nuevas clases de filtros y modificar los existentes.
DATOS A ALMACENAR	Especifica que porción de las tramas capturadas se van almacenar, ya sea una parte seleccionada de la trama, una trama completa, también se puede almacenar únicamente la cabecera.
ESPACIO LIBRE EN DISCO	Determina el espacio disponible en el disco duro.
TAMAÑO DEL ARCHIVO	Determina el máximo tamaño del archivo a ser grabado, este debe ser menor que el espacio disponible en el disco.

Tabla D.7 Descripción de las opciones del set up del registro de fondo.

Corriendo el proceso de registro de fondo: Una vez completado el proceso de set up se puede dar inicio al proceso dando un click en el botón GO, ver Figura D.18.

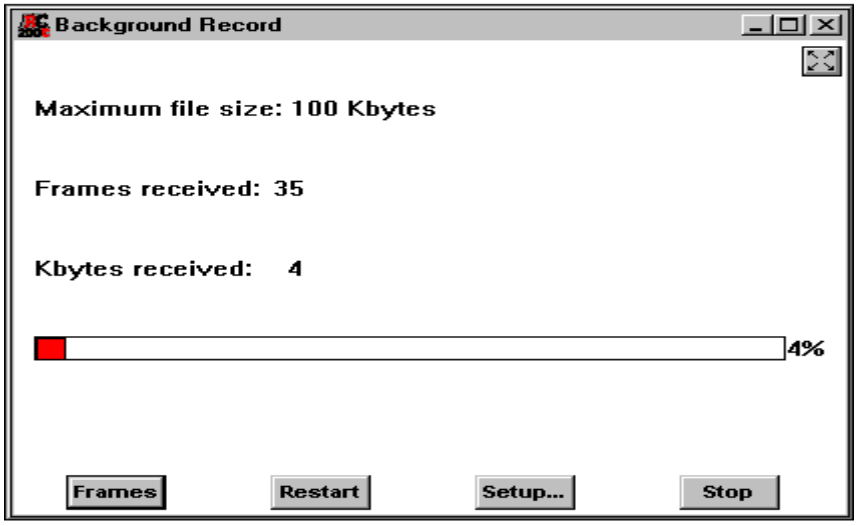

Figura D.18 Ventana que identifica que el proceso registro de fondo esta corriendo.

La barra de progreso indica el porcentaje del máximo tamaño del archivo que se esta usando en determinado momento. El botón denominado tramas despliega el registro de fondo de captura, entonces se empezara a mostrar información del proceso.

Estadísticas.

La ventana de estadísticas es utilizada para definir los parámetros necesarios para el proceso de sacar las estadísticas de los datos que circulan en una red de datos, ver Figura D.19.

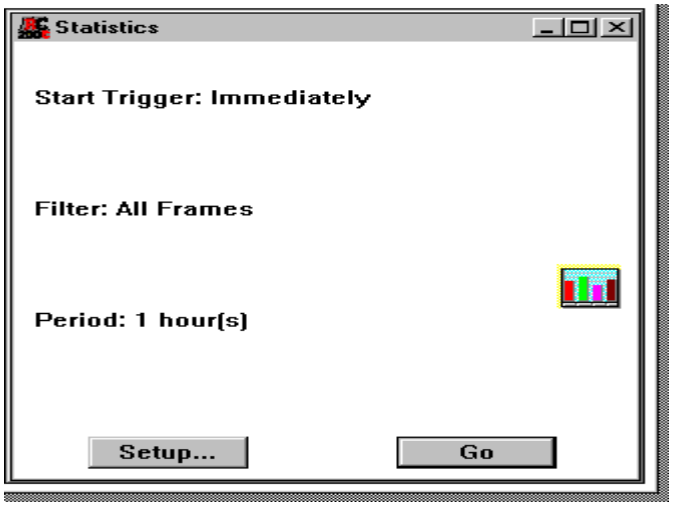

Figura D.19 Ventana del proceso de estadística.

Introducción de los datos para el proceso de estadística: Los parámetros para este proceso pueden ser definidos para determinar un rango de monitor, entre estos parámetros tenemos: Filtros, gatillos y periodos de tiempo, parámetros útiles para la producción de determinada estadística, para introducir los parámetros se da click en el botón set up, ver Figura D.20.

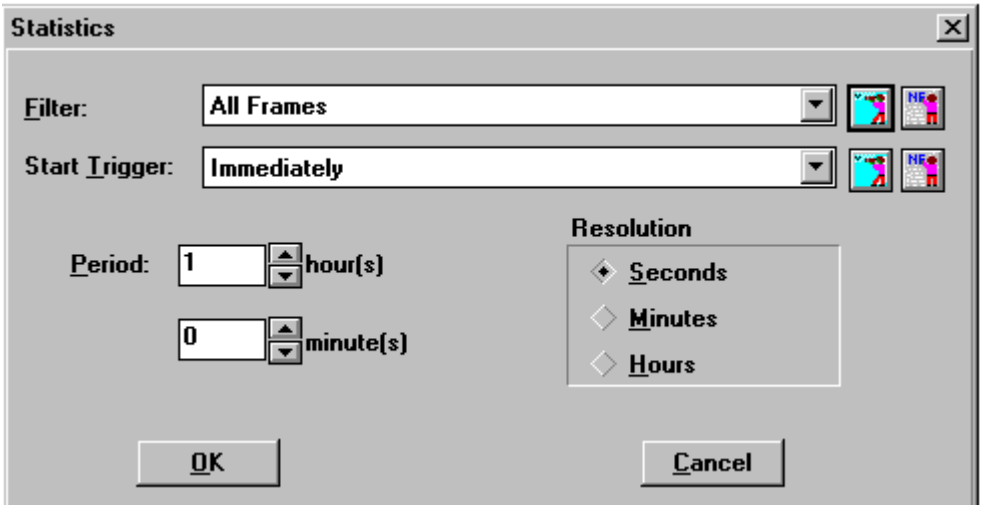

Figura D.20 Ventana del set up del proceso de estadística.

USAR LA OPCION	PARA
FILTRO	Específica el filtro para la realización de las estadísticas, al igual que en los casos anteriores se puede seleccionar un filtro de una lista predeterminada, además se puede crear o modificar un filtro preseleccionado.
GATILLO DE COMIENZO	Determina cuando el proceso de estadística debe comenzar.
PERIODO	Define el periodo de duración del proceso de estadística en horas y minutos, este periodo comenzará después de la activación del gatillo.
RESOLUCION	Selecciona la resolución de los datos, una gran cantidad de datos, pueden llenar muy rápidamente el buffer.

Tabla D.8 Descripción de las opciones del set up proceso estadística.

Corriendo el proceso de estadística: Mediante el accionamiento del botón GO se da inicio a este acto, la ventana que se visualiza en la Figura D.21.

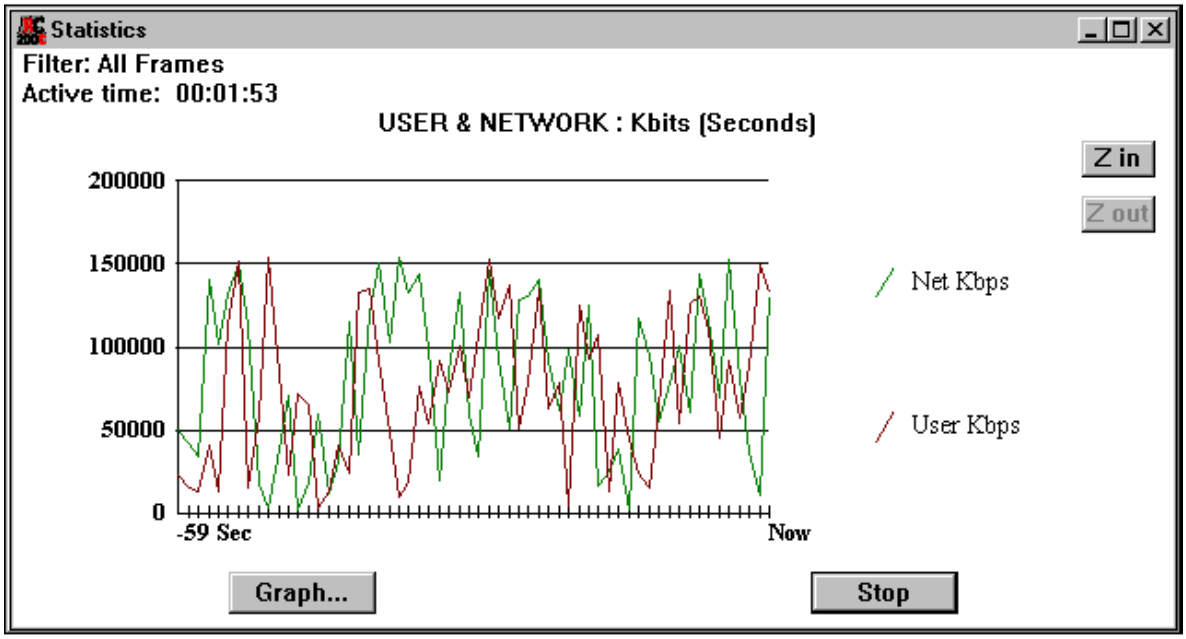

Figura D.21 Ventana del proceso de estadística corriendo.

El filtro escogido en el ejemplo anterior (*All Frames*) se muestra en la parte superior de la pantalla, seguido por el tiempo activo, que es el tiempo que la estadística ha estado corriendo.

En la gráfica se muestra la cantidad de datos en kilobits por segundo que pasan en ambas direcciones, net, representa datos desde la red, user, representa datos del usuario del analizador.

Análisis.

La ventana de análisis es utilizada para definir los parámetros y dar comienzo al proceso de análisis, ver Figura D.22.

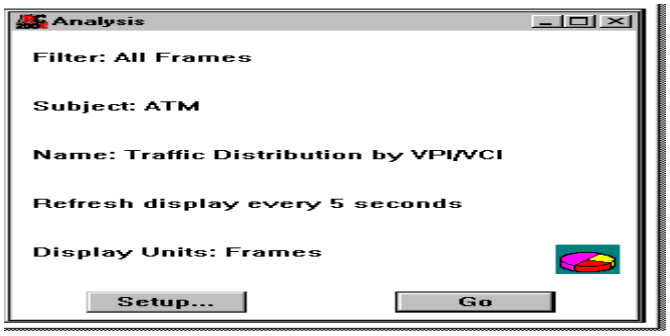

Figura D.22 Ventana del proceso de análisis.

El análisis se realiza a porciones específicas de los datos, en la Figura D.23 se muestra la ventana del set up del proceso de análisis.

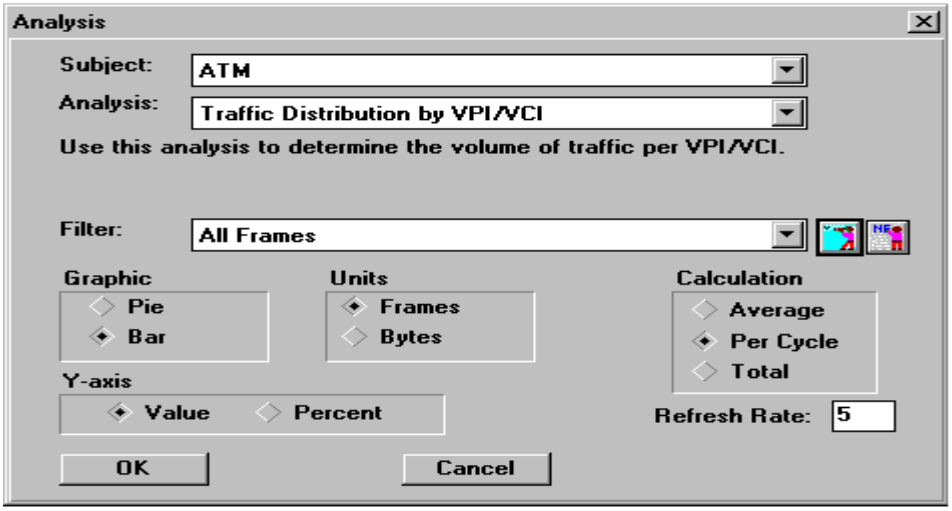

Figura D.23 Ventana del set up del proceso de análisis.

USAR LA OPCION	PARA
ASUNTO	En esta opción, se encuentra una lista que contiene una pila de protocolos.
ANALISIS	Especifica el tipo de análisis, el asunto que se escogió esta relacionado con los análisis en la lista. Un análisis puede estar representado por una tabulación, una gráfica o ambos.
DESCRIPCION	Una corta descripción del análisis seleccionado, esto es útil en la determinación del análisis a realizar.
FILTRO	Especifica el filtro a ser usado en los datos en orden a lo deseado, al igual que en los demás casos existe una lista de filtros o también se puede modificar o crear uno.
GRAFICA	Especifica si mostrar la gráfica en barras o en diagrama de pastel.

UNIDADES	Especifica si el análisis es realizado en bytes o tramas completas.
CALCULO	Especifica el tipo de calculo ha ser realizado en el análisis : Promedio: El número total de tramas o bytes, es dividido por el total del tiempo transcurrido. Pro ciclo: El número promedio de tramas de cada ciclo. Total: El número total de tramas incluidas en el análisis.

Tabla D.9 Descripción de las opciones del set up del proceso de análisis.

Una vez introducidos los datos del set up para el análisis, se puede, correr el proceso dando click en el botón GO, ver Figura D.24.

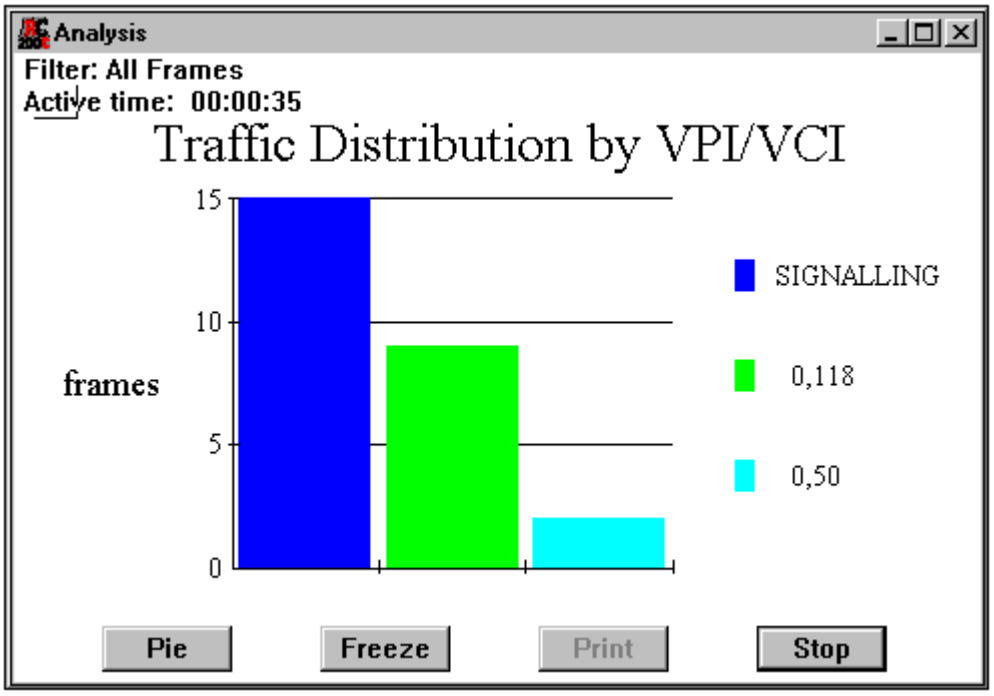

Figura D.24 Ventana del proceso de análisis corriendo.

D.6 Prácticas con el software del analizador RC-WL100.

D.6.1 Practica 1: Descripción de las tramas IPv4 e IPv6 utilizando la aplicación RC-100WL.

Descripción de la trama IPv4.

Para realizar esta práctica se debe iniciar el software, seguir los siguientes pasos:

1. Si instalo el programa en la ruta por defecto que le indico el set up, vaya al menú inicio, de Windows.
2. Busque programas.
3. Busque la aplicación RC-100WL versión 3.20, haga click en RC-100WL Demo. Observará la ventana indicada en la Figura D.25.

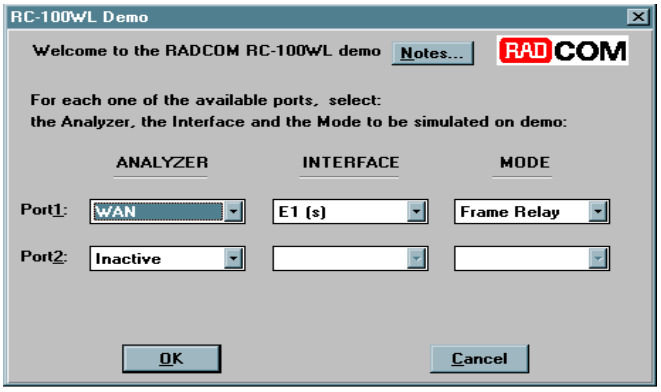

Figura D.25 Ventana para la inicialización de la aplicación RC-100WL.

4. Una vez con esta interfaz, seleccione de la opción ANALYZER, en port 1 la red a analizar para este caso seleccione LAN, cuando haga esto, la opción INTERFACE cambiará a LAN y el modo a ETHERNET, deje estas opciones sin cambio, va a visualizar lo que aparece en la Figura D.26.

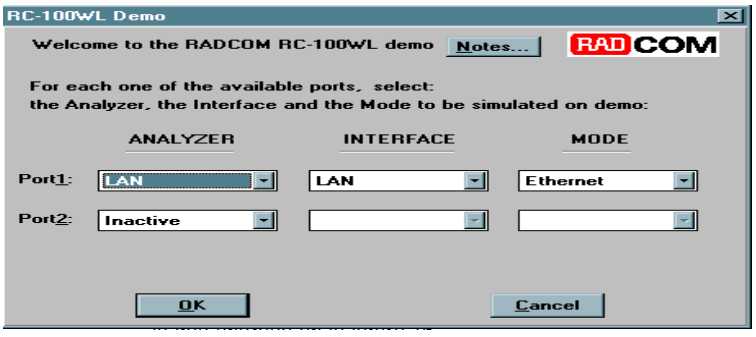

Figura D.26 Configuración de la aplicación para realizar los distintos análisis.

5. De click en OK para iniciar la aplicación. Con esta acción la aplicación cargará los diferentes paquetes necesarios para realizar las distintas simulaciones.
6. En este momento debe estar visualizando la ventana mostrada por la Figura D.27.

En esta ventana se pueden observar además del proceso de captura, otros procesos descritos con anterioridad en este anexo. Para esta práctica se va a utilizar el proceso de captura, los parametros que se describen en el set up de este proceso también se describieron con anterioridad en este mismo anexo. Para esta práctica no se debe realizar ningún cambio en el set up del proceso captura.

Con el software iniciado en el proceso captura, se va a continuar con la descripción de la trama IPv4, para lo cual debe hacer lo siguiente:

1. Dar click en el boton GO de la ventana mostrada en la Figura D.27, observara la ventana mostrada en la Figura D.28.
2. Una vez este el proceso de captura corriendo, en la opción PROTOCOL, escoger IP. Con ello visualizará la trama del protocolo IPv4 como lo indica la Figura D.29.

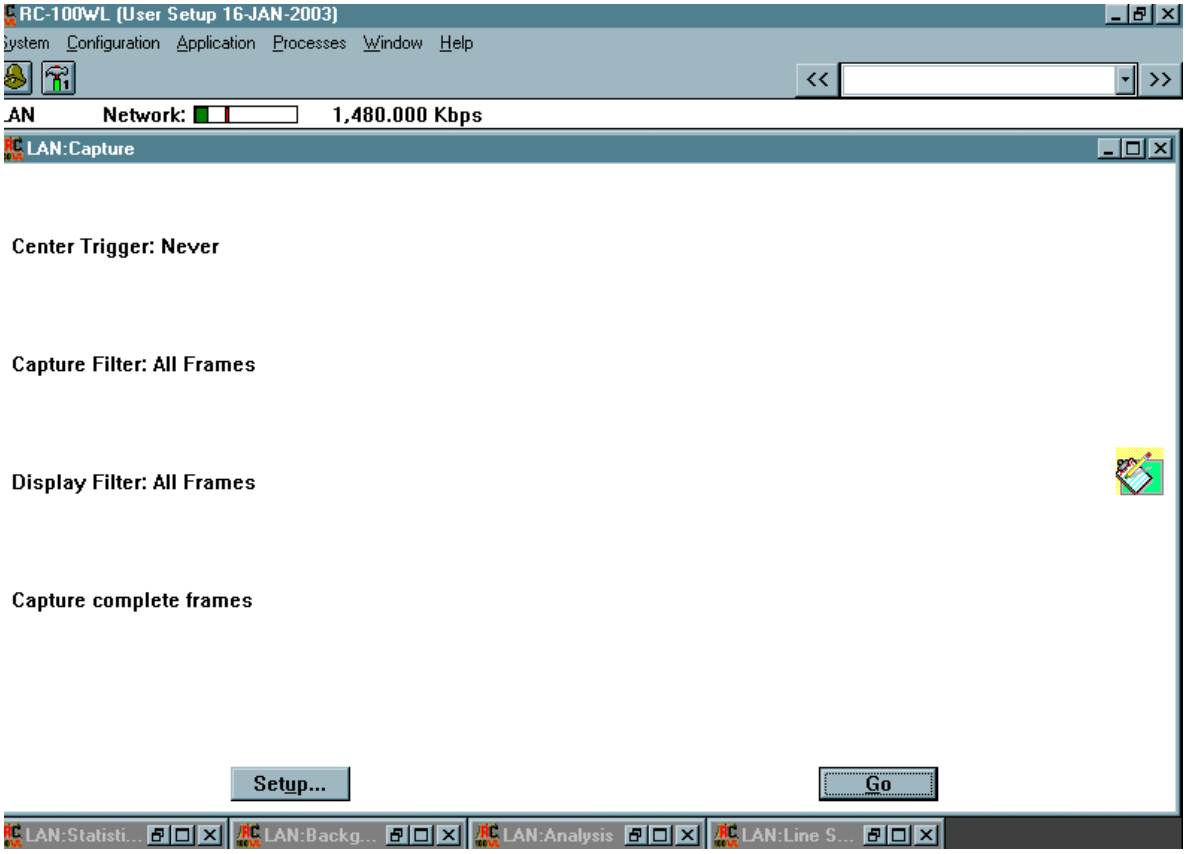

Figura D.27 Ventana del proceso de captura del sofware RC-100WL.

Utilizando esta figura se va a realizar la descripción de la trama IPv4. Con lo cual se tiene una visión más realista de lo mostrado por un analizador de protocolos.

La descripción en este anexo de las diferentes cabeceras, es hecha de acuerdo a la simulación de tráfico y representación de tramas, procedimientos realizados por la aplicación RC-100WL.

Se entra a describir la trama IPv4, basándose en la Figura D.29. En esta se puede ver:

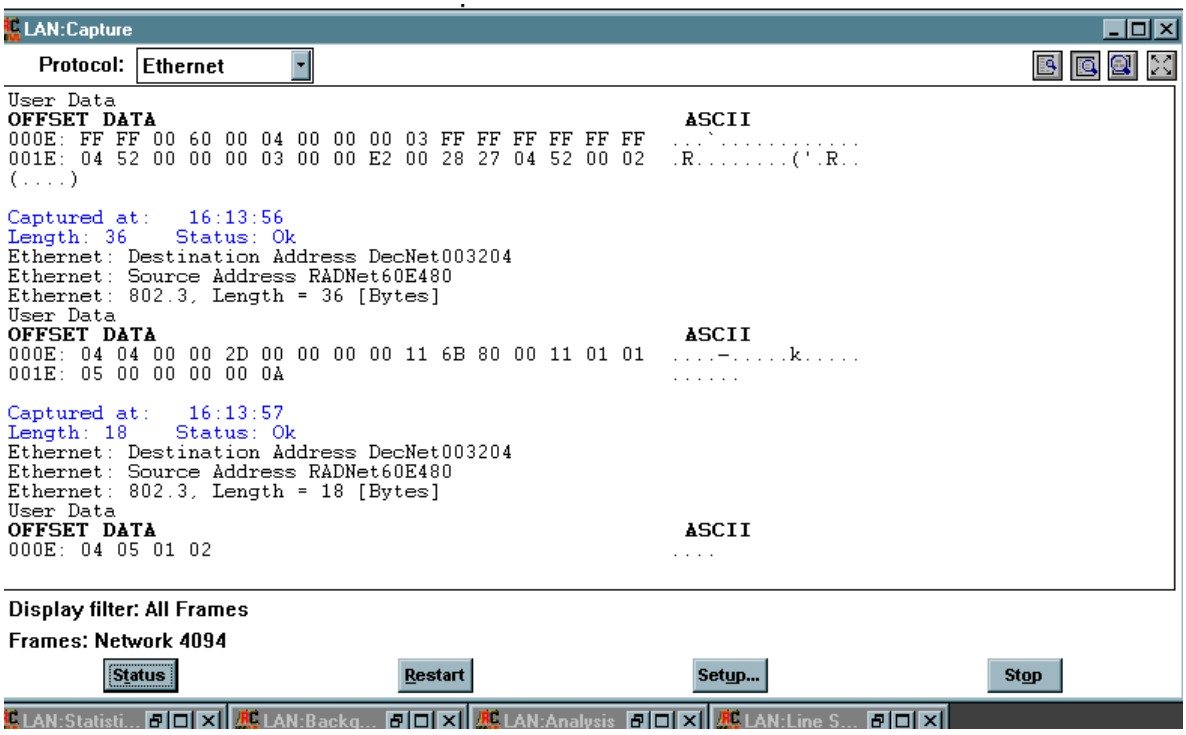

Figura D.28 Ventana del proceso captura corriendo.

IP: version = 4: 4 bits. El campo de versión indica la estructura de la cabecera utilizada, en este caso nos determina que el protocolo utilizado en este flujo de datos es IPv4.

IP: Total length = 84: 16 bits. Longitud de la trama medida en bytes, incluyendo la cabecera y la carga útil. Esta campo permite que la longitud de la trama sea mayor de 65,535 bytes, aunque datagramas tan grandes son no prácticos para la mayoría de los hosts y redes. Todos los hosts deben estar listos para recibir datagramas que estén por encima de los bytes, independientemente de como lleguen, completos o en fragmentos. Es recomendable que los hosts envíen datagramas mayores que 576 bytes, si el destino esta preparado para aceptar tramas largas. En el caso del ejemplo, esta longitud es de 84bytes.

IP: Identifiers = 701: 16 bits. Determina un valor asignado por el que envía, que ayuda en el reensamblaje de fragmentos de la trama, cuando esta ha sido fragmentada.

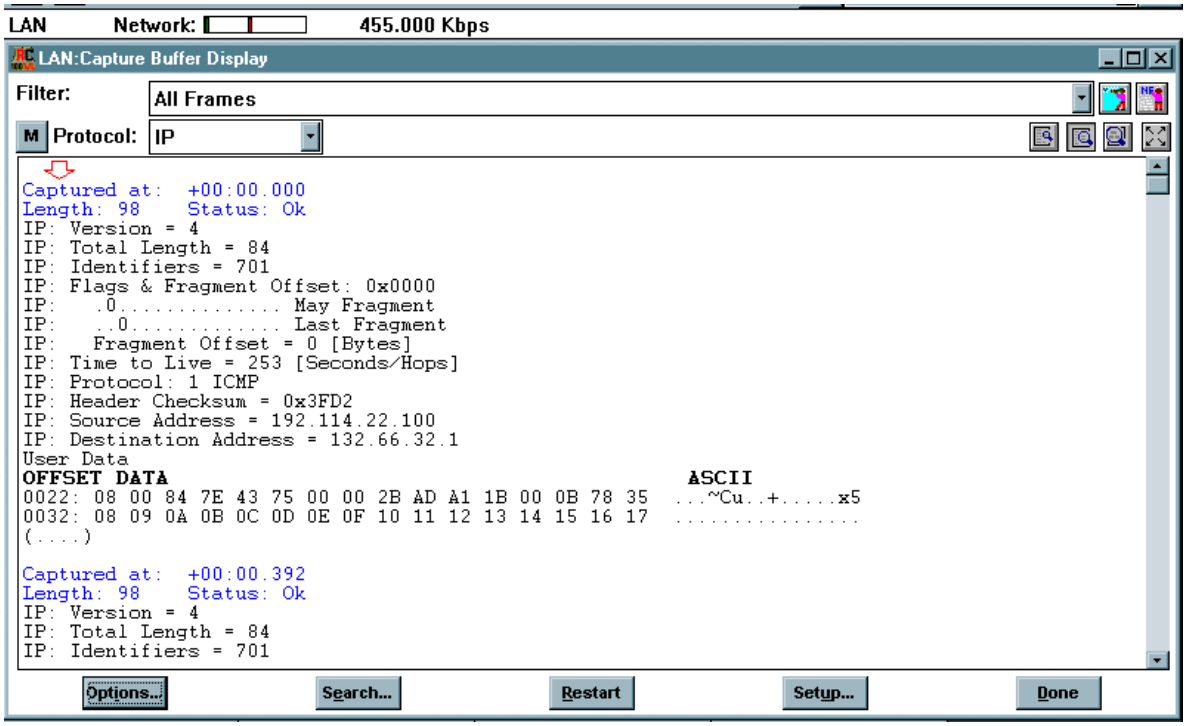

Figura D.29 Visualización de la trama IPv4.

IP: Flags & Fragment Offset: 0x0000

IP: .0.....May Fragment

IP: ....0.....Last Fragment

Lo anterior describe lo denominado Flags o banderas, son 3 bits. Banderas de Control flags:

Bit 0: Es reservado y debe ser cero.

Bit 1: Don't fragment bit: indica si la trama es fragmentada

0 May fragment.
1 Don't fragment.

Bit 2: More fragments bit: indica si es el último fragmento de la trama o existen más.

0 Last fragment.
1 More fragments.

IP: Fragmente Offset = 0 [bytes]: 13 bits. Indica a donde pertenece este fragmento en el datagrama total. El fragment offset es medido en unidades de 8bytes (64 bits).

IP: Time To Live = [253 sec/hops]: 8 bits. Indica el tiempo máximo que la trama tiene permitido permanecer en el sistema de Internet. Si este campo tiene un valor de cero, la trama debe ser destruida. Este campo es modificado en el procesamiento de la cabecera de Internet. El tiempo es medido en segundos. De todas formas, el TTL debe bajar en 1 segundo cada vez que la trama es procesada, con ello se consigue que tramas que no han podido ser entregadas se descarten.

IP: Protocol: 1 ICMP: 8 bits. Indica el protocolo de próximo nivel utilizado en determinada porción de datos en la trama de Internet, en este caso este protocolo es el ICMP.

IP: Header Checksum = 0x3FD: 16 bits. Un chequeo únicamente realizado en la cabecera. Con el cambio de algunos campo por ejemplo: TTL, el header checksum es recalculado y verificado en cada punto en que la cabecera de Internet es procesada.

IP: Source Address = 192.114.22.100 IP: Destination Address = 132.66.32.1: 32 bits cada una. Una distinción, es hecha entre nombres, direcciones y rutas. Un nombre indica un objeto a ser buscado. Una dirección indica la localización de ese objeto. Una ruta indica como llegar a ese objeto. El protocolo de Internet trata principalmente con direcciones. Esta es la tarea de protocolos de niveles más altos (como lo es host-to-host o aplicaciones), el determinar el mapeo de nombres a direcciones.

User Data: Datos de usuario o la cabecera de protocolos de un nivel más alto.

Se entra a describir la trama IPv6, para lo cual se debe hacer lo siguiente:

Viendo la Figura D.29, especificamente la ventana de protocolo, y si en ella se selecciona IPv6, se obtiene lo que se muestra en la Figura D.30. De esta información no es mucho lo que se puede sacar para describir la trama IPv6, por lo tanto, debemos utilizar una de las características que tiene el analizador RC-100WL, la cual consiste en la importación de paquetes previamente existentes. Para la importación de estos paquetes que nos permitirán visualizar la trama IPv6, se deben seguir los siguientes pasos.

1. Teniendo en pantalla la ventana mostrada en la Figura D.30, dar click en la opción aplicación del menú superior.
2. De las opciones desplegadas, dar click en la opción RESTORE FILE. Al hacer esto se despliega la ventana mostrada en la Figura D.31.
3. Con la ventana de la Figura D.31 desplegada, dar click en browse, y escoger la carpeta en donde se encuentran los paquetes para el análisis, estos paquetes para el análisis se encuentran en el CD que se entregó con la monografía del trabajo de grado IPv6 para el manejo de redes multiservicio.
4. Escoger el archivo TUNN_AUT.BIN, para con el poder visualizar la trama IPv6. Una vez hecho esto en el campo From (full path of file), ver Figura D.31, aparece el nombre de este archivo así como la ruta completa para acceder a el.

5. El campo To(description), ver Figura D.31, debe escribirse el nombre del archivo sin extensión: TUNN_AUT. Depues de esto hacer click en OK, con lo cual se ha cargado este paquete en el sistema.
6. Luego de este procedimiento dar click nuevamente en la opcion aplicación del menu superior, ver Figura D.30.

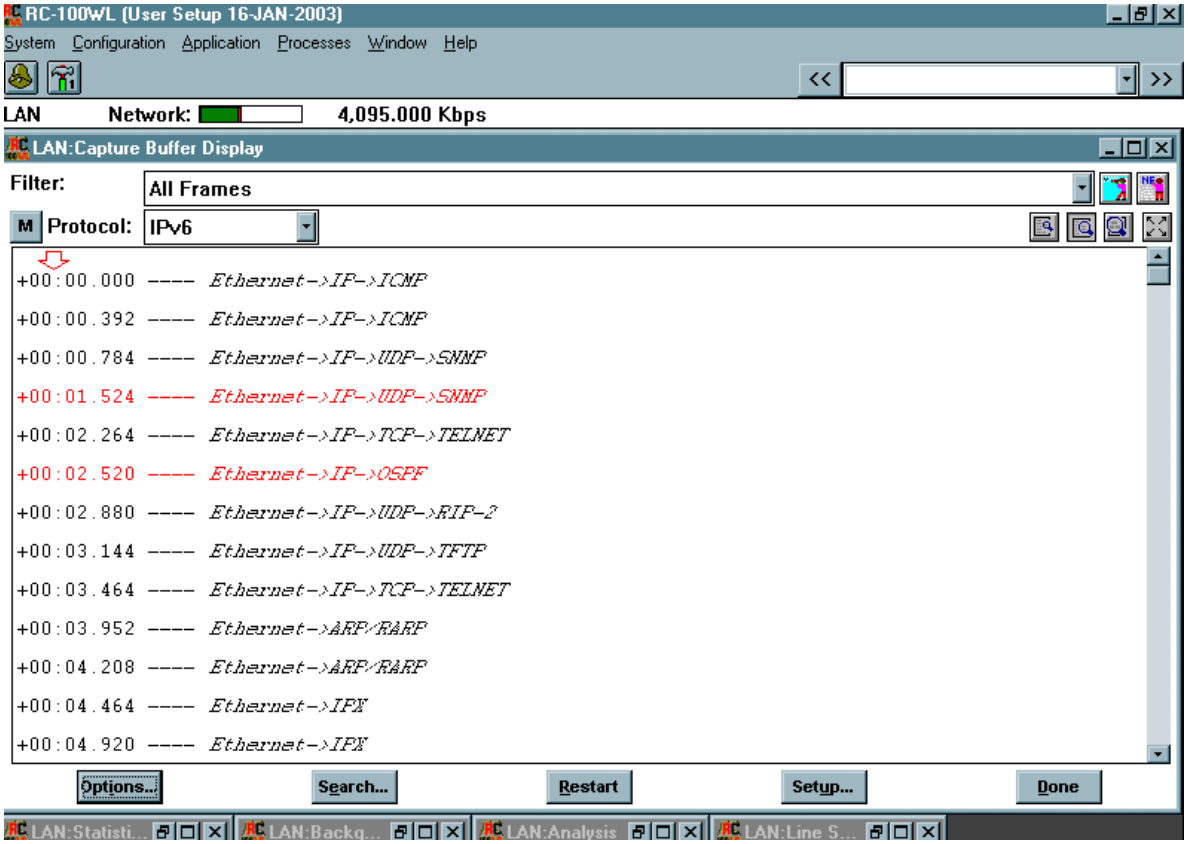

Figura D.30 Selección de la opción IPv6 en la ventana protocol.

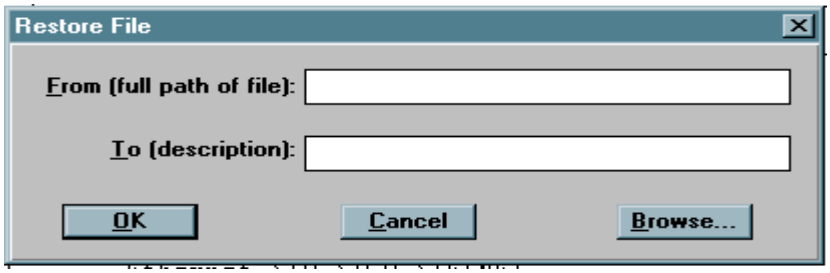

Figura D.31 Ventana para escogencia del paquete a ser analizado.

7. Dar click en la opción off line Analysis, se despliega una ventana en donde debemos seleccionar el archivo que se cargo, ver Figura D.32.

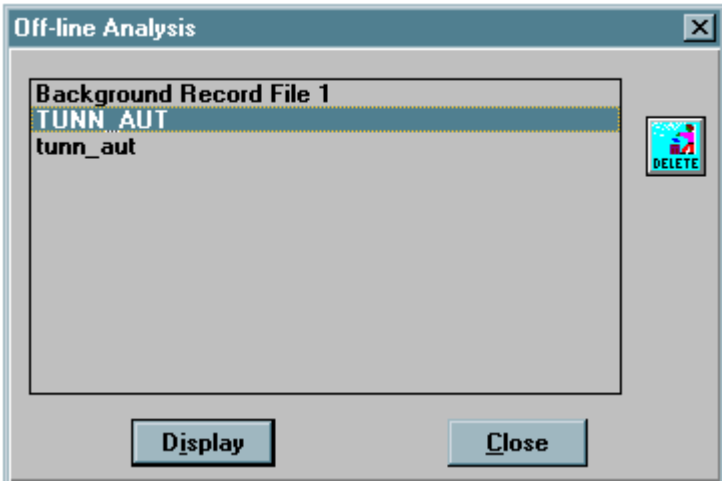

Figura D.32 Ventana en la cual aparece el paquete a analizar.

8. Dar click en display, con lo que se observa lo mostrado en la Figura D.33.

Una vez realizados los pasos anteriores, ya es posible entrar a describir la trama IPv6, según lo que se observa en la Figura D.33.

IPv6: Version: 6: Determina la versión de la trama IP utilizada en Internet, en este caso IPv6.

IPv6: Priority: 15: Permite determinar la prioridad deseada en la entrega de los paquetes. Los valores de prioridad son divididos en rangos: tráfico donde la fuente proporciona control de congestión y cuando no proporciona control de congestión.

IPv6: Flow label: 0x000000 (Packet don´t belong to a flow carry) <000000>: Utilizado por una fuente para nombrar aquellos productos para los cuales se requiere un manejo especial por parte del enrutador IPv6. El flujo es esepcionalmente identificado por la combinación de una dirección y una etiqueta de flujo que no es cero.

IPv6: Pay load lenght: 32: Longitud de la carga útil (en octetos).

IPv6: Next Header: 58 Internet Control Message Protocol: Identifica el tipo de cabecera que inmediatamente le sigue a la cabecera IPv6.

IPv6: Hop Limit: 255: Entero de hasta 8-bits que es decrementada uno a uno en cada nodo que reenvia el paquete. El paquete es desechado si Hop Limit Hop Limit es decrementado a cero.

IPv6: Source Address: FE80::800:2B55:A7A8: Dirección de 128-bits del equipo que origina el paquete.

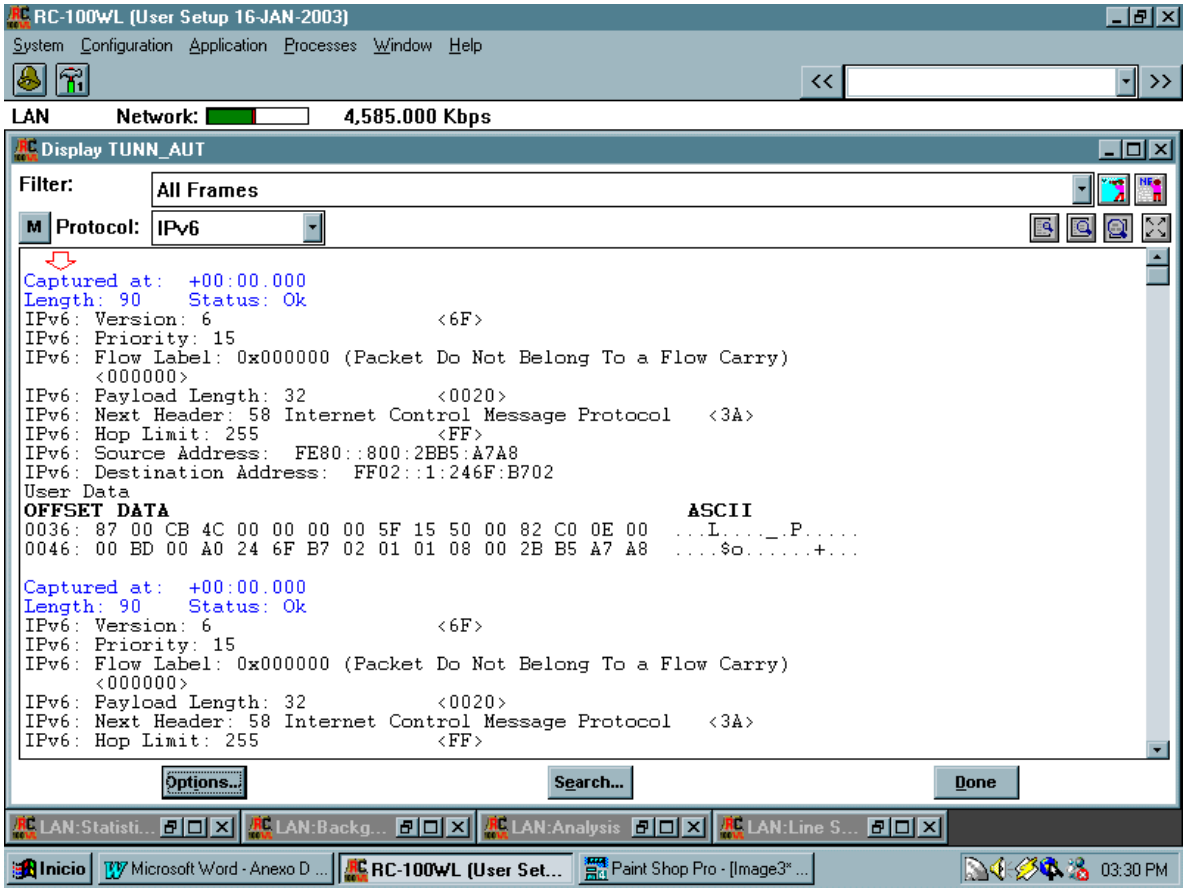

Figura D.33 Visualización de la trama IPv6.

IPv6: Destination Address: FF02::1:246F:B702: Dirección 128-bits del equipo que va a recibir el paquete.

User Data: Carga útil a transportar.

D.6.2 Practica 2: Descripción de algunos mensajes ICMPv6.

Después de realizar la descripción de las tramas IPv4 e IPv6 según se muestran decodificadas por la aplicación RC-100WL, se entra a describir varios ejemplos del protocolo ICMPv6 en las siguientes páginas.

Para visualizar la trama ICMPv6 se deben tener en cuenta los siguientes pasos:

- De la opción protocol que se muestra en la figura 23, seleccionar ICMPv6.
- Con la selección de ICMPv6 se observa lo mostrado en la figura 24.
- Se entra a describir el mensaje ICMPv6 de solicitud de vecindario, ver figura 24.

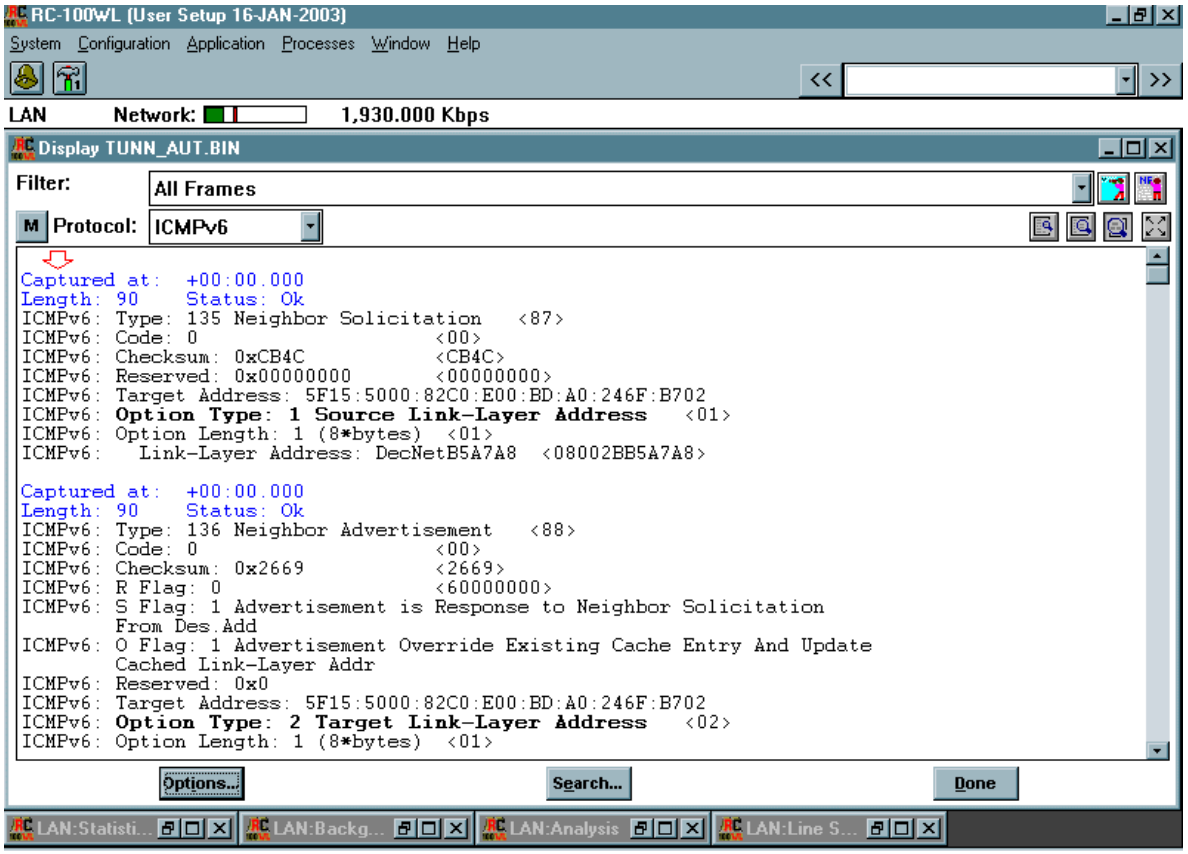

Figura D.34 Visualización mensaje ICMPv6

ICMPv6: Type: 135 Neighbor Solicitation: Con lo cual se presentan mensajes que pueden determinar la existencia de un error en la transmisión o simplemente pueden ser información. Los mensajes de error pueden ser: destino no reconocido, paquete demasiado grande, tiempo excedido, problemas de parámetros. Algunos de los mensajes de información son: petición de eco, respuesta de eco, solicitud afiliación a un grupo, reporte de afiliación a un grupo, reducción de un grupo, entre otras. Cada una de estas opciones es identificada por un número el 135 del ejemplo determina el mensaje de información: solicitud de vecindario.

ICMPv6: Code: 0: Para cada tipo de mensaje varios códigos diferentes son definidos. Un ejemplo de esto es el mensaje de destino no reconocido, donde se puede tener: no hay ruta al destino, comunicación con destino prohibido por el administrador, no existe vecindario, dirección no alcanzable, puerto desconocido. En el caso de los mensajes de solicitud de vecindario este valor de code es cero.

ICMPv6: Checksum: 0xCB4C: Utilizado para verificar el daño de los datos en el mensaje ICMPv6 y de la cabecera IPv6.
ICMPv6: Reserved: 0x00000000: Debe ser inicializando a cero por el que envía e ignorado por quien recibe.

ICMPv6: Target Address: 5F15:5000:82C0:E00:BD:A0:246F:B702: Determina la dirección del nodo objetivo , esto es la dirección IPv6 del nodo al cual el mensaje de solicitud de vecindario a sido enviado.

ICMPv6: Option Type: 1 Source link layer address: Especifica la dirección de capa de enlace de la fuente.

ICMPv6: Option lenght: 1 (8bytes): Determina la longitud del mensaje.

ICMPv6: Link Layer Address: Decnet: B57A8: Determina la dirección de capa de enlace que fue primero presentada por el option type.

Descripción del mensaje ICMPv6 divulgación de vecindario, ver Figura D.34.

ICMPv6: Type: 136 Neighbor Advertisement: El décimal 136, indica el tipo de mensaje ICMPv6 como divulgación de vecindario.

ICMPv6: Code: 0: Tiene una descripción similar a la del mensaje solicitud de vecindario.

ICMPv6: Checksum: 0x2669: Tiene una descripción similar a la del mensaje solicitud de vecindario.

ICMPv6: R Flag: 0

S Flag: 1

Si R tiene un valor distinto de cero, el nodo fuente es un enrutador.

Si S esta a 1 indica que el mensaje se produce como una respuesta a un mensaje de solicitud de vecindario.

ICMPv6: O Flag: 1: Si esta en 1 indica que el mensaje debe actualizar la dirección de la capa de enlace.

ICMPv6: Reserved: 0x0: No se utiliza esta opción, es inicializado a cero por el que envía e ignorado por el que recibe.

ICMPv6: Target Address: 5F15:5000:82C0:E00:BD:A0:246F:B702: Para divulgaciones solicitadas determina la dirección del nodo que incita la creación del mensaje, para divulgaciones no solicitadas se determina la dirección IPv6 de la capa de enlace que por algún motivo a cambiado su dirección.

ICMPv6: Option Type: 2: Determina la dirección de la capa de enlace del nodo que envió el mensaje de divulgación.

ICMPv6: Option lenght: 1 (8bytes): Similar a lo descrito en el mensaje anterior.

ICMPv6: Link Layer Address: 00A0246Fb702: Dirección de la capa de enlace del nodo que envió el mensaje de divulgación.

Descripción del mensaje ICMPv6 respuesta eco.

Para ver la decodificación de este mensaje simplemente se debe bajar un poco la barra vertical visualizando así lo que se muestra en la Figura D.35.

ICMPv6: Type: 129 Echo reply: El valor decimal 129 determina que es un mensaje de respuesta eco surgido por la realización de ping6.

ICMPv6: Code: 0: Similar a lo descrito en los anteriores mensajes ICMPv6.

ICMPv6: Checksum: 0xD0E0: Similar a lo descrito en los anteriores mensajes ICMPv6.

ICMPv6: Identifier: 42752: Este valor es copiado del valor que se encuentra en el mensaje de petición de eco, relacionando los dos mensajes.

ICMPv6: Sequence number: 256: Este valor es copiado del valor que se encuentra en el mensaje de petición de eco, relacionando los dos mensajes.

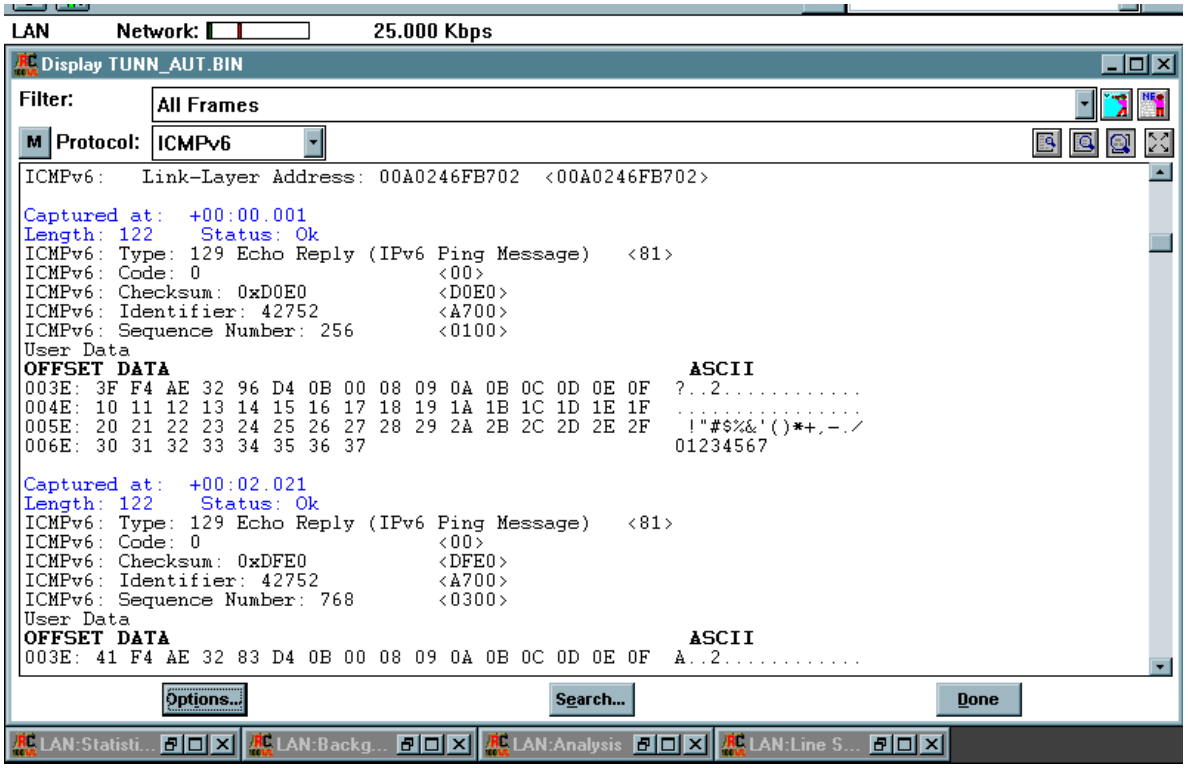

Figura D.35 Mensaje respuesta eco

User data: Los datos de usuario son también copiados del mensaje de solicitud eco. En general, estos datos son un numero determinado de octetos que resultan de un proceso de diagnostico.

D.6.3 Práctica 3: Proceso de análisis para TUNN_AUT.BIN.

Luego de describir tanto el protocolo IPv6 como el protocolo ICMPv6, se va a realizar el proceso que es utilizable en off-line, este proceso el de análisis. Se analizará aspectos como por ejemplo la cantidad y clase de paquetes ICMPv6 que se encuentran en TUNN_AUT

Nota: Se trabaja con el paquete TUNN_AUT, debido a que en las otras prácticas se trabajo sobre todo con túneles automáticos (referirse a este mismo anexo para detallar las otras prácticas).

Realización del proceso análisis para TUNN_AUT.

Para ello se deben tener en cuenta los siguientes pasos:

- Visualizar en la ventana del analizador la trama IPv6 como se indica en la Figura D.33.
- Hacer click en el botón OPTIONS.
- De la ventana desplegada hacer click en el botón PREFERENCES.
- Señalar la opción multiprotocol y dar click en ok.
- Se observará lo mostrado por la Figura D.36.

Esta aproximación mostrada en la figura 26, es la que se asemeja más a una transmisión real, ya que por lo general en la cabecera IPv6 se llama un paquete ICMPv6.

Para realizar el análisis de cuantos y cuales paquetes ICMPv6 intervienen en TUNN_AUT se deben tener en cuenta los siguientes pasos:

- Dar click en el botón OPTIONS.
- De la ventana desplegada dar click en ANALYSIS.
- De la ventana desplegada, en la opción SUBJECT, escoger ICMPv6.
- Dar click en ok.

La distribución de mensajes ICMPv6 es como se muestra en la Figura D.37.

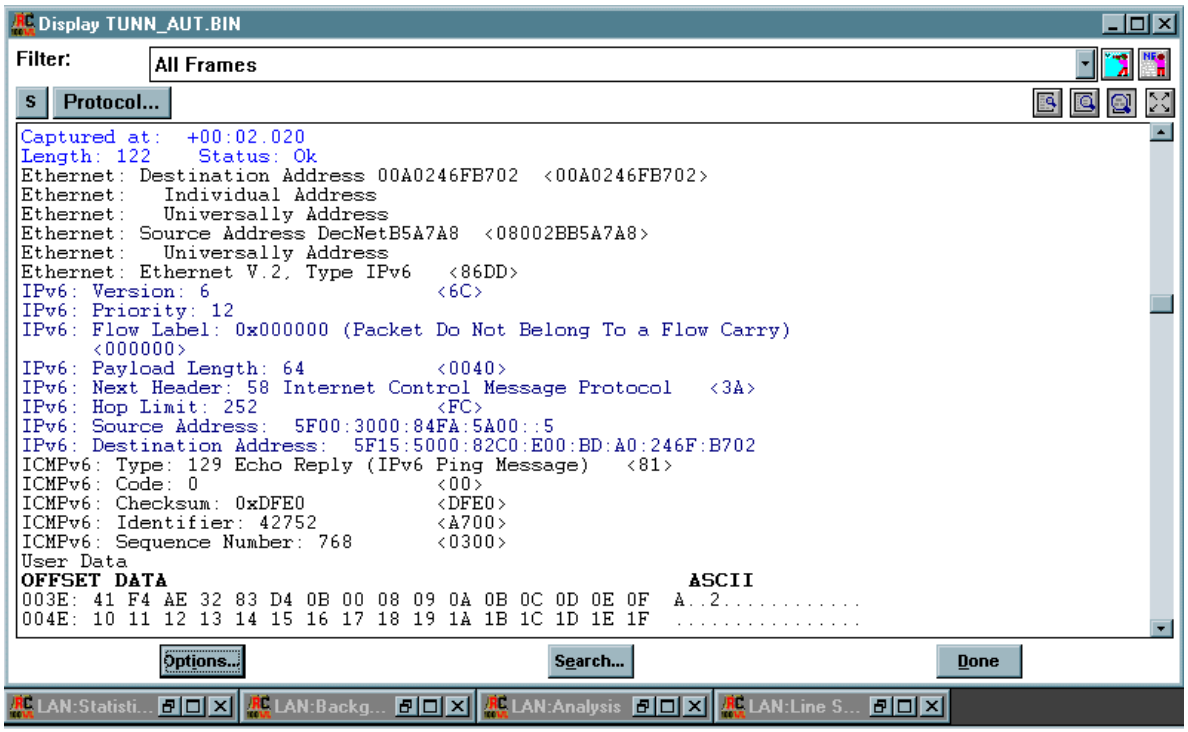

Figura D.36 Tramas IPv6 e ICMPv6 intercaladas

Se pueden realizar otro tipo de análisis, como por ejemplo la distribución de tráfico por dirección de destino, para hacer ello se tienen en cuenta los siguientes pasos:

- Dar click en OPTIONS.
- De la ventana desplegada dar click en ANALYSIS.
- En subject escojer ethernet.
- En analisis escoger Traffic distribution by destination address.

Se verá lo mostrado por la Figura D.38.

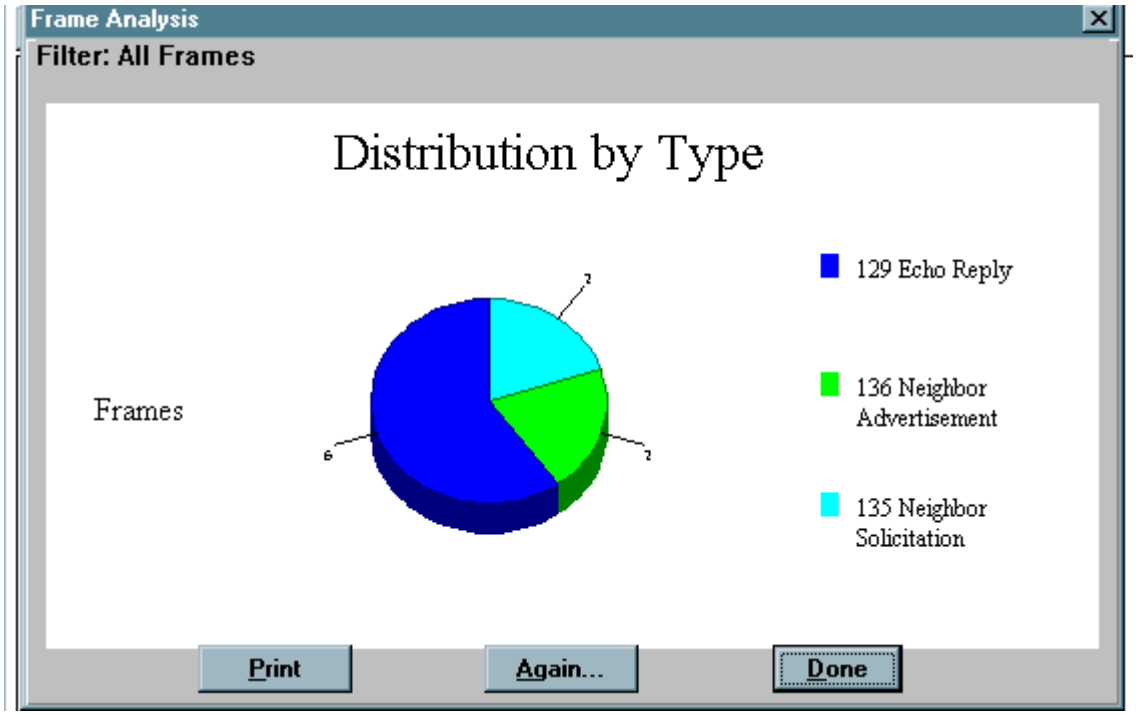

Figura D.37 Distribución de mensajes ICMPv6 en TUNN_AUT

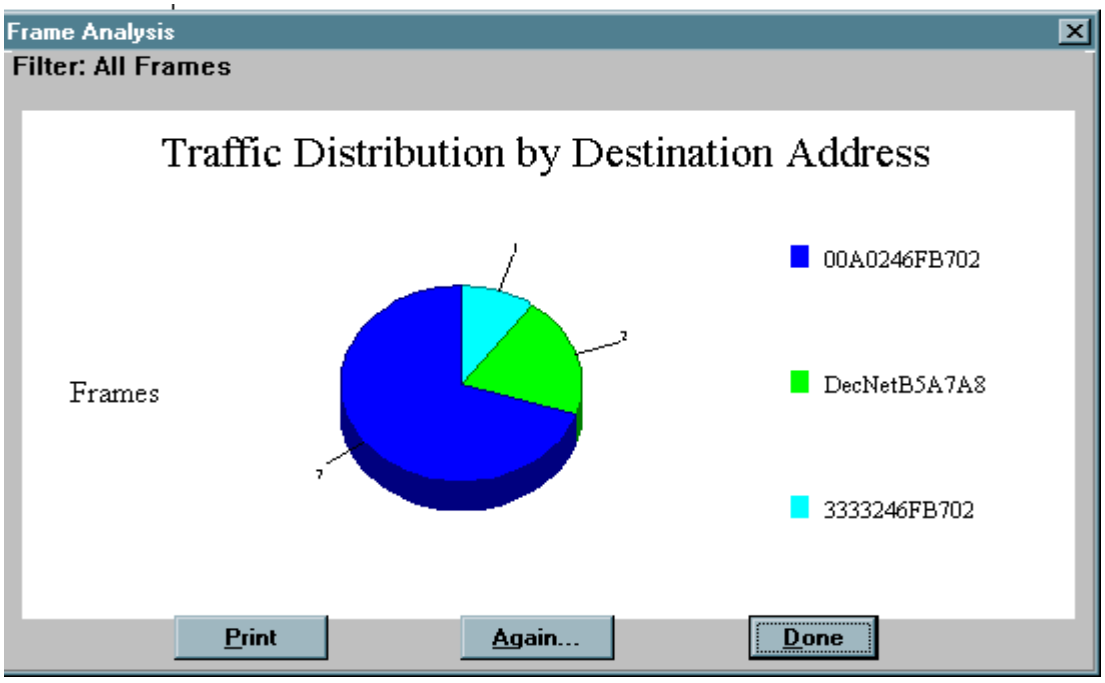

Figura D.38 Distribución de tráfico por dirección de destino

Estos son algunos ejemplos de análisis al paquete TUNN_AUT.