UNIVERSIDAD CENTRAL "MARTA ABREU" DE LAS VILLAS
VERITATE SOLA NOBIS IMPONETUR VIRILIS TOGA. 1948

FACULTAD DE INGENIERÍA ELÉCTRICA

Departamento de Electrónica y Telecomunicaciones

Trabajo de Diploma

"Prácticas de laboratorio virtual sobre configuración de direcciones IPv6"

Autora: Yailin Carvajal Benavides

Tutor: Ing. Jorge Luis Obregón Hernández

Santa Clara

2014

"Año 56 de la Revolución"

Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Electrónica y Telecomunicaciones

TRABAJO DE DIPLOMA

“Prácticas de laboratorio virtual sobre configuración de direcciones IPv6”

Autor: Yailin Carvajal Benavides.
E-mail: cbenavidez@uclv.edu.cu

Tutor: Ing. Jorge Luis Obregón Hernández
E-mail: jorge_luis@uclv.edu.cu

Santa Clara

2014

“Año 56 de la Revolución”

Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Telecomunicaciones y Electrónica, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____ _____

Firma del Tutor

Firma del Jefe de Departamento donde se defiende el trabajo

_____

Firma del Responsable de Información Científico-Técnica

PENSAMIENTO

“A las estrellas no se sube por caminos llanos.”

José Martí.

DEDICATORIA

A mi madre, mayor regalo que existe en mi corazón.

A mi padre, fuente de energía y fe que me ayuda a levantar cuando me siento abatida.

A mi hermana, ardiente luz que mantiene relucida siempre mi vida.

A mi gran amiga la Dra. Estrella Rodríguez Luna, más que estrella, bello arco iris que dió colorido a mis días.

A mi abuela, brillante estrella a seguir.

A mi novio, lindo sendero que se abrió cuando me sentía sola y me daba miedo avanzar.

AGRADECIMIENTOS

A Dios por permitirme llegar hasta aquí.

A toda mi familia por su apoyo, en especial:

A mi madre por su agnegación incansable.

A mi padre por darme la alegría de existir.

A mi hermana por ser mi fuente de inspiración .

A mi abuela por estar siempre ahí.

A mi novio por su amor y comprensión.

A mi tía Mery por confiar en mi.

A mis suegros por su cariño y preocupación.

A mis segundos papás Osmany y Juanka por apoyarme.

A mi médico el Dr. Bárbaro por su esfuerzo y ayuda.

A mi gran amiga la Dra. Estrella Rodríguez Luna por permitirme ser quien soy.

A mis grandes amistades Anabel, Aylin, Olguita, por darme fuerzas para seguir.

Al maravilloso claustro de profesores de la FIE por su buena preparación profesional y humana, la que me permitió llegar hasta aquí, en especial a mi tutor Jorge Luis Obregón por su apoyo y dedicación.

A los compañeros de aula que durante estos 6 años han sido una gran familia para mí y a los cuales quiero muchísimo, en especial: a Ernesto, Dany, Miguel, Yaima, Zaily, César, Asiel, José Luis, Andy, Yasmany, Dariel.

En fin, agradezco a todo el que de una manera u otra hizo lo más mínimo para que este sueño se hiciera realidad.

TAREA TÉCNICA

Con el propósito de dar cumplimiento a los objetivos trazados para la realización de este trabajo, se tomaron en cuenta las siguientes tareas técnicas para la confección del informe final.

1. La realización de una revisión bibliográfica acerca de los aspectos fundamentales que describen el funcionamiento básico de IPv6, ICMPv6 y las técnicas de configuración de direcciones IPv6.
2. La determinación de los rasgos o características que intervienen en la implementación de las técnicas de configuración de direcciones IPv6.
3. La realización de un análisis detallado de los elementos fundamentales que se deben tener en cuenta para el desarrollo de las prácticas de laboratorio virtual.
4. La implementación en las diferentes herramientas virtuales, de cada uno de los escenarios de red a utilizar en las prácticas de laboratorio virtual y de los elementos que conforman dichos escenarios de red.
5. La elaboración del informe final.

Firma del Autor

Firma del Tutor

RESUMEN

El explosivo despliegue de Internet en conjunto con el enorme crecimiento de usuarios, originó que el espacio de direcciones IPv4 sea insuficiente para cubrir toda la demanda, lo que ha conllevado a la implementación de un nuevo protocolo denominado IPv6, con un espacio de direccionamiento mucho mayor que solventa las deficiencias de IPv4. El desafío que se impone con la implementación de IPv6 y la preparación de los especialistas en el tema, hacen que se justifique el estudio sobre el mismo.

En este trabajo se desarrollan prácticas de laboratorio virtual sobre las diferentes técnicas de configuración de direcciones IPv6 utilizando las herramientas virtuales GNS3, VirtualBox y Wireshark. Primeramente se realiza la descripción de los elementos fundamentales en el funcionamiento básico de IPv6 e ICMPv6, se destacan además los aspectos esenciales sobre las técnicas de configuración de direcciones IPv6. Posteriormente se describen las prácticas y los escenarios de red referentes a cada práctica, así como las potencialidades de las herramientas virtuales a utilizar, y por último se fundamenta la estructura seguida referente a los documentos guías de cada una de las prácticas.

Se demuestra la importancia que posee el desarrollo de prácticas de laboratorio virtual utilizando diferentes herramientas virtuales en temas relacionados a las técnicas de configuración de direcciones IPv6.

TABLA DE CONTENIDOS

INTRODUCCIÓN

El surgimiento del protocolo de red llamado Protocolo de Internet (***Internet Protocol,* IP**) versión 4 (***Internet Protocol version 4,* IPv4**) (Postel, 1981, Touch, 2013) en los años 70, fue un suceso que conmovió al mundo de las comunicaciones. Con un inmenso espacio de direcciones para ese tiempo (32 bits), ofrecía más de 4 mil millones de posibles direcciones IPv4, lo cual representó un éxito para sus creadores que imaginaron rebasar el número de direcciones necesarias para el acceso de los usuarios.

El explosivo despliegue de Internet en conjunto con el enorme crecimiento de usuarios, específicamente usuarios de tecnologías inalámbricas, originó que el espacio de direcciones IPv4 sea insuficientemente para cubrir toda la demanda, a tal punto que ya el último lote de direcciones IPv4 fue vendido por La Autoridad de Números Asignados de Internet (***Internet Assigned Numbers Authority,* IANA**) (IANA, 2014) aspecto que los creadores de IPv4 no previeron y que ha dado paso en conjunto con otras deficiencias presentes en IPv4 a la utilización de una nueva versión del protocolo IP (***Internet Protocol version 6,* IPv6**) (Deering and Hinden, 1998, Gont and Manral, 2014).

Esta nueva variante del protocolo IP, IPV6, no llegó con el objetivo de sustituir o desplazar de primer momento a la versión que le antecedía, sino para actuar de conjunto e integración, evolucionando cada vez más las redes de comunicación global. Por ello se hace necesario profundizar en el tema para afrontar el reto que impone el desarrollo de este nuevo protocolo, preparando a los estudiantes que se formarán como futuros profesionales en telecomunicaciones para que puedan dar respuesta acertada a las múltiples interrogantes y situaciones que pueda traer consigo la implementación de IPv6.

Teniendo en cuenta las grandes ventajas que ofrece IPv6, su pobre desarrollo en Cuba, aun cuando algunos profesionales en la rama de las telecomunicaciones se hayan interesado en

el tema; y sumando a ello, que el entendimiento del funcionamiento de dicho protocolo posee un alto grado de dificultad, hacen que se haga necesario profundizar en su estudio, desarrollando materiales que apoyen en la docencia a los estudiantes de la carrera de Telecomunicaciones y Electrónica en la Universidad Central ¨Marta Abreu¨ de Las Villas (**UCLV**), futuros profesionales encargados de contribuir al mejoramiento de las redes en Cuba. De ahí que surja la necesidad de preguntarse:

- ¿Cómo desarrollar prácticas de laboratorio virtual sobre las técnicas de configuración de direcciones IPv6 utilizando herramientas virtuales?

Para dar respuesta a esta interrogante científica se traza el siguiente objetivo general:

- Desarrollar prácticas de laboratorio virtual sobre las técnicas de configuración de direcciones IPv6 utilizando herramientas virtuales.

Para dar curso a este trabajo se trazan las siguientes interrogantes científicas:

- ¿Qué aspectos se deben tener en cuenta para enfocar el estudio sobre la configuración básica IPv6?
- ¿Cuáles son los temas fundamentales a tener en cuenta para el desarrollo de las prácticas de laboratorio virtual referentes a las técnicas de configuración de direcciones IPv6?
- ¿Qué características permiten fundamentar la selección de las herramientas virtuales?
- ¿Cuáles son los elementos fundamentales desde el punto de vista pedagógico a tener en cuenta para el desarrollo de las prácticas de laboratorio virtual referentes a las técnicas de configuración de direcciones IPv6?
- ¿Cómo llevar a cabo el desarrollo de las prácticas de laboratorio virtual?

A las que se les da respuesta con los siguientes objetivos específicos:

- Realizar un estudio teórico para profundizar sobre el principio de funcionamiento básico de IPv6 y sobre el estado actual de las investigaciones en este campo.
- Fundamentar los principales aspectos que describen las diferentes técnicas de configuración de direcciones IPv6, para enfocar el desarrollo de las prácticas de laboratorio virtual.
- Abordar los temas a desarrollar en las prácticas.

- Profundizar sobre las potencialidades de las herramientas virtuales escogidas para el desarrollo de las prácticas de laboratorio virtual, haciendo énfasis en la herramienta de simulación de red.
- Desarrollar las prácticas correspondientes en función de la selección realizada.
- Fundamentar los elementos esenciales que se deben tener en cuenta para el desarrollo de prácticas de laboratorio virtual, desde el punto de vista pedagógico.

Con la culminación de este trabajo se pondrá a disposición de los especialistas, estudiantes y profesores de la Facultad de Ingeniería Eléctrica de la UCLV, un material de consulta que servirá de apoyo para el buen entendimiento del protocolo de red IPv6, desarrollando habilidades en la configuración de los diferentes dispositivos de red cuando es IPv6 el protocolo de red utilizado.

Organización del Informe

Como estrategia para alcanzar los objetivos planteados el informe de la investigación se estructurará en introducción, capitulario, conclusiones, referencias bibliográficas y glosario de términos.

- Introducción, en la cual se define la importancia, actualidad y necesidad del tema que se aborda y donde se deja explícito los elementos del diseño teórico.
- Primer capítulo, el cual se dedica a tratar los principios básicos sobre el funcionamiento de IPv6, ICMPv6 y de las técnicas de configuración de direcciones IPv6.
- Segundo capítulo, el cual se dedica a recrear los fundamentos que validan la construcción de los escenarios desarrollados en las prácticas de laboratorio virtual y a analizar las potencialidades de las herramientas virtuales a utilizar, enfatizando en la herramienta de simulación de red escogida.
- Tercer capítulo, el cual se dedica al análisis de la estructura de los documentos guías referentes a cada una de las prácticas de laboratorio virtual desarrolladas.
- Conclusiones, donde se exponen las consideraciones finales sobre la problemática investigada.
- Recomendaciones, que solicitan la profundización y ampliación de los estudios sobre la temática.

- Referencias Bibliográficas, que dan origen y validan a la conformación del cuerpo investigativo.
- Glosario de Términos.

CAPÍTULO 1. CONFIGURACIÓN DE DIRECCIONES IPV6

El siguiente capítulo se dedica a tratar los elementos que describen el funcionamiento básico de IPv6 y de las técnicas de configuración de direcciones IPv6, con el objetivo de destacar aspectos que son vitales para el buen desarrollo de las prácticas de laboratorio virtual.

1.1 IPv6

IPv6 o también conocido como IPng (***Next Generation Internet Protocol***) es un protocolo diseñado por la IETF (***Internet Engineering Task Force***) (IETF, 2014). Este estándar se desarrolló para trabajar en el nivel de red, donde tiene la responsabilidad de dirigir y encaminar los paquetes a través de la red, además está destinado a reemplazar de forma gradual a IPv4 cuyo límite de direcciones IP admisibles restringe el crecimiento de Internet. (Deering and Hinden, 1998, Gont and Manral, 2014).

1.1.1 Formato de las direcciones IPv6

Las direcciones IPv6 son representadas como 8 grupos de 16 bits separadas por el carácter dos puntos (:), donde cada grupo se representa por cuatro dígitos hexadecimales, tal como se muestra en el siguiente ejemplo:

3223:0BA0:01E0:D001:0000:0000:D0F0:0010

Existen varias formas convencionales que pueden utilizarse para representar las direcciones IPv6. Ver (Kawamura and Kawashima, 2010).

1.2 Tipos de direcciones

Las direcciones IPv6 están formadas por dos partes esenciales al igual que las direcciones IPv4, los bits de la parte superior pertenecen al prefijo de red que se encarga de identificar la red de la que forma parte dicha dirección y los bits de la parte inferior están encargados de identificar la interfaz dentro de la red. El tamaño de ambas partes es variable, en consecuencia del tipo de dirección y sus características. Ver Figura 1.1.

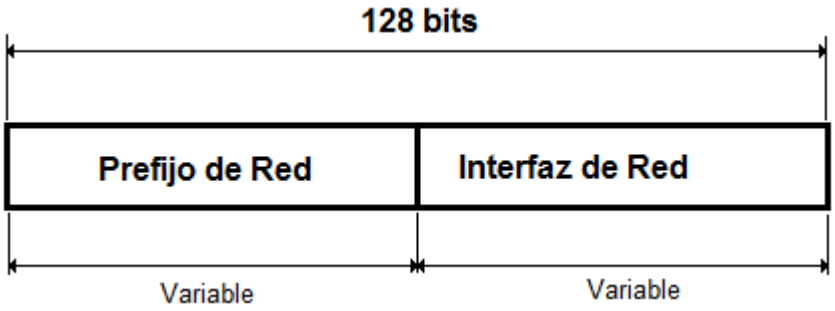


Figura 1.1 Estructura general de una dirección IPv6.

A la interfaz de un nodo se le puede asignar múltiples direcciones IPv6. Los bits iniciales de la dirección definen el tipo de dirección IPv6 específica. Existen tres grupos fundamentales de direcciones IPv6 (Headquarters, 2012b, Deering and Hinden, 2006, Jiang and Carpenter, 2014) los cuales se muestran a continuación:

- ***Unicast:*** Se usa para identificar a una simple interfaz. Un paquete enviado a una dirección Unicast es entregado a la interfaz identificada por la dirección.
- ***Anycast:*** Es un identificador para un conjunto de interfaces (típicamente pertenecientes a diferentes nodos). Un paquete enviado a una dirección Anycast es entregado a la interfaz más cercana acorde a los protocolos de enrutamiento que se implementen.
- ***Multicast:*** Se utiliza como identificador de un conjunto de interfaces, típicamente pertenecientes a diferentes nodos. Un paquete enviado a una dirección Multicast es entregado a todas las interfaces identificadas por la dirección.

Se debe señalar que IPv6 no implementa ***broadcast*** como hace IPv4. El mismo efecto puede lograrse enviando un paquete al grupo Multicast de enlace local. (Deering and Hinden, 1998).

Toda interfaz requiere tener al menos una dirección Local de Enlace Única (***Link Local Unicast Address***). Mientras que una simple interfaz puede tener múltiples direcciones IPv6 de cualquier tipo (***Unicast, Anycast y Multicast***).

Para la identificación del tipo de direcciones IPv6 se utilizan los 8 bits más significativos de la dirección. Tabla 1.1.

Es importante destacar que las direcciones Anycast son tomadas del espacio de direcciones Unicast (de cualquier alcance) y no son distinguibles sintácticamente.

Tabla 1.1 Tipos de direcciones IPv6

Tipo de Dirección	Prefijo Binario	Notación IPv6	Observación
No especificada	000.....0	: : /128	128 bits a "0", no es asignada a ningún nodo.
Loopback	000.....1	: : 1/128	Un nodo IPV6 envía un paquete a si mismo. No es asignada a ningún nodo.
Multicast	11111111	FF00::/8	
Link Local Unicast	11111010	FE80::/10	
Global Unicast	Todas las demás		

1.2.1 Dirección Unicast

Una dirección IPv6 Unicast identifica una simple interfaz. Cuando una interfaz pertenece a un solo nodo, la dirección puede ser utilizada además para identificar al nodo.

Son agregadas con prefijos de cualquier longitud. A continuación se especifican algunos de los diferentes tipos de dirección Unicast:

- Global Agregable.
- Enlace Local.
- Local Única.

➢ **Dirección Unicast Global Agregable**

Una dirección Unicast Global Agregable es aquella que se crea a partir de un prefijo Unicast Global Agregable. La estructura de una dirección Unicast Global Agregable habilita la agregación estricta de prefijos de enrutamiento que limitan el número de entradas

en la tabla de rutas global. Estas direcciones son usadas en enlaces que están ubicados hacia una organización superior o de mayor jerarquía y eventualmente para proveedores de servicio de Internet (***Internet Service Provider,* ISP**). (Headquarters, 2012b, Deering and Hinden, 2006, Jiang and Carpenter, 2014).

Las direcciones Unicast Globales Agregables IPv6 son definidas por un prefijo global de enrutamiento, un identificador de subred y un identificador de interfaz. Excepto para direcciones que comienzan con el código binario 000, todas las direcciones Unicast Globales Agregables tienen 64 bits de identificador de interfaz. Las direcciones Unicast Globales Agregables IPv6 asignadas usan el rango de direcciones que inician con el código binario 001, ejemplo: 2000::/3. La Figura 1.2 muestra la estructura de una dirección Unicast Global Agregable.

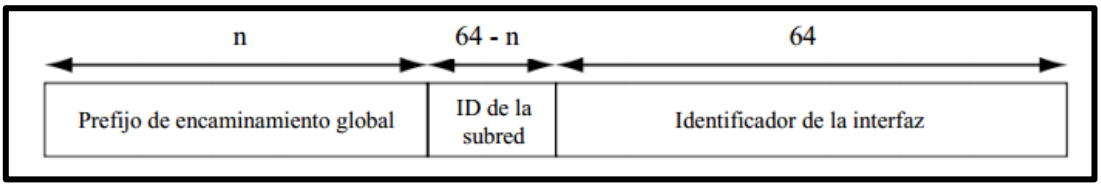


Figura 1.2 Estructura de una dirección Unicast Global Agregable.

Las direcciones con un prefijo de 2000::/ 3 (001) a través de E000::/ 3 (111) son requeridas para tener identificadores de interfaz de 64 bits en el formato de identificador universal extendido (***Extended Universal Identifier,* EUI-64**) (Deering and Hinden, 2006, Jiang and Carpenter, 2014). La IANA asigna el espacio de direccionamiento IPv6 en el rango de 2000:/ 16 a registros regionales.

Además constituyen la parte fundamental de la estructura de direccionamiento IPv6, lo que permite una agregación estricta de prefijos de enrutamiento para limitar el tamaño de la tabla de enrutamiento global de Internet.

- **Dirección Unicast de Enlace Local**

Las direcciones Unicast de Enlace Local son utilizadas sobre enlaces locales y las mismas tienen el siguiente formato: los primeros 10 bits son representados por el siguiente código binario ¨1111111010¨, los siguientes 54 bits se fijan a ¨0¨ y por último los 64 bits restantes se utilizan para identificar la interfaz. Figura 1.3.

Estas direcciones son designadas para ser utilizadas sobre un simple enlace con propósitos tales como la configuración automática de direcciones, descubrimiento de vecinos, cuando no hay Routers presentes o simplemente para comunicarse entre estaciones en el enlace perteneciente a la misma red IPv6. (Headquarters, 2012b, Deering and Hinden, 2006, Jiang and Carpenter, 2014).

El tráfico que utiliza estas direcciones posee un alcance local en el enlace, los Routers IPv6 no conducen tráfico de enlace local más allá del enlace. Una dirección de Enlace Local es utilizada para descubrir vecinos y este proceso es configurado automáticamente aún en la ausencia de todas las otras direcciones.

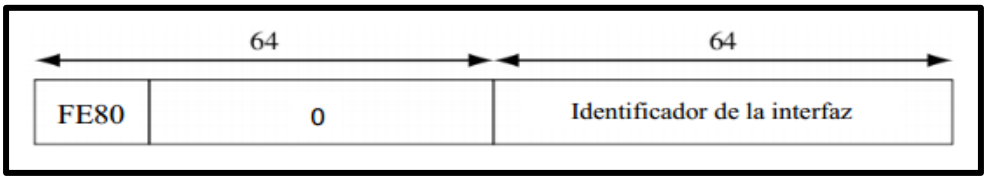


Figura 1.3 Dirección Unicast de Enlace Local

- **Dirección Unicast compatible con IPv4**

Una dirección Unicast IPv6 compatible con IPv4 es una dirección IPv6 que tiene ceros en los 96 bits superiores de la dirección y una dirección IPv4 en los 32 bits de la parte baja de la dirección. La Figura 1.4 muestra la estructura de una dirección Unicast IPv6 compatible con IPv4. (Headquarters, 2012b, Deering and Hinden, 2006, Jiang and Carpenter, 2014).

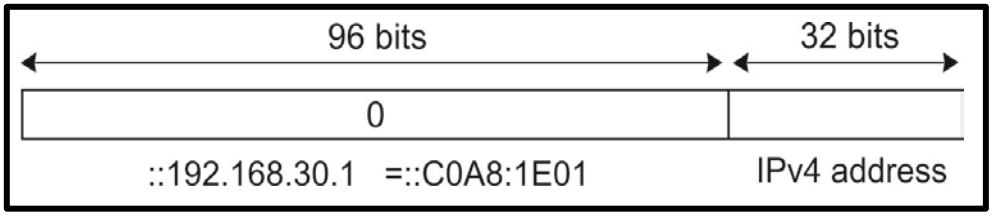


*Figura 1.4 Estructura de una dirección Unicast **IPv6** compatible con **IPv4***

- **Dirección Unicast Local Única**

Una dirección Unicast Local Única es una dirección que es única globalmente y que está prevista para comunicación local. Es poco probable que se enruten hacia la Internet Global, o sea, solo se enrutan en un área limitada, como por ejemplo: un sitio. También pueden ser enrutadas entre un conjunto limitado de sitios. La Figura 1.5 muestra la

estructura de una dirección Unicast Local Única. (Headquarters, 2012b, Deering and Hinden, 2006, Jiang and Carpenter, 2014).

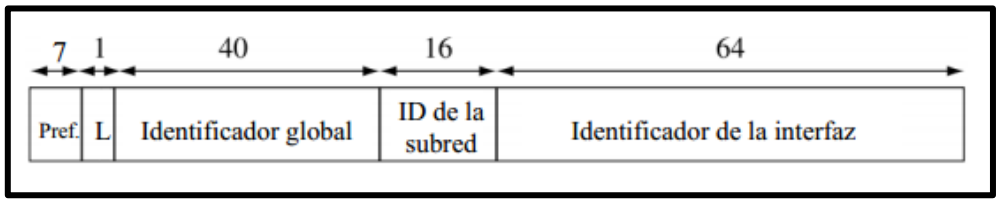


Figura 1.5 Estructura de una dirección Unicast Local Única

1.2.2 Dirección Anycast

Las direcciones Anycast se diferencian de las direcciones Multicast en que el paquete enviado a una dirección Anycast no es entregado a todos los miembros del grupo, sino que el paquete es enrutado hacia la interfaz más cercana que tenga esa dirección, acorde con los protocolos de enrutamiento que calculan distancia. (Headquarters, 2012b, Deering and Hinden, 2006, Jiang and Carpenter, 2014).

Un uso esperado de las direcciones Anycast es el de identificar un conjunto de Routers pertenecientes a una organización que ofrece servicios de Internet. Tales direcciones pueden ser utilizadas como direcciones intermedias en el encabezado de un enrutamiento IPv6. El encabezado de enrutamiento ocasionará que un paquete sea entregado mediante una vía particular al proveedor de servicio o a una secuencia de proveedores de servicio.

Otro posible uso está en identificar un conjunto de Routers conectados a una subred particular, o al conjunto de Routers que ofrecen acceso a un dominio de enrutamiento particular.

La dirección Anycast de Router-Subred es predefinida y su formato es mostrado en la Figura 1.6.

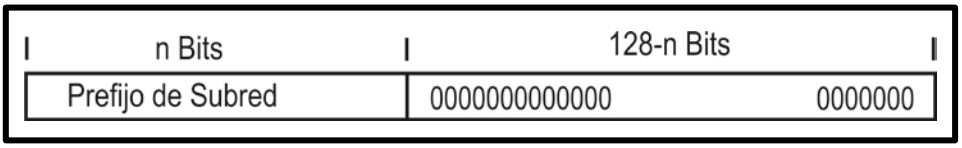


Figura 1.6 Estructura de la Dirección Anycast de subred para un Router.

En la Figura 1.6 se muestra la estructura de la dirección Anycast de subred para un Router; la dirección tiene un prefijo concatenado por una serie de ceros (el identificador de

interfaz). La dirección de subred del Router Anycast puede usarse para alcanzar un Router en el enlace que es identificado por el prefijo en la dirección de subred del Router Anycast.

El formato de este tipo de direcciones es muy sencillo debido a que toda la carga se centra en el sistema de encaminamiento. De esta forma, para cada Router debe guardar un solo registro que le indica cual es el miembro más cercano al del grupo especificado, y al recibir un paquete con una dirección de destino Anycast comprobar la existencia de este registro especial en su tabla de encaminamiento o encaminar normalmente el paquete.

Las direcciones Anycast poseen una serie de restricciones, las cuales se muestran a continuación:

- Una dirección Anycast no puede ser utilizada como dirección origen de un paquete IPv6.
- Una dirección Anycast no debe ser asignada a un host IPv6, es decir, sólo puede ser asignada a un Router IPv6.

Las direcciones Anycast agrupan las siguientes direcciones ya definidas en Unicast:

- Dirección Agregable Global.
- Dirección Local Única.
- Dirección Enlace Local.

1.2.3 Dirección Multicast

Una dirección Multicast es una dirección creada para identificar a un grupo de interfaces que típicamente pertenecen a nodos diferentes, tiene un prefijo FF00::/ 8 (1111 1111). Un paquete enviado a una dirección Multicast es entregado a todas las interfaces identificadas por la dirección Multicast. El segundo octeto siguiendo el prefijo define el tiempo de vida y el alcance de la dirección Multicast. La Figura 1.7 muestra el formato de las direcciones Multicast. (Headquarters, 2012b, Deering and Hinden, 2006, Jiang and Carpenter, 2014).

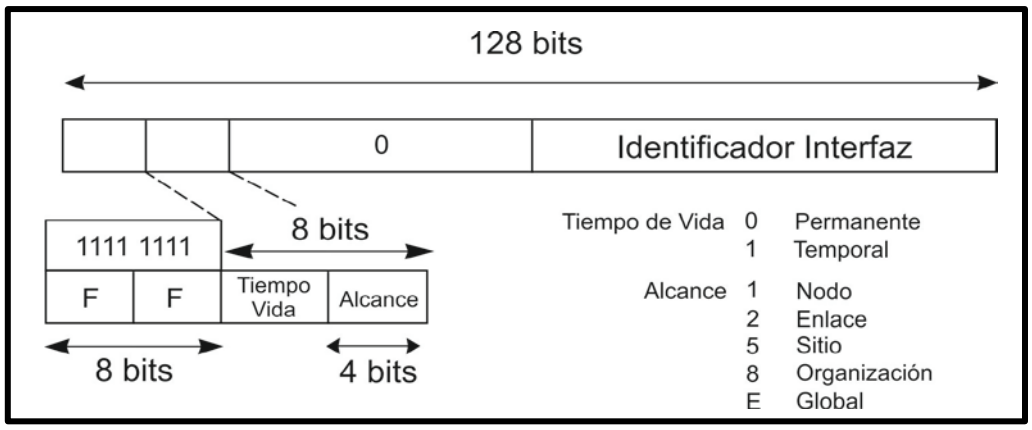


Figura 1.7 Estructura general de las direcciones Multicast.

La Tabla 1.2 muestra las diferentes tipos de direcciones Multicast.

Tabla 1.2 Direcciones Multicast comúnmente utilizadas.

Dirección	Significado
FF01::1	Todas las direcciones en un Nodo
FF02::1	Todas las direcciones sobre un Enlace
FF01::2	Todas las direcciones de Routers sobre el Nodo
FF02::2	Todos los Routers sobre el Enlace
FF05::2	Todos los Routers en la Organización

La estructura referente a cada uno de estos tipos de direcciones se puede ver con más detalle en (Headquarters, 2012b, Deering and Hinden, 2006, Jiang and Carpenter, 2014).

1.2.4 Otras direcciones

- **Dirección Loopback**

Se define como 15 bytes nulos y un byte con el último bit a 1 (0:0:0:0:0:0:0:1). Esta dirección es interna y de ninguna forma puede circular por la red o ser dirección de origen o destino de un paquete. Su utilidad viene dada para los ordenadores que no dispongan de una conexión de red y deseen simular el comportamiento de conexión a una red mediante una dirección fantasma que nunca saldrá del propio ordenador. (Headquarters, 2012b, Deering and Hinden, 2006, Jiang and Carpenter, 2014).

- **Dirección Sin Especificar (*Unspecified Address*)**

Está compuesta por 16 bytes nulos (0:0:0:0:0:0:0:0) y puede representarse como ::, representa una dirección no especificada, tal como 0.0.0.0 era en IPv4. Sólo puede utilizarse como dirección inicial mientras se inicializa y se recibe una dirección fija. También puede utilizarse para funciones internas que requieran la especificación de una dirección IP. (Headquarters, 2012b, Deering and Hinden, 2006, Jiang and Carpenter, 2014).

1.3 Técnicas de configuración de direcciones IPv6

En el entorno IPv6 existen diferentes técnicas de configurar direcciones IP a una interfaz, las cuales se mencionan a continuación:

- Configuración estática
- Configuración dinámica
    - SLAAC ***(Stateless Address Autoconfiguration).*** (Headquarters, 2012b, Narten et al., 2007).
    - Configuración sin estado utilizando un servidor DHCPv6 (***Dynamic Host Configuration Protocol for IPv6***). (Droms et al., 2003, Droms, 2004, Headquarters, 2012a, Krishnan et al., 2014).
    - Configuración con estado utilizando un servidor DHCPv6. (Droms et al., 2003, Headquarters, 2012a, Volz and Troan, 2013, Krishnan et al., 2014).

1.3.1 Configuración estática

Como en IPv4, las direcciones IPv6 de las interfaces de red pueden ser definidas estáticamente. En este caso la dirección IPv6, el prefijo de red y la dirección del Gateway son todas definidas estáticamente en el Host.

La configuración estática se usa típicamente para la configuración de la interfaz de un Router o de un servidor, pero no es común usarlo en Host IPv6, usar configuración estática es desaprovechar todos los beneficios suministrados por IPv6.

1.3.2 Configuración Dinámica

- **SLAAC**

Los nodos pueden usar SLAAC para generar direcciones sin la necesidad de un servidor DHCPv6.

El mecanismo SLAAC es desarrollado en el protocolo IPv6 para facilitar la administración de Internet. Admite un gran número de Hosts IP, los cuales poseen soporte para protocolos relacionados al descubrimiento de redes y que reciben direcciones IPv6 globalmente únicas asociadas con su localización. Facilita además el despliegue de nuevos dispositivos en Internet, como pueden ser: dispositivos inalámbricos, equipos electrodomésticos, etc. Como consecuencia, los dispositivos de la red pueden conectarse sin la necesidad de configuración estática y de servidores DHCPv6.

Un Host puede construir su dirección IPv6 a partir de un prefijo de red de 64 bits recibidos desde el Router a través de un mensaje de advertencia de Router (***Router Advertisement,* RA**) (Headquarters, 2012b, Moore, 2006). Como consecuencia, el Host se crea su dirección IPv6 a partir de la información obtenida desde el Router y de la autoconfiguración de su identificador de Host. El identificador de Host se puede crear a partir de su dirección MAC (***Media Access Control***) aplicando el mecanismo EUI-64 extendido o aleatoriamente.

En SLAAC, el papel fundamental lo juega el Router de la red. El Router es el encargado de anunciar en la red el prefijo a usar mediante un mensaje RA, dichos mensajes se retransmiten periódicamente o en respuesta a un mensaje de solicitud de Router (***Router Solicitation,* RS**) (Headquarters, 2012b, Moore, 2006).

- **Configuración sin estado utilizando un servidor DHCPv6**

La configuración de direcciones IPv6 sin estado utilizando un servidor DHCPv6, normalmente combina SLAAC para la asignación de direcciones con el intercambio DHCPv6 para todas las demás configuraciones. En este caso, DHCPv6 es usado sólo para que el Host adquiera parámetros adicionales de configuración, como la dirección IPv6 de servidores de nombre de dominio, de transferencia de fichero, etc.

El Host autoconfigura su dirección IPv6 mediante el proceso EUI-64 extendido o aleatoriamente y luego envía un mensaje DHCPv6 solicitando al servidor DHCPv6 el resto de los parámetros de configuración.

- **Configuración con estado utilizando un servidor DHCPv6**

Muchas empresas actualmente utilizan DHCP para distribuir direcciones IP a sus Hosts. IPv6 también puede ser desplegado utilizando el mecanismo DHCPv6.

El proceso de adquirir los datos de configuración para un cliente en IPv6 es similar a IPv4. Sin embargo, DHCPv6 usa Multicast para muchos de sus mensajes. Inicialmente, el cliente debe detectar la presencia de Routers en el enlace utilizando el protocolo de descubrimiento de vecinos (***Neighbor Discovery,* ND**) (Headquarters, 2012b, Moore, 2006). Si un Router es encontrado, el cliente examina los mensajes del Router para determinar si DHCPv6 debería ser usado. Para que el Router permita el uso de DHCPv6 en ese enlace debe estar desactivada la bandera autoconfiguración y habilitada la bandera de administración en el mensaje RA, dejando así que el Host pueda utilizar DHCPv6 para obtener una dirección IPv6, luego el cliente inicia una fase de solicitud DHCPv6 para encontrar un servidor DHCPv6.

Usar DHCPv6 genera los siguientes beneficios:

- Provee un mayor control sobre la asignación de direcciones IPv6.
- Puede ser usado simultáneamente con SLAAC.
- Puede usarse para reenumerar.
- Puede usarse para registrar nombres de dominio automáticos (***Domain Name System,* DNS**) utilizando DNS dinámico.
- Puede utilizarse para delegar el prefijo IPv6 a las tablas de enrutamiento del equipo de premisa del cliente (***Client Premise Equipment,* CPE*).***

El propósito de DHCPv6 es el mismo que DHCPv4: asignar una dirección IPv6 a un equipo de red. Una diferencia importante está en que la dirección del Router que funciona como puerta de enlace predeterminada que se incluye en DHCPv4, en DHCPv6 no se incluye, el Router por defecto de la red se anuncia utilizando mensajes RA originados por el propio Router.

1.4 ICMPv6

El protocolo de mensaje de control de Internet para IPv6 (***Internet Control Message Protocol version 6,* ICMPv6**) (Conta and Gupta, 2006, Bonica et al., 2007, Headquarters, 2012b, Carrell, 2013), funciona de igual manera que la variante creada para IPv4 (***Internet Control Message Protocol,* ICMP**) (Conta and Gupta, 2006, Bonica et al., 2007, Headquarters, 2012b, Carrell, 2013). ICMPv6 genera mensajes de error, como pueden ser: mensajes de destinos inalcanzables; y mensajes informativos, como pueden ser: mensajes de solicitud de eco y mensajes de respuesta a la solicitud de eco. Adicionalmente, los paquetes ICMPv6 son usados en el proceso de ND, descubrimiento de máxima unidad de transferencia de paquetes **(*Maximun Transmition Unit,* MTU**) (McCann et al., 1996) mínima para un camino determinado, y otros protocolos como MLD (***Multicast Listener Discovery***) (Vida et al., 2004, Asaeda, 2013), siendo este último un protocolo utilizado por los Routers IPv6 para descubrir nodos que quieren recibir paquetes Multicast destinados a direcciones Multicast específicas.

La Figura 1.8 muestra el formato de mensaje ICMPv6. Los campos referentes al encabezado del mensaje ICMPv6 se explican con más detalle en (Conta and Gupta, 2006, Bonica et al., 2007, Headquarters, 2012b, Carrell, 2013).

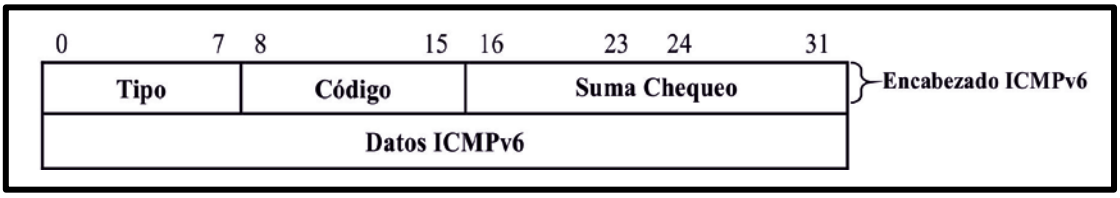


Fig. 1.8 Formato del ICMP versión 2 compatible con la versión 6 de IP.

La Tabla 1.3 muestra un resumen de los mensajes ICMPv6 más utilizados en función de la información expuesta en el campo código referente al encabezado ICMPv6.

Tabla 1.3 Mensajes ICMPv6.

Código	Significado
1	Destino Inalcanzable (***Destination Unrechable***)
2	Datagrama Demasiado Grande (***Packet too Big***)
3	Tiempo de Respuesta Agotado (***Time Exceeded***)
4	Parámetros Incorrectos (***Parameter Problem***)
128	Solicitud de Eco (***ECHO Request***)
129	Respuesta de Eco (***ECHO Reply***)
133	Solicitud de Router (***Router Solicitation,* RS**)
134	Advertencia de Router (***Router Advertisement,* RA)**
135	Solicitud de Vecino ***(Neighbor Solicitation,* NS**)
136	Advertencia de Vecino ***(Neighbor Advertisement,* NA**)

1.4.1 Descubrimiento de Vecino

El protocolo ND es el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros en su mismo enlace, determina sus direcciones en la capa de enlace, localiza los Routers y mantiene la información de conectividad acerca de las rutas a los vecinos activos.

El protocolo ND se emplea también para mantener actualizadas las memorias intermedias donde se almacena la información relativa al contexto de la red a la que está conectada un Host o un Router, y para detectar cualquier cambio en la misma. Si un Router o una ruta falla, el Host buscará alternativas funcionales.

ND se apoya fundamentalmente en mensajes ICMPv6 como: RS, RA, NS y NA.

- **RS**: Este mensaje es generado por una interfaz cuando es activada para pedir a los Routers que se anuncien inmediatamente y así obtener la información proveniente del mensaje RA.
- **RA**: Este mensaje es generado por los Routers periódicamente o como respuesta a un mensaje RS, posee información referente a: prefijos de red (uno o varios), tiempo de vida, límite de salto sugerido, MTU, etc.

- **NS**: Este mensaje puede ser generado por los nodos para solicitar la dirección física de la capa de enlace (***dirección MAC***) de su vecino, así como para detectar direcciones duplicadas (***Duplicate Address Detection,* DAD**) (Moore, 2006, Costa et al., 2013).
- **NA:** Este mensaje es generado como respuesta a un mensaje de NS.

El protocolo ND corresponde a una combinación de los protocolos ICMP y ARP (***Address Resolution Protocol***) (Arkko and Pignataro, 2009) en IPv4. A continuación se presentan algunas ventajas de ND frente a los mecanismos existentes en IPv4:

- El descubrimiento de Routers es parte de la base del protocolo, no se tiene que recurrir a protocolos de enrutamiento.
- El anuncio de Router incluye las direcciones de la capa de enlace, no es necesario ningún intercambio adicional de paquetes para su resolución.
- El anuncio de Router incluye los prefijos para el enlace, por lo que no hay necesidad de un mecanismo adicional para configurar la máscara de red.
- El anuncio de Router permite la autoconfiguración de direcciones.
- Los Routers pueden anunciar a los Host del mismo enlace la MTU del enlace.
- Se pueden asignar múltiples prefijos al mismo enlace y por defecto los Hosts aprenden todos los prefijos gracias al mensaje RA.
- A diferencia de ARP, en ND se pueden detectar fallos de la mitad del enlace, es decir, con conectividad en un solo sentido, evitando el tráfico hacia ellos.
- El uso de direcciones de Enlace Local para identificar Routers, permite a las máquinas que mantengan su asociación con los mismos, en el caso de que se realice una renumeración para usar nuevos prefijos globales.

CAPÍTULO 2. PRÁCTICAS DE LABORATORIO VIRTUAL

Este capítulo se dedica a tratar los elementos que describen los escenarios referentes a cada una de las prácticas a desarrollar, donde, sobre cada uno de los dispositivos de red que conforman dichos escenarios se enfatiza en aspectos como: Tipos de dispositivos de red, sistemas operativos, función general de cada dispositivo de red, etc. Además se dedica a tratar las potencialidades de las herramientas virtuales a utilizar para el desarrollo de las prácticas.

2.1 Prácticas a Desarrollar

Los temas seleccionados para el desarrollo de las prácticas fueron: Configuración Estática y Configuración Dinámica. En el primer tema se desarrolla solo una práctica de laboratorio virtual, la cual tiene como objetivo, mostrar los elementos fundamentales sobre el proceso de configuración estática en las interfaces de cada uno de los diferentes dispositivos de red. Por su parte, en el segundo tema se desarrollan dos prácticas de laboratorio virtual, las cuales tienen como objetivo, mostrar los elementos fundamentales sobre las diferentes formas de configuración dinámica utilizadas por los diferentes dispositivos de red.

2.1.1 Práctica Configuración Estática

La primera práctica trata acerca de la configuración estática de cada una de las interfaces de los diferentes dispositivos de red a utilizar en el escenario. La Figura 2.1 muestra el escenario de red escogido para el desarrollo de dicha práctica.

Los dispositivos de red que se muestran en el escenario son:

- Un Host (PC1)
- Un Switch capa 2 (SW1)

- Un Router (GW)

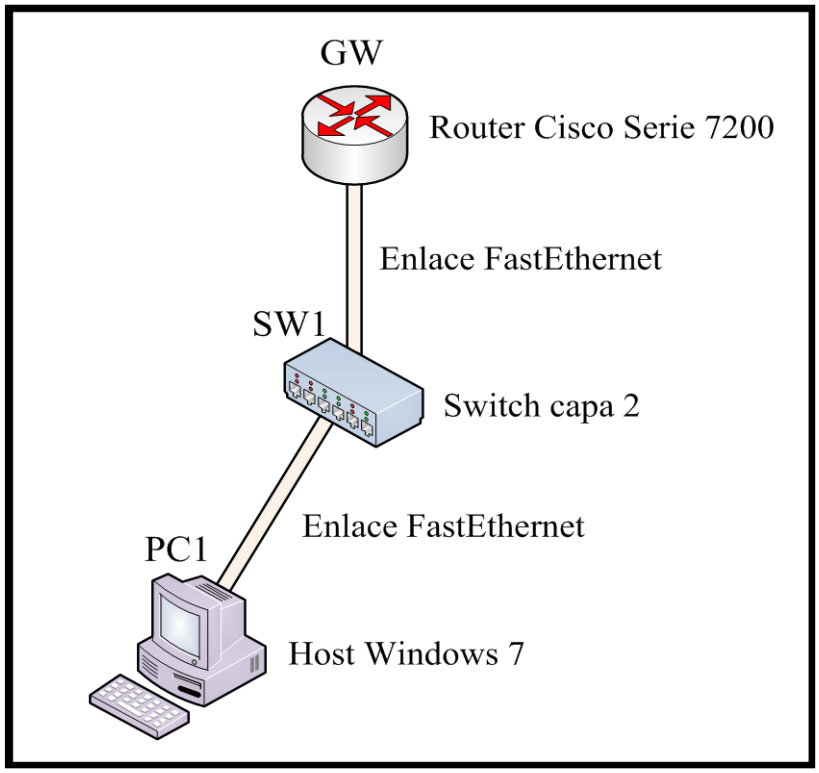


Figura 2.1 Escenario práctica de laboratorio virtual 1

El sistema operativo escogido para el Host a utilizar en el escenario de la Figura 2.1 fue ***Window 7*** (Microsoft, 2014). Es importante señalar que dicha selección no se realizó por alguna razón en específico, simplemente se escogió el mismo por su capacidad de soportar cualquier técnica de configuración IPv6 en sus interfaces. Este sistema operativo puede ser sustituido por cualquier otro sistema operativo, ya sea otra versión de Windows u otra versión de cualquier otro tipo de sistema operativo (Linux, Unix, Solaris, etc) (Linux, 2014, Unix, 2014, Solaris, 2014), en cualquiera de los casos, el requerimiento fundamental es que el mismo tenga soporte para las diferentes técnicas de configuración de direcciones IPv6.

El Switch SW1 simplemente es un Switch capa 2 Ethernet (IEEE, 2014) encargado de conmutar paquetes en la capa de enlace. La configuración de dicho dispositivo se mantiene como viene por defecto en la herramienta de simulación.

El Router GW se crea con el objetivo de que funcione como puerta de enlace predeterminada para el Host. Es un Router de la serie 7200 de Cisco (System, 2010), este Router provee soporte para cualquier técnica de configuración de direcciones IPv6 en sus interfaces. Es importante señalar que dicha selección no se realizó por alguna razón en específico, simplemente se escogió dicho Router puesto que el mismo soporta cualquier técnica de configuración de direcciones IPv6 en sus interfaces y se cuenta con los ficheros imágenes de esta serie de Routers de Cisco. Cualquier otro Router con soporte para IPv6 puede ser utilizado.

Los enlaces utilizados son del tipo FastEthernet.

El objetivo fundamental es lograr que las interfaces de los dispositivos de red implicados (Host y Router) se configuren de manera estática, haciendo énfasis en la configuración del Router, pues es recomendable que este tipo de dispositivo posea una dirección de red configurada de manera estática y más aún por la función que realiza el mismo en este escenario (puerta de enlace predeterminada).

2.1.2 Práctica autoconfiguración sin estado

La primera práctica referente al segundo tema, trata acerca del proceso SLAAC en cada una de las interfaces de los diferentes dispositivos de red a utilizar en el escenario. El escenario referente a esta práctica es el mismo que el mostrado en la Figura 2.1.

El objetivo fundamental es lograr que las interfaces de los dispositivos de red implicados (Host y Router GW) utilicen SLAAC para la autoconfiguración de sus interfaces. Para ello se configura la interfaz del Router GW de manera que brinde al Host la información requerida para que el mismo autoconfigure su interfaz de red, se hace énfasis en este proceso de configuración por su amplia utilidad.

2.1.3 Práctica DHCPv6

La segunda práctica referente al segundo tema, trata acerca de la configuración mediante DHCPv6 en cada una de las interfaces de los diferentes dispositivos de red a utilizar en los escenarios. Dicha práctica se divide en dos partes fundamentales: la primera parte trata acerca de la configuración mediante DHCPv6 sin estado en cada una de las interfaces,

mientras que la segunda parte trata acerca de la configuración mediante DHCPv6 con estado en cada una de las interfaces.

Las funcionalidades de servidor DHCPv6 en cada una de las partes de la práctica va a ser configurada en el Router GW. Esta funcionalidad también puede ser realizada por un Servidor profesional. La Figura 2.2 muestra el escenario de red escogido para el desarrollo de dicha práctica.

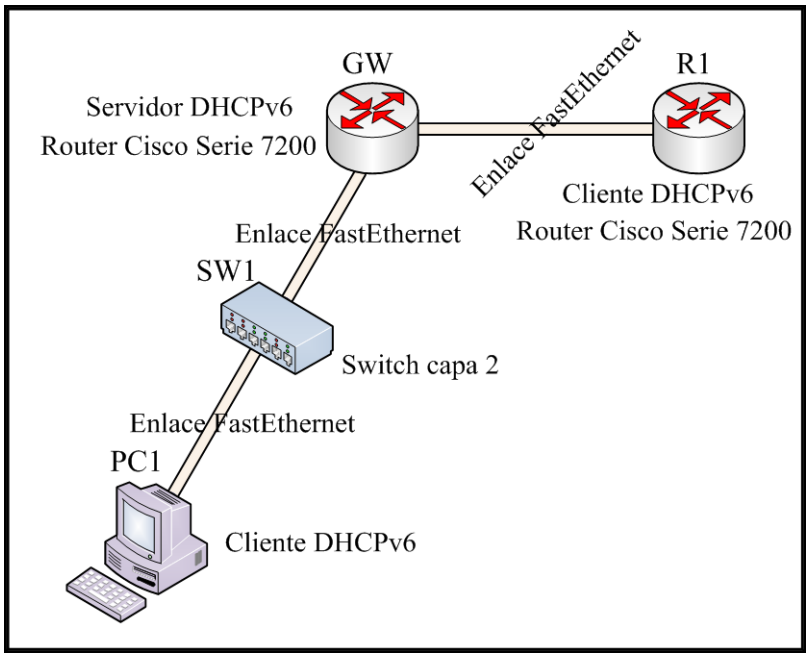


Figura 2.2 Escenario práctica de laboratorio virtual 3

El objetivo fundamental de la primera parte de la práctica es lograr que las interfaces de los dispositivos de red implicados (Host y Router R1) configuren su interfaz utilizando la combinación de SLAAC y DHCPv6. Este escenario se diferencia al de la Figura 2.1 en que utiliza además otro Router (R1), se agrega este dispositivo para que el mismo al igual que el Host PC1 funcionen como clientes DHCPv6, mostrando que los clientes no necesariamente tienen que ser equipos terminales de red. (Headquarters, 2012a).

El objetivo fundamental de la segunda parte de la práctica es lograr que las interfaces de los dispositivos de red implicados (Host y Router R1) configuren su interfaz utilizando DHCPv6. Para esta parte de la práctica se utiliza el mismo escenario de la Figura 2.2.

2.2 GNS3

GNS3 (***Graphical Network Simulator 3***) es un emulador de redes que permite la virtualización de redes complejas. Es empleado para virtualizar sistemas operativos como Windows, Linux, etc. GNS3 es usado además para la emulación de imágenes IOS (***Internetwork Operating System***) de Routers Cisco. (Cioara, 2014).

GNS3 utiliza las herramientas *Dynamips* y *Dynagen*, las cuales son las herramientas que permiten la emulación de las imágenes IOS de Routers Cisco. Usando un simple editor de textos, un usuario podría crear su propio fichero de topología con la red a emular por Dynagen. GNS3 facilita este proceso creando para ello una sencilla interfaz gráfica que abstrae al usuario de los detalles de configuración del escenario.

GNS3 es un emulador de código abierto (***Open Source***) multiplataforma que está disponible para Linux, Windows y Mac OS X (Apple, 2014).

Para virtualizar los dispositivos de red (Routers, Switches, etc.) son necesarias las imágenes del sistema operativo IOS. Sin embargo, por restricciones de licencia, el simulador no viene con las imágenes IOS de Routers Cisco. Estas deben ser descargadas directamente desde el sitio oficial de Cisco. (System, 2014).

Entre las características más importantes de GNS3 (Cioara, 2014), podemos destacar:

- Diseño gráfico de topologías de red a emular.
- Emulación de una gran variedad de IOS Cisco, JunOS, IPS y firewalls CISCO de tipo ASA y PIX.
- Conexión de la red simulada a un entorno real.
- GNS3 permite a varios usuarios trabajar sobre la misma topología.
- Integración con Qemu y VirtualBox para emular Hosts.
- Captura de paquetes integrada usando Wireshark.

GNS3 permite estudiar protocolos de red, hacer espejos de despliegues reales de infraestructuras de red para probar efectos en los cambios de configuración. Con este emulador se pueden desplegar infraestructuras tan complejas como se necesite.

GNS3 es una herramienta que está en continuo desarrollo, agregando nuevas funcionalidades. Actualmente la compañía Cisco certifica sus especialistas con esta herramienta. (CCNA, CCNP, CCIE, etc). (System, 2014).

A continuación se muestra un resumen de las características fundamentales que hacen que este sea la herramienta de simulación de red escogida para el desarrollo de las prácticas:

- Se encuentra disponible de forma gratuita en Internet para múltiples plataformas.
- Permite emular imágenes de equipos reales. Ejemplo: Routers de Cisco.
- Se integra con herramientas virtuales como VirtualBox y Wireshark.
- Es la herramienta utilizada actualmente para la certificación de los especialistas de la compañía líder mundialmente en equipos de comunicación (Cisco).
- Permite conectar la red virtual con la red real a través del Host anfitrión.

La Figura 2.3 muestra el área general de trabajo de dicha herramienta virtual. Las partes correspondientes al área general de trabajo de GNS3 se explican con más detalle en (Cioara, 2014).

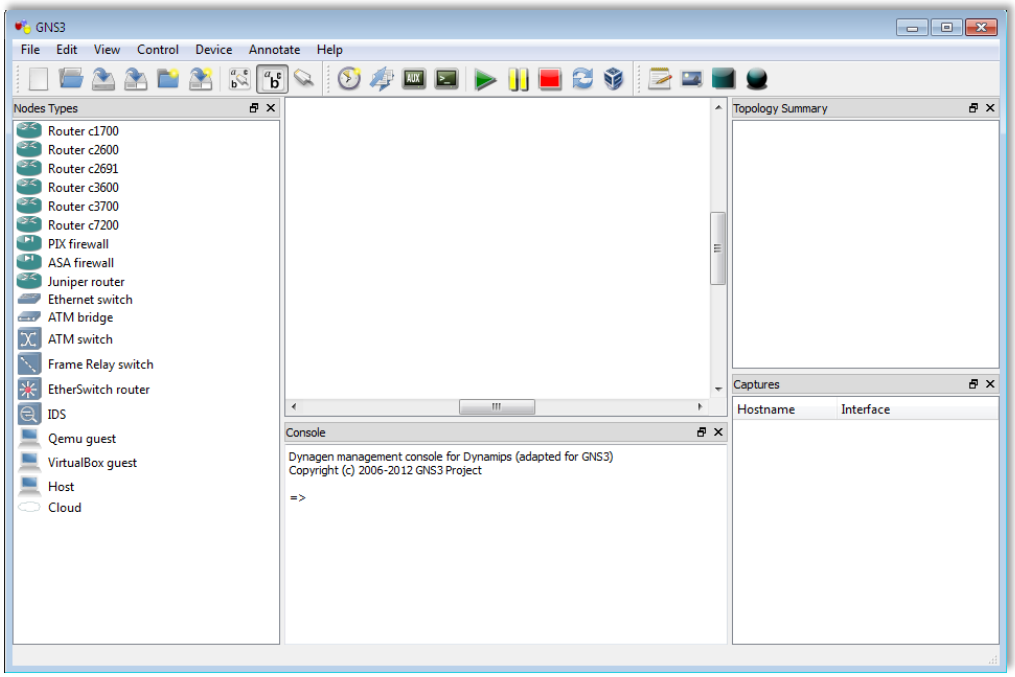


Figura 2.3 Área general de trabajo GNS3

2.2.1 GNS3 en las prácticas de laboratorio virtual

Las funciones fundamentales de GNS3 en el desarrollo de las prácticas de laboratorio virtual son:

- Describir la topología de red referente a cada escenario a desarrollar.
- Emular la o las imágenes referentes a los equipos de red a utilizar. En el caso de las prácticas sería emular la imagen del Router Cisco de la serie 7200 a utilizar.
- Conectar la o las máquinas virtuales creadas en VirtualBox a la red virtual.
- Propiciar el uso de Wireshark como analizador de red para comprobar el funcionamiento de la red.

La Figura 2.4 muestra parte del proceso de creación de la topología perteneciente a la práctica de laboratorio virtual 2.

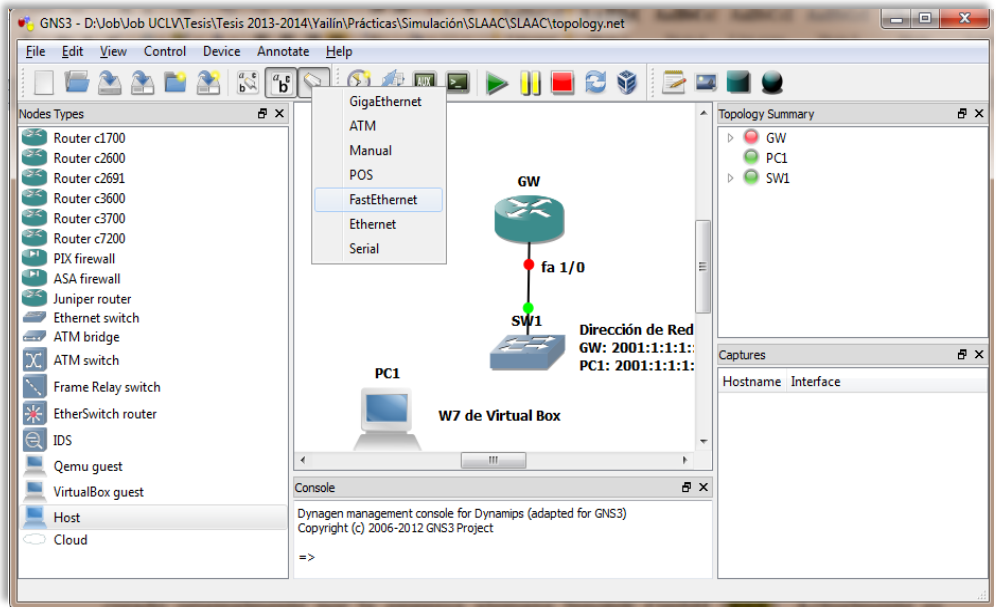


Figura 2.4 Creación de la Topología de red práctica de laboratorio virtual 2

2.3 VirtualBox

Oracle VM VirtualBox es un software de virtualización para arquitecturas x86/amd64, creado originalmente por la empresa alemana Innotek GmbH. Actualmente es desarrollado por la Corporación Oracle (Oracle, 2014a) como parte de su familia de productos de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos

adicionales (sistemas invitados), dentro de otro sistema operativo (anfitrión), cada uno con su propio ambiente virtual.

Entre los sistemas operativos soportados (en modo anfitrión) se encuentran GNU/Linux, Mac OS X, OS/2 Warp, Microsoft Windows, y Solaris/OpenSolaris, y dentro de ellos es posible virtualizar los sistemas operativos FreeBSD, GNU/Linux, OpenBSD, OS/2 Warp, Windows, Solaris, MS-DOS y muchos otros. (Oracle, 2014b).

VirtualBox ofrece algunas funcionalidades interesantes, como la ejecución de máquinas virtuales de forma remota, por medio de la herramienta **RDP** (***Remote Desktop Protocol***).

En cuanto a la emulación de hardware, los discos duros de los sistemas invitados son almacenados en los sistemas anfitriones como archivos individuales en un contenedor llamado **VDI** (***Virtual Disk Image)***, incompatible con los demás software de virtualización. Otra de las funciones que presenta es la de montar imágenes ISO como unidades virtuales ópticas de CD (***Compact Disc***) o DVD (***Digital Versatile Disc***). (Oracle, 2014b).

VirtualBox es una herramienta potente que permite experimentar con los sistemas operativos actuales más utilizados. Además, está integrado a GNS3.

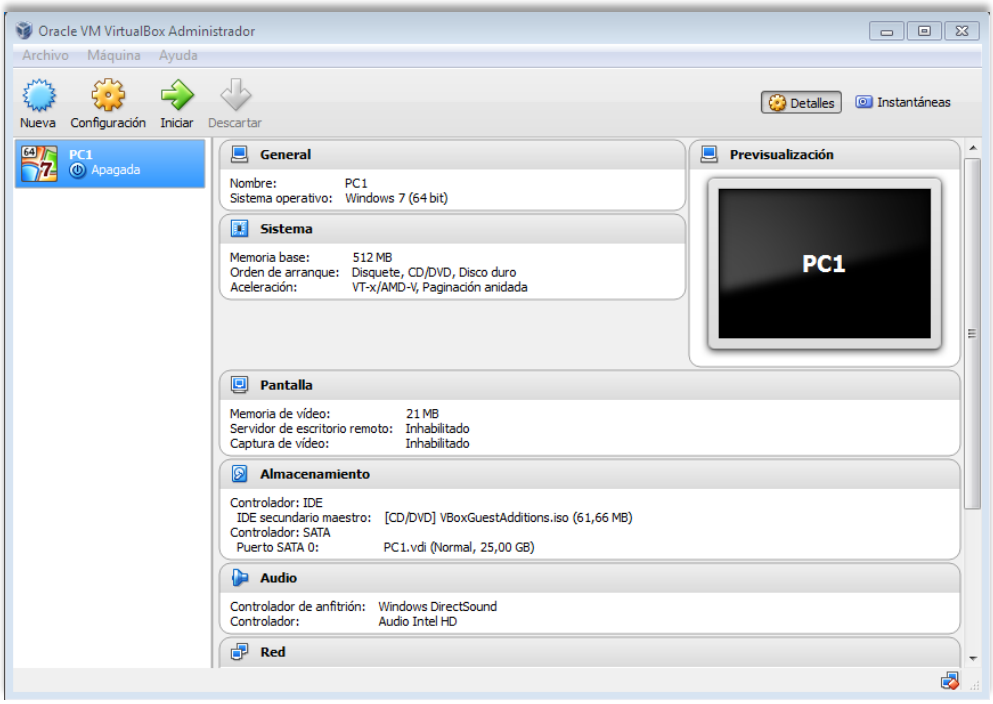


Figura 2.5 Área general de trabajo VirtualBox

La Figura 2.5 muestra el área general de trabajo de dicha herramienta virtual. Las partes correspondientes al área general de trabajo de VirtualBox se explican con más detalle en (Oracle, 2014b).

2.3.1 VirtualBox en las prácticas de laboratorio virtual

La función fundamental de VirtualBox en el desarrollo de las prácticas de laboratorio virtual es la de crear el Host PC1, el cual va a ser una máquina virtual con sistema operativo ***Windows 7***, sobre la cual se van a desarrollar la mayor parte de las pruebas y así comprobar el buen desarrollo de la configuración de la red. Figura 2.6.

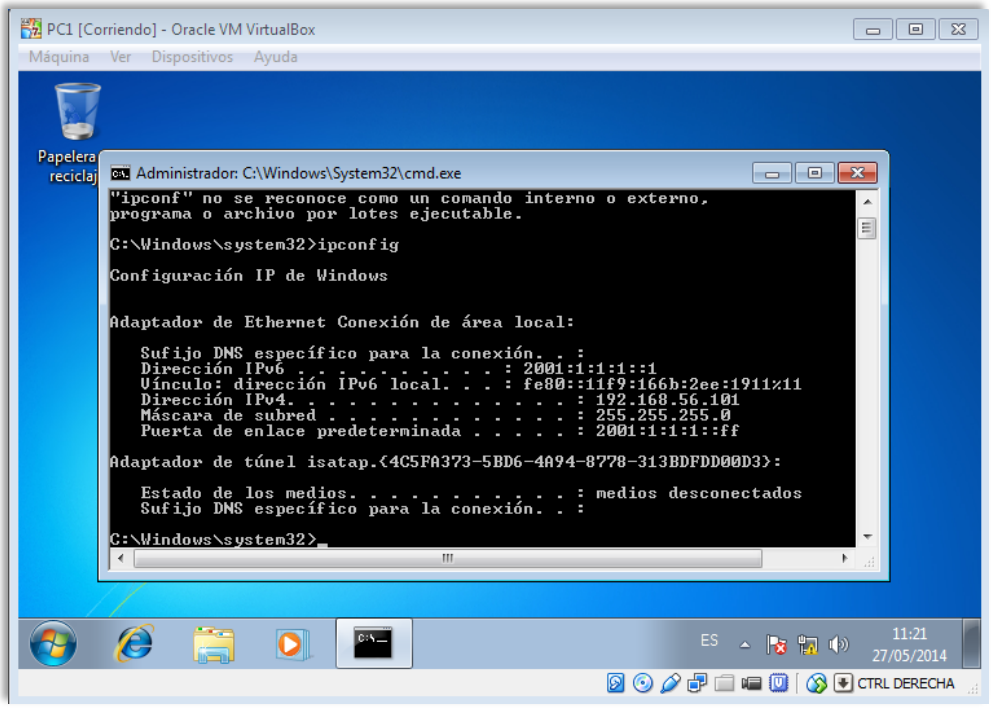


Figura 2.6 PC1 creada en VirtualBox

2.4 Wireshark

El analizador Wireshark, es uno de los más populares analizadores que existen. Se trata de una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo de tráfico en un momento determinado. Se trata de un producto gratuito cuyas características (Wireshark, 2014) más relevantes son:

- Disponible para UNIX, LINUX, Windows y Mac OS.

- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.
- Permite obtener estadísticas.
- Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

Este analizador de protocolos de red (***Sniffer***), visualiza el tráfico de paquetes que circulan por las redes de computadores, permitiendo analizar el comportamiento de las mismas, detectando errores, congestión, etc.

Su funcionamiento consiste en capturar una copia de estos paquetes para realizar un análisis posterior, el cual se presenta textual o gráficamente, dependiendo de las capacidades de la herramienta en cuestión.

Normalmente realiza dos tipos de análisis: el estructural y el estadístico. Con el análisis estructural se observa la composición y detalles de los paquetes capturados como contenido de cabeceras, nombre protocolo, datos del cuerpo del mensaje, etc. Con el análisis estadístico se obtienen estimados de tráfico: cantidad de paquete por tipo y tiempo. Por ejemplo, un administrador de red puede estudiar qué partes de la red están más saturadas y cuáles protocolos y máquinas están generando más tráfico, y de ese modo podrá sugerir las acciones correctivas necesarias.

Adicionalmente, muchos analizadores son capaces de seguir una conversación con lo que facilitan la resolución de problemas y la depuración del software de red durante su desarrollo.

La Figura 2.7 muestra el área general de trabajo de dicha herramienta virtual. Las partes correspondientes al área general de trabajo de Wireshark se explican con más detalle en (Lamping and Warnicke, 2013).

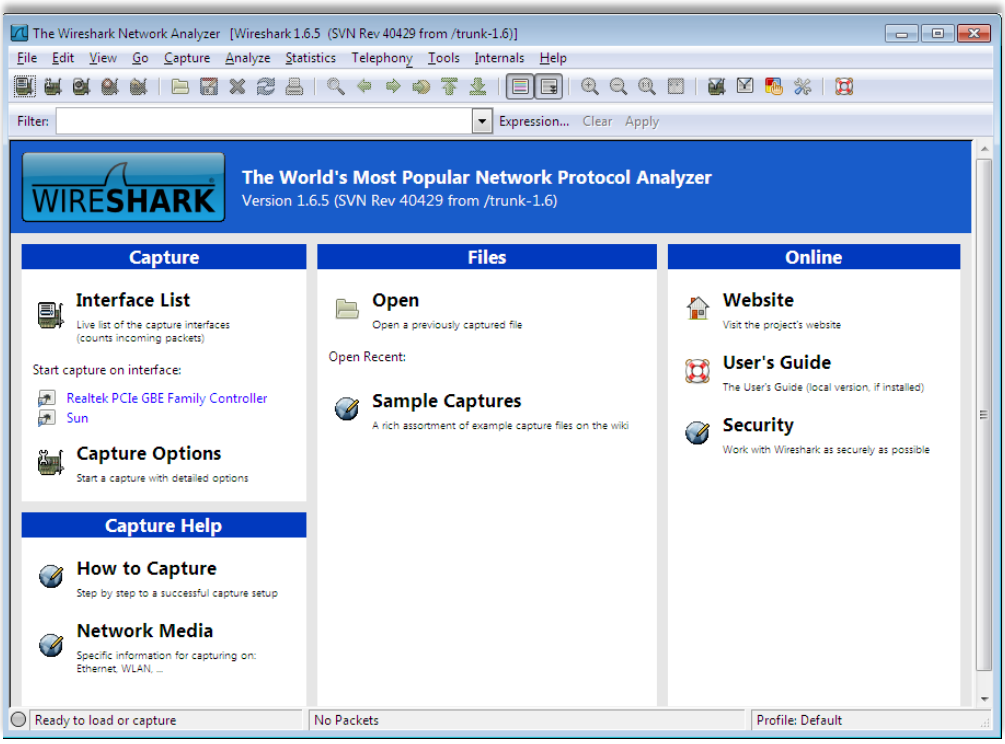


Figura 2.7 Área general de trabajo Wireshark

2.4.1 Wireshark en las prácticas de laboratorio virtuales

Las funciones fundamentales de Wireshark en el desarrollo de las prácticas de laboratorio virtual son:

- Mostrar los procesos dinámicos de las técnicas de configuración de direcciones IPv6.
- Comprobar el buen funcionamiento de la red.

La Figura 2.8 muestra la captura de mensajes RA en la interfaz perteneciente al Host PC1 en la práctica de laboratorio virtual 2, en la misma se muestra parte de la información contenida en este tipo de mensaje.

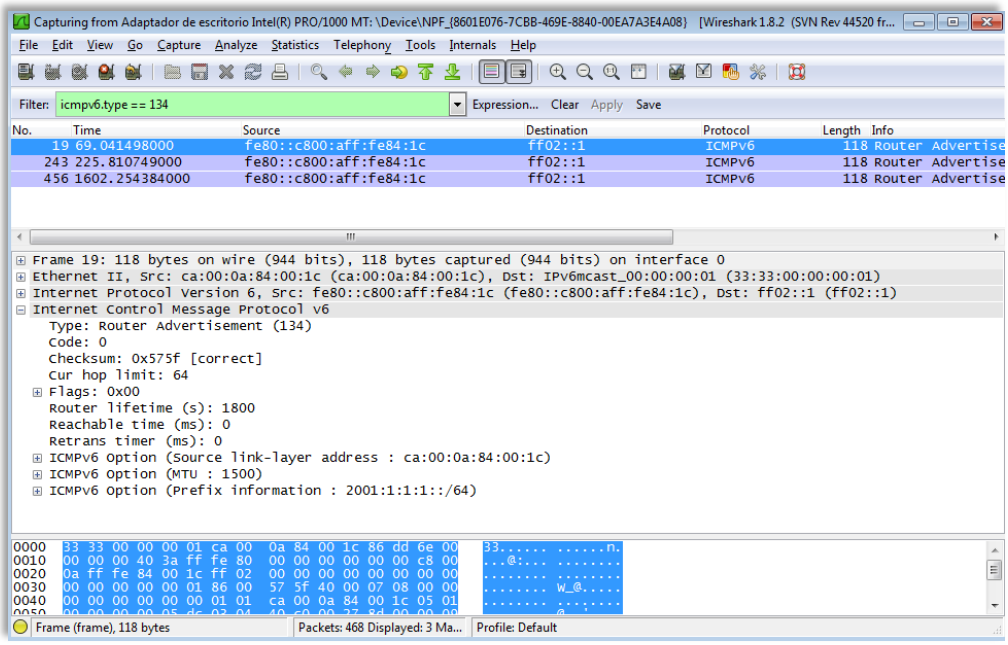


Figura 2.8 Captura de mensajes RA en el Host PC1

CAPÍTULO 3. ESTRUCTURA DE LAS PRÁCTICAS DE LABORATORIO VIRTUAL

3.1 Las Nuevas Tecnologías de la Información y las Comunicaciones en el proceso de enseñanza y aprendizaje

Las tendencias de cambio que han introducido las Nuevas Tecnologías de la Información y las Comunicaciones (***NTIC*****)** en el proceso de desarrollo tecnológico producido por el hombre, ha desencadenado un aprovechamiento transformador entorno a diversas actividades humanas, las cuales llevan a aumentar la productividad del trabajo en su gran diversidad. Uno de los campos invadidos por las NTIC es la educación, que a pesar de no ser creadas de manera específica para este fin, por las características propias de estas tecnologías, constituyen una oportunidad extraordinaria y al mismo tiempo un reto para la enseñanza en todos sus niveles. Las NTIC brindan las condiciones óptimas para hacer de la educación un terreno más participativo, centrado en alcanzar diversos aprendizajes que posean una real significación para cada estudiante, aumentando de esta manera la capacidad creativa e innovadora. (Avila, 2003, Valiente and González, 2013, Pérez, 2013).

Las NTIC brindan la posibilidad al estudiante de interactuar en un entorno digital aplicando sus conocimientos y la facilidad de construir de manera práctica lo que de forma real no pudiera efectuar; una de las formas más concretas de explotar las NTIC es mediante el desarrollo de prácticas de laboratorio virtual.

Las prácticas de laboratorio virtual se efectúan mediante el uso de herramientas virtuales, donde el usuario interactúa con dichas herramientas virtuales las cuales generalmente se encuentran corriendo sobre una computadora personal (***Personal Computer,* PC**) para

simular situaciones reales, brindándole al estudiante la posibilidad de desarrollar sus habilidades y de tomar decisiones ante diversas situaciones que pudiera experimentar.

Las ventajas que ofrecen las NTIC permiten a los centros de estudio racionalizar recursos y a su vez formar habilidades en el estudiante que por el camino del experimento real no podrían ser costeadas.

3.2 Estructura del documento guía

La estructura seguida en la confección de los documentos guías referentes a cada una de las prácticas de laboratorio virtual es la siguiente:

- Tema
- Título
- Objetivos
- Conocimientos Previos
- Habilidades
- Tarea Preliminar
- Técnica Operatoria
- Conclusiones
- Estudio Independiente.
- Referencias Bibliográficas

Para la selección de la estructura seguida en la confección de los documentos guías referente a cada una de las prácticas de laboratorio virtual se toma como referencia a (Chaljub et al., 1999, Paliza, 2013), documentos desarrollados por profesores de prestigio de la UCLV que validan dicha selección.

A continuación se realiza una breve descripción de cada una de las partes que conforman la estructura de los documentos guías tomando como referencia una de las prácticas de laboratorio virtual desarrollada.

3.2.1 Tema y Título

Tema: Es una frase relativamente pequeña que da a conocer el tema a tratar, el mismo se puede desarrollar en una o varias actividades, en el caso que nos ocupa se desarrollan varias prácticas de laboratorio virtual para tratar dicho tema.

Título: Es una frase relativamente pequeña que da a conocer un asunto específico dentro de un tema general.

La Figura 3.1 muestra un fragmento de la práctica de laboratorio virtual 2, en la misma aparece el tema general a tratar y el título referente a dicha práctica de laboratorio virtual. Se puede ver como el tema hace referencia de manera general a la configuración de direcciones IPv6, mientras que el título se encarga de hacer referencia a las técnicas de configuración de direcciones IPv6 específicas a tratar en dicha práctica.

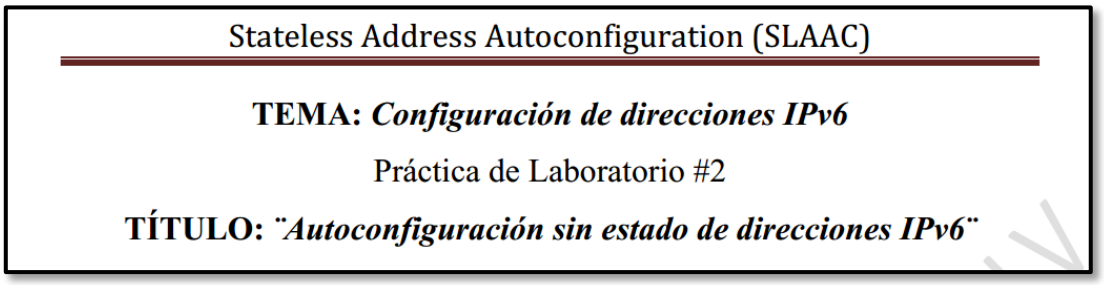
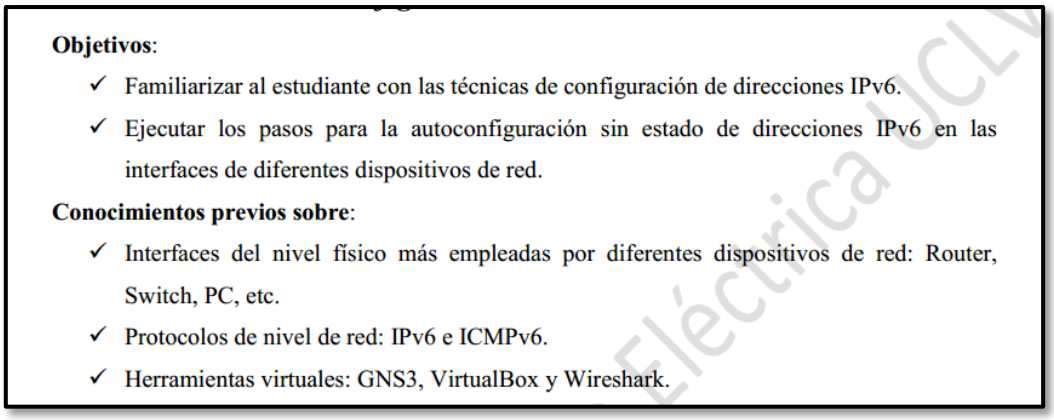


Figura 3.1 Tema y Título referentes a la práctica de laboratorio virtual 2.

3.2.2 Objetivos y Conocimientos Previos

Objetivos: Identifican la finalidad a la cual deben dirigirse los recursos y esfuerzos en aras de dar cumplimiento a los propósitos. La Figura 3.2 muestra un fragmento de la práctica de laboratorio virtual 2, en la misma aparecen los objetivos referentes a dicha práctica, los cuales plantean que es lo que se desea conseguir al culminar la actividad. Es importante señalar que el resto de los puntos a tratar en la práctica se deben enfocar de manera tal que tributen al logro de los objetivos planteados.

Conocimientos Previos: Se refiere a los conocimientos teóricos que el estudiante debe tener en aras de tributar al cumplimiento de los objetivos trazados en la práctica, además, dar cumplimiento a este punto propicia dinamismo al desarrollo de la actividad. La Figura 3.2 muestra un fragmento de la práctica de laboratorio virtual 2, en la misma aparecen los aspectos teóricos que el estudiante debe dominar en esta práctica.



Objetivos:

- ✓ Familiarizar al estudiante con las técnicas de configuración de direcciones IPv6.
- ✓ Ejecutar los pasos para la autoconfiguración sin estado de direcciones IPv6 en las interfaces de diferentes dispositivos de red.

Conocimientos previos sobre:

- ✓ Interfaces del nivel físico más empleadas por diferentes dispositivos de red: Router, Switch, PC, etc.
- ✓ Protocolos de nivel de red: IPv6 e ICMPv6.
- ✓ Herramientas virtuales: GNS3, VirtualBox y Wireshark.

Figura 3.2 Objetivos y Conocimientos Previos referentes a la práctica de laboratorio virtual 2.

3.2.3 Habilidades y Tarea Preliminar

Habilidades: El termino habilidad se puede definir como la destreza para ejecutar alguna acción en aras de alcanzar un objetivo. La Figura 3.3 muestra un fragmento de la práctica de laboratorio virtual 2, en la misma aparece la habilidad práctica que el estudiante debe tener en aras de tributar al cumplimiento de los objetivos referentes a dicha práctica. Es importante señalar que las habilidades para todas la prácticas de laboratorio virtual a desarrollar están destinadas únicamente al dominio de los comandos referentes al sistema operativo IOS de Cisco, esto se debe a que gran parte del contenido práctico referente a la Técnica Operatoria se realiza configurando Routers de Cisco con la ayuda de estos comandos, por tanto, se hace importante que el estudiante domine al menos los comandos esenciales, y así fluya con más dinamismo la actividad.

Tarea Preliminar: Este punto recomienda al estudiante preparar el Host a utilizar en los escenarios referentes a las prácticas de laboratorio virtual. Dicha recomendación se realiza debido a que el proceso de instalación referente a cualquier sistema operativo puede representar un tiempo valioso en el desarrollo de la actividad. Es importante señalar que a pesar de que pudieron explotarse otros mecanismos que exoneraran al estudiante del desarrollo de este paso, se considera que es un punto importante pues propicia el desarrollo de habilidades en los procesos referentes al manejo de sistemas operativos. La Figura 3.3 muestra un fragmento de la práctica de laboratorio virtual 2 donde aparece la Tarea Preliminar a desarrollar por el estudiante.

Habilidades

Saber utilizar los comandos del sistema operativo IOS de CISCO.

Tarea Preliminar

Prepare la máquina virtual a utilizar en la práctica. Para ello guíese por la información ofrecida en (Oracle, 2014).

Nota: *Instale* ***Windows*** *7 como sistema operativo para dicha PC virtual.*

Figura 3.3 Habilidades y Tarea Preliminar referentes a la práctica de laboratorio virtual 2.

3.2.4 Técnica Operatoria

Técnica Operatoria: Contiene las acciones que el estudiante debe realizar durante el desarrollo de la práctica de laboratorio virtual en aras de dar cumplimiento a los objetivos propuestos.

Las acciones a realizar por los estudiantes durante la Técnica Operatoria se pueden desglosar en los siguientes puntos:

- Creación del o los escenarios de red a utilizar.
- Configuración de los dispositivos de red que conforman el o los escenario de red a utilizar.
- Preguntas de comprobación.

A continuación se muestra una breve descripción de los puntos que conforman la Técnica Operatoria.

➢ **Creación del o los escenarios de red**

En este punto de la Técnica Operatoria el estudiante debe mostrar sus conocimientos sobre el manejo de la herramienta virtual GNS3, así como sus conocimientos sobre las interfaces físicas de los dispositivos de red. Igualmente este punto propicia el desarrollo de nuevas habilidades por parte de los estudiantes. La Figura 3.4.

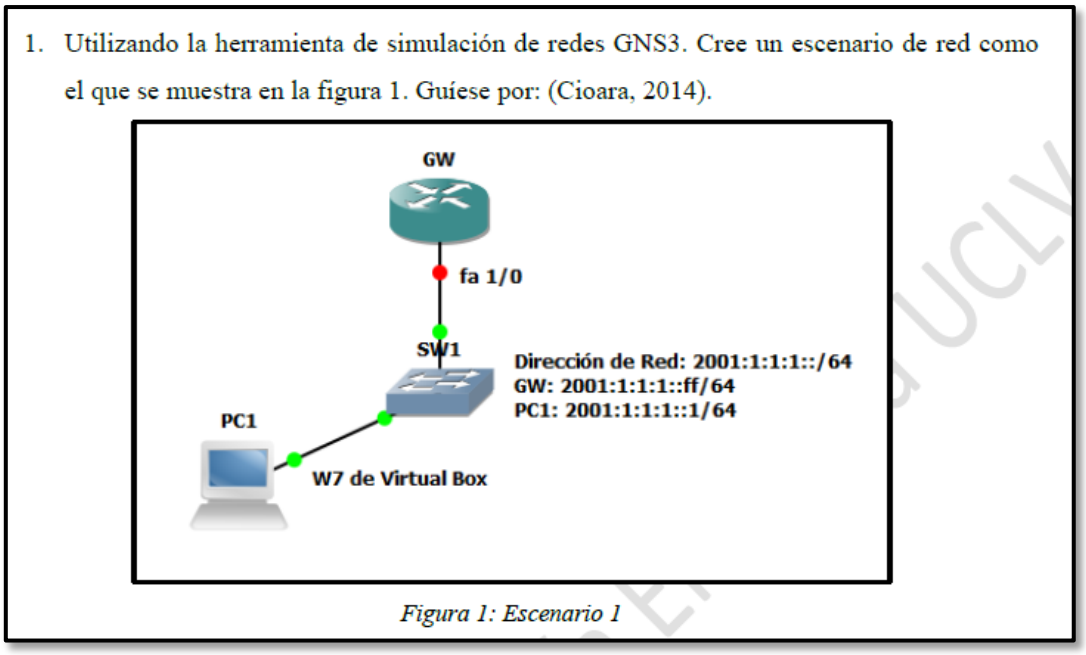


Figura 3.4 Fragmento donde se recrea el primer punto de la Técnica Operatoria referente a la práctica de laboratorio virtual 2.

- **Configuración de los dispositivos de red**

Este punto de la Técnica Operatoria tiene un alto componente práctico. Para el desarrollo del mismo el estudiante tiene que configurar cada una de las interfaces referentes a los dispositivos de red, protocolos de enrutamiento en caso de que sean necesarios, y por último la técnica en si a tratar en la práctica, para ello deben guiarse por la información ofrecida en el escenario que se expone en el primer punto de la Técnica Operatoria (Figura 3.4), por la bibliografía ofrecida y por otras figuras informativas que se les brindan durante la Técnica Operatoria. Figura 3.5.

Es importante señalar que en mucho de los casos la información ofrecida no es suficiente, por ello, el estudiante tiene que ser capaz de adaptar la información con la que cuenta para dar cumplimiento a este punto de la Técnica Operatoria, de esta forma se desarrolla la capacidad de análisis y solución en los estudiantes.

5. Prenda el Router GW y pase a configurar la interfaz fa 1/0 vía comandos a través de la consola. Para ello guíese por la información ofrecida en el escenario de la Figura 1, del documento (Headquarters, 2012b) y de la información ofrecida en la Figura 3.

```
GW>enable
GW#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
GW(config)#ipv6 unicast-routing
GW(config)#interface fa 1/0
GW(config-if)#ipv6 address 2001:1:1:1::/64 eui-64
GW(config-if)#ipv6 address autoconfig
GW(config-if)#ipv6 enable
GW(config-if)#no shutdown
GW(config-if)#^Z
GW#
```

Figura 3. Pasos para la configuración de la interfaz fa 1/0 del Router GW

Figura 3.5 Fragmento donde se recrea parte del segundo punto de la Técnica Operatoria referente a la práctica de laboratorio virtual 2.

8. Vaya al analizador de red Wireshark ya ejecutado en la PC1 y filtre la captura aplicando la siguiente línea de comandos: ***ipv6.dst==ff02::1 or ipv6.dst==ff02::2***

Responda los siguientes puntos:

- Diga que tipos de mensajes ICMPv6 son capturados con estas características. Argumente.
- Seleccione uno de los mensajes ICMPv6 de solicitud de Router y del mismo responda:

Del Encabezado IPv6

Próximo encabezado: ____ Diga el significado.

Dirección IPv6 fuente: _____ ¿Por qué usa esta dirección?

Dirección IPv6 destino: _____ ¿Por qué usa esta dirección?

Del Encabezado ICMPv6

Tipo: ___ Código: ___ Diga el significado.

¿Qué función tiene este mensaje?

Figura 3.6 Fragmento donde se recrea parte del tercer punto de la Técnica Operatoria referente a la práctica de laboratorio virtual 2.

3.2.5 Conclusiones, Estudio Independiente y Referencias Bibliográficas

Conclusiones: Son determinaciones hechas mediante el estudio de los resultados del trabajo. Las conclusiones referentes a las prácticas se realizan a modo de preguntas, propiciando de esta forma que se pueda evaluar la capacidad de análisis y resumen por parte de los estudiantes, los cuales tienen que ser capaces en sus respuestas de resumir los puntos esenciales tratados en las prácticas. Figura 3.7.

Conclusiones

¿Qué ventajas tiene para la configuración de direcciones IPv6 utilizar el mecanismo SLAAC?

¿Qué limitaciones para los administradores de red tiene utilizar el mecanismo SLAAC?

Figura 3.7 Conclusiones referentes a la práctica de laboratorio virtual 2.

Estudio Independiente: Es el momento en el que se le indica al estudiante que ejercite y amplíe de manera independiente los conocimientos adquiridos en clases, además donde se indica el próximo contenido a tratar.

Estudio Independiente

1. Cree un escenario como el que se muestra en la Figura 4 y realice las siguientes operatorias:
   a. Configure el Router R2 de modo que adquiera su configuración IPv6 de red a través de la información ofrecida por el Router R1 utilizando SLAAC. Ver (Headquarters, 2012b).
   b. Confeccione un informe donde muestre los pasos elementales del desarrollo del inciso a y del éxito del proceso de configuración.

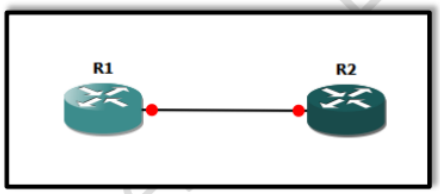


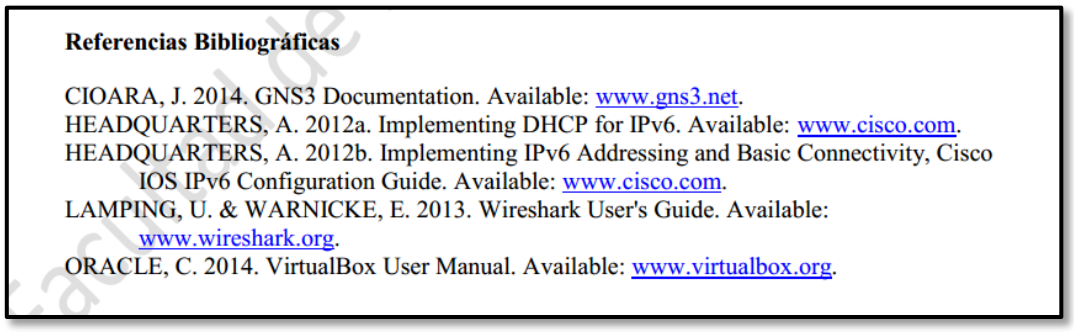
Figura 4. Escenario 2.

2. Estudiar el documento (Headquarters, 2012a) referente a la implementación de DHCPv6.

Figura 3.8 Estudio Independiente referente a la práctica de laboratorio virtual 2.

La Figura 3.8 muestra un fragmento de la práctica de laboratorio virtual 2, la misma muestra un primer punto donde el estudiante tiene que de manera independiente realizar un ejercicio y entregar un informe del mismo al profesor, propiciando así que el estudiante ejercite y amplíe los conocimientos adquiridos durante la práctica. El segundo punto se dedica a indicar el estudio del contenido a tratar en la siguiente práctica.

Referencias Bibliográficas: Validan el desarrollo y los resultados de la práctica de laboratorio virtual. La Figura 3.9 muestra un fragmento de la práctica de laboratorio virtual 2, en la misma se observa la bibliografía utilizada para el desarrollo de dicha práctica.



Referencias Bibliográficas

CIOARA, J. 2014. GNS3 Documentation. Available: www.gns3.net.
HEADQUARTERS, A. 2012a. Implementing DHCP for IPv6. Available: www.cisco.com.
HEADQUARTERS, A. 2012b. Implementing IPv6 Addressing and Basic Connectivity, Cisco IOS IPv6 Configuration Guide. Available: www.cisco.com.
LAMPING, U. & WARNICKE, E. 2013. Wireshark User's Guide. Available: www.wireshark.org.
ORACLE, C. 2014. VirtualBox User Manual. Available: www.virtualbox.org.

Figura 3.9 Referencias Bibliográficas referentes a la práctica de laboratorio virtual 2.

CONCLUSIONES

El informe reúne los elementos esenciales que definen el funcionamiento básico de los protocolos IPv6 e ICMPv6, así como los fundamentos acerca de las técnicas de configuración de direcciones IPv6 y de los temas escogidos para el desarrollo de las prácticas de laboratorio virtual, de donde, se concluye que:

- Dominar a plenitud las técnicas de configuración de direcciones IPv6 es un tema de vital importancia para los administradores de red, puesto que influyen directamente sobre el desempeño, administración y seguridad de las redes.
- Poseer un amplio conocimiento acerca del protocolo de control ICMPv6 es importante para determinar fallas en los procesos de configuración referentes a las técnicas de configuración de direcciones IPv6.

El informe fundamenta además acerca de las potencialidades de las herramientas virtuales utilizadas en la confección de las prácticas de laboratorio virtual, de donde, se concluye que:

- GNS3 es un potente simulador de redes que trabaja con imágenes reales de equipos de red lo que posibilita un mayor acercamiento al manejo de situaciones reales.

RECOMENDACIONES

Con el propósito de profundizar en el estudio del protocolo IPv6 y de las técnicas de configuración de direcciones IPv6 se recomienda considerar los siguientes aspectos.

- Extender el desarrollo de las prácticas de laboratorio virtual sobre DHCPv6 sin estado y con estado utilizando un servidor de red profesional.
- Poner a prueba las prácticas desarrolladas en aras de realizar los ajustes necesarios en cuanto a su estructura para un mayor aprovechamiento de las mismas.
- Desarrollar prácticas de laboratorio virtual sobre nuevos temas de IPv6 referentes a mecanismos de enrutamiento, Calidad de Servicio, Seguridad, Administración, etc.

REFERENCIAS BIBLIOGRÁFICAS

APPLE. 2014. *Mac OS* [Online]. www.apple.com.

ARKKO, J. & PIGNATARO, C. 2009. RFC 5494: IANA Allocation Guidelines for the Address Resolution Protocol (ARP). www.ietf.org.

ASAEDA, H. 2013. Draft: IGMP/MLD-Based Explicit Membership Tracking Function for Multicast Routers. www.ietf.org.

AVILA, E. 2003. Las Nuevas Tecnologías de la Información y la Comunicación como herramientas necesarias en la formación profesional de los estudiantes universitarios. Disponible en: http://www.ugr.es.

BONICA, R., GAN, D., TAPPAN, D. & PIGNATARO, C. 2007. RFC 4884: Extended ICMP to support Multi-Part Messages. www.ietf.org.

CARRELL, J. L. 2013. *Guide to TCP-IP*, http://www.google.com.cu/books, Cengage Learning.

CHALJUB, J. A., ROCHE, C. & HERNÁNDEZ, D. 1999. Prácticas de Laboratorio.

CIOARA, J. 2014. GNS3 Documentation. Disponible en: www.gns3.net.

CONTA, A. & GUPTA, M. 2006. RFC 4443: Internet Control Message Protocol (icmpv6) for the Internet Protocol Version 6 (ipv6) Specification. www.ietf.org.

COSTA, F., COMBES, J.-M. & POUGNARD, X. 2013. RFC 6957: Duplicate Address Detection Proxy. www.ietf.org.

DEERING, S. & HINDEN, R. 1998. RFC 2460: Internet Protocol, Version 6 (IPv6) Specification. www.ietf.org.

DEERING, S. E. & HINDEN, R. M. 2006. RFC 4291: IP version 6 addressing architecture. www.ietf.org.

DROMS, R. 2004. RFC 3736: Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6. www.ietf.org.

DROMS, R., BOUND, J., VOLZ, B., LEMON, T., PERKINS, C. & CARNEY, M. 2003. RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6). www.ietf.org.

GONT, F. & MANRAL, V. 2014. RFC 7112: Implications of Oversized IPv6 Header Chains. www.ietf.org.

HEADQUARTERS, A. 2012a. Implementing DHCP for IPv6. Disponible en: www.cisco.com.

HEADQUARTERS, A. 2012b. Implementing IPv6 Addressing and Basic Connectivity, Cisco IOS IPv6 Configuration Guide. Disponible en: www.cisco.com.

IANA 2014. Internet Assigned Numbers Authority. https://www.iana.org/.

IEEE 2014. IEEE 802.3 Ethernet Working Group. www.ieee.org.

IETF. 2014. *Internet Engineering Task Force Official Page* [Online]. www.ietf.org.

JIANG, S. & CARPENTER, B. 2014. RFC 7136: Significance of IPv6 Interface Identifiers. www.ietf.org.

KAWAMURA, S. & KAWASHIMA, M. 2010. RFC 5952: A Recommendation for IPv6 Address Text Representation. www.ietf.org.

KRISHNAN, S., MRUGALSKI, T., SIODELSKI, M., JIANG, S. & HANKINS, D. 2014. RFC 7227: Guidelines for Creating New DHCPv6 Options. www.ietf.org.

LAMPING, U. & WARNICKE, E. 2013. Wireshark User's Guide. Disponible en: www.wireshark.org.

LINUX. 2014. *Linux Official Page* [Online]. www.linux.com.

MCCANN, J., MOGUL, J. & DEERING, S. E. 1996. RFC 1981: Path MTU Discovery for IP version 6. www.ietf.org.

MICROSOFT. 2014. *Microsoft Official Page* [Online]. www.microsoft.com.

MOORE, N. 2006. RFC 4429: Optimistic Duplicate Address Detection (DAD) for IPv6. www.ietf.org.

NARTEN, T., THOMSON, S. & JINMEI, T. 2007. RFC 4862: IPv6 stateless address autoconfiguration. www.ietf.org.

ORACLE, C. 2014a. *Oracle VM VirtualBox Official Page* [Online]. www.virtualbox.org.

ORACLE, C. 2014b. VirtualBox User Manual. Disponible en: www.virtualbox.org.

PALIZA, F. A. 2013. Transición IPv4- IPv6 en una Red Empresarial.

PÉREZ, M. R. 2013. NTIC y los Procesos de Enseñanza y Aprendizaje.

POSTEL, J. 1981. RFC 791: Internet protocol. www.ietf.org.

SOLARIS, O. 2014. *Oracle Solaris Official Page* [Online]. www.oracle.com.

SYSTEM, C. 2010. Cisco Router Guide. Disponible en: www.cisco.com.

SYSTEM, C. 2014. *Cisco Official Page* [Online]. www.cisco.com.

TOUCH, J. 2013. RFC 6864: Updated Specification of the IPv4 ID Field. www.ietf.org.

UNIX. 2014. *Unix Official Page* [Online]. www.unix.org.

VALIENTE, I. B. Á. & GONZÁLEZ, H. C. F. 2013. Didáctica del proceso de formación de los profesionales asistido por las tecnologías de la información y la comunicación. ***Pedagogía Universitaria*** **[Online], 10. Disponible en: www.mes.edu.cu.**

VIDA, R., COSTA, L., FDIDA, S., DEERING, S., FENNER, B., KOUVELAS, I. & HABERMAN, B. 2004. RFC 3810: Multicast listener discovery version 2 (MLDv2) for IPv6. www.ietf.org.

VOLZ, B. & TROAN, O. 2013. Draft: Issues with multiple stateful DHCPv6 options. www.ietf.org.

WIRESHARK. 2014. ***Wireshark Official Page*** **[Online]. www.wireshark.org.**

GLOSARIO DE TÉRMINOS

ARP	Address Resolution Protocol
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CCIE	Cisco Certified Internetwork Expert
CD	Compact Disc
CPE	Client Premise Equipment
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DHCPv4	Dynamic Host Configuration Protocol version 4
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
DVD	Digital Versatile Disc
EUI-64	Extended Universal Identifier
GNS3	Graphical Network Simulator 3
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol versión 6
IETF	Internet Engineering Task Force
IOS	Internetwork Operating System
IP	Internet Protocol
IPng	Next Generation Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
MAC	Media Access Control
MLD	Multicast Listener Discovery
MTU	Maximun Transmition Unit
NA	Neighbor Advertisement
ND	Neighbor Discovery
NS	Neighbor Solicitation
NTIC	New Technologies of the Information and the Communications
PC	Computer Personal
RA	Router Advertisement
RDP	Remote Desktop Protocol

RS	Router Solicitation
SLAAC	Stateless Address Autoconfiguration
VDI	Virtual Disk Image